SANDIA REPORT
SAND2006-0193
Unlimited Release
Printed January 2006

Mathematical Investigation of One-Way Transform Matrix Options

Arlin Cooper

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2006-0193
Unlimited Release
Printed January 2006

Mathematical Investigation of One-Way Transform Matrix Options

Arlin Cooper, Airworthiness Assurance Department

Sandia National Laboratories
P.O. Box 8500
Albuquerque, NM 87185-0615

Key words: Unique Signals, one-way transforms, matrices

ABSTRACT

One-way transforms have been used in weapon systems processors since the mid- to late-1970s in order to help recognize insertion of correct pre-arm information while maintaining abnormal-environment safety. Level-One, Level-Two, and Level-Three transforms have been designed. The Level-One and Level-Two transforms have been implemented in weapon systems, and both of these transforms are equivalent to matrix multiplication applied to the inserted information. The Level-Two transform, utilizing a 6×6 matrix, provided the basis for the "System 2" interface definition for Unique-Signal digital communication between aircraft and attached weapons. The investigation described in this report was carried out to find out if there were other size matrices that would be equivalent to the 6×6 Level-Two matrix. One reason for the investigation was to find out whether or not other dimensions were possible, and if so, to derive implementation options. Another important reason was to more fully explore the potential for inadvertent inversion. The results were that additional implementation methods were discovered, but no inversion weaknesses were revealed.

Acknowledgment

The work documented in this report was supported by the Advanced System and Technology Unique Signal research program under the management of Mike McGlaun. Other key personnel who provided support and guidance were Heather Schriner, Jeffrey Brewer, and Matt Kerschen. The supporting software executions were performed by Bob Roginski.

Contents

Background 7
Transform Constraints 8
2×2 Matrix 9
3×3 Matrix 9
4×4 Matrix 10
6×6 Matrix. 11
8×8 Matrix. 19
12×12 Matrix. 22
24×24 Matrix. 23
Conclusions 25
Appendix A: Matrix Dimensions that Divide 48 27
16×16 Matrix 27
48×48 Matrix 41
Appendix B: Additional Pre-Arm Inversion Ranks that Divide 24 42
References 43

List of Tables

Table 1. Bit-Pattern Constraints for One-Way Transform 8
Table 2. Conditions for First Column of 6×6 Matrix 14
Table 3. Conditions for Second Column of 6×6 Matrix 15
Table 4. Conditions for Third Column of 6×6 Matrix 16
Table 5. Conditions for Fourth Column of 6×6 Matrix 16
Table 6. Conditions for Fifth Column of 6×6 Matrix 17
Table 7. Conditions for Sixth Column of 6×6 Matrix 18
Table 8. Conditions for First Column of 8×8 Matrix 21
Table 9. Conditions for First Column of 16×16 Matrix 32
Table 10. Conditions for Second Column of 16×16 Matrix 33
Table 11. Conditions for Third Column of 16×16 Matrix 33
Table 12. Conditions for Fourth Column of 16×16 Matrix 34
Table 13. Conditions for Fifth Column of 16×16 Matrix 34
Table 14. Conditions for Sixth Column of 16×16 Matrix 35
Table 15. Conditions for Seventh Column of 16×16 Matrix 35
Table 16. Conditions for Eighth Column of 16×16 Matrix 36
Table 17. Conditions for Ninth Column of 16×16 Matrix 36
Table 18. Conditions for Tenth Column of 16×16 Matrix 37
Table 19. Conditions for Eleventh Column of 8×8 Matrix 37
Table 20. Conditions for Twelfth Column of 8×8 Matrix 38
Table 21. Conditions for Thirteenth Column of 8×8 Matrix 38
Table 22. Conditions for Fourteenth Column of 8×8 Matrix 39
Table 23. Conditions for Fifteenth Column of 8×8 Matrix 39
Table 24. Conditions for Sixteenth Column of 8×8 Matrix 40

Background

The current System 2 digital interface document [Ref. 1] specifies how 48 messages[1], each message containing a 16-bit word, are used to send a 48-event Unique Signal[2] sequence from an aircraft. The sequence will be interpreted in Sandia National Laboratories implementations as two 24-event Unique Signals. The least-significant bit of each event-word is used to determine the bi-valued event type [Ref. 2]. The System 2 document also specifies how a 48-bit status response is to be structured in three 16-bit words that are part of a weapon status response message from the weapon to the aircraft. In deriving the status response for the original System 2 specification, the protocol was designed to consist of two 24-bit responses, each contained in two 16-bit words. A change was introduced in Ref. 1 to prescribe a more efficient single three-word 48-bit response, but this caused no safety concern. The 48-bit status response is defined for two situations: "Pre-Arm" (correct 48 events received and in weapon memory), and "Safe" (safe pattern contained in weapon memory). The basis for all of the Unique Signal bit specifications was the information contained in the Unique Signal Design Guide DG10276/A, "Implementation of Unique Signal and Related Components" [Ref. 3], which gives the pertinent Unique Signal patterns, safe patterns, and one-way transform[3] characteristics.

A Level-One (acceptable robustness) one-way transform was first implemented in the mid-to-late 1970s using a 6×6 nonsingular matrix over GF(2) (Galois field of two symbols, 0 and 1, using multiplication and exclusive-or addition for basic operations) [Ref. 4]. The matrix computation was "chained" (first matrix computation added to an initialization vector, and subsequent computations added to the previous result). The reason for the GF(2) math structure was that these operations were directly available in the microprocessors that were then entering weapon system use. The most significant reasons for the 6×6 matrix size were that six divided the 24-event pattern length targeted for future Unique Signal patterns, and that six differed from the eight-bit word length used in the contemporary microprocessors.[4] The reason for nonsingularity was to assure a "one-to-one and onto" [Ref. 5] transformation so that each possible input pattern would correspond to an output pattern that differed from all other output patterns. The main reason for chaining was to prevent an all-zero input from generating an all-zero output.

In the late 1980s, improvements in the one-way characteristics of the Level-One transform were considered, and a new Level-Two (no known inadvertent inversion bypasses) 6×6 transform was designed [Ref. 6]. The implementation was designed so

---

[1] System 2 messages contain a message-specific number of 16-bit words. For the Unique Signal event aircraft-generated messages, there is one word per message.

[2] Unique Signals are used to provide unambiguous intent to use a weapon, in a manner consistent with abnormal-environment protection.

[3] A "one-way" transform is intended to be straightforward to compute, but very difficult (difficulty equivalent to exhaustive try) to accidentally invert, even in any abnormal-environment situation.

[4] This choice was also intended to discourage "packing" eight Unique Signal events into a single processor word, which would have been contrary to separate-event communication. Separate-event communication is a key safety principle as specified in DG10276/A.

that the input sequence could be processed one event at a time[5]. This new Level-Two transform was the basis for the status response defined in the first System 2 specification and also that defined in the current System 2 specification. Since the Level-Two transform robustness was well established, no attempt was made to implement other types of transforms or other matrix dimensions, although a Level-Three (optimum robustness) transform was then under development [Ref. 7].[6]

There are two main reasons for carrying out an investigation of other matrix dimensions. First, since larger processor word sizes are now available (e.g., 64 bits), it is appropriate to question whether or not larger matrix sizes could be used to better match contemporary processors. A second reason is that finding additional implementation candidates helps reveal whether there might be previously undiscovered weaknesses in the one-way robustness because of inversion by matrices that have other dimensions than that used in the implemented transformation. These factors are the motivation for this report.

Transform Constraints

There are four pairs of 24-bit input/output streams that must be matched for compliance with the current System 2 specification. Two of the four pairs represent Unique Signal inputs and their "Pre-Arm" transforms; the other two pairs represent the safe patterns and their "Safe" transforms. Since the latter two pairs are identical, three pairs of 24-bit input/output streams are sufficient to define the bit pattern constraints. The three pairs are shown in the following table.

Table 1. Bit-Pattern Constraints for One-Way Transform

Inputs	Outputs
1,0,0,0,0,1,1,1,0,1,1,1,0,0,1,1,0,0,0,1,0,1,1,0	111101010000011101111001
0,1,1,1,1,0,1,1,0,1,0,0,0,0,1,0,1,1,1,0,0,1,0,0	100100100001111101100011
110110110110110110110110	110111110100110111110100

The commas separating Unique Signal input events are to denote that events must be communicated separately and processed separately in the one-way transformation computation in order to maintain abnormal-environment safety.

Constraints imposed for the investigation described in this report are that the transforms must be $n \times n$ nonsingular[7] chained matrix transformations, where n evenly divides 24,[8] and where all three of the input/output pairs in the above table can be produced. The

[5] The Level-One transform was implemented to transform six events at a time to meet efficiency constraints, even though it was recognized that it could have been implemented to transform one event at a time.

[6] The Level-Three transform was documented and patented, but has never been implemented in any weapon system.

[7] An $n \times n$ nonsingular matrix is said to have "rank" n. Rank and dimension are synonymous in this report.

[8] Also considered (in the Appendix) are the dimensions 16 and 48, which evenly divide 48 but not 24.

matrix constraint is imposed for practicality to obviate (in this report) consideration of the potentially infinite set of all possible transformation methods. The following mathematical descriptions and proofs are based on matrix representations, which in turn can lead to multiple equations for multiple "unknowns" (matrix entries).

2×2 Matrix

Consider the transformation of the first input pair in the first row of Table 1 (Eq. 1).

$$[10]\begin{bmatrix} m_{11}m_{12} \\ m_{21}m_{22} \end{bmatrix} = [11] + [i_1 i_2] \tag{1}$$

The symbol "+" is for exclusive-or GF(2) addition[9]. The last vector is the initialization vector. The transformation of the first input pair in the third row of Table 1 is (Eq. 2):

$$[11]\begin{bmatrix} m_{11}m_{12} \\ m_{21}m_{22} \end{bmatrix} = [11] + [i_1 i_2] \tag{2}$$

Since a nonsingular transformation cannot give identical results for different inputs, this is sufficient proof that there is no possible 2×2 nonsingular matrix that will produce the required transformations.

3×3 Matrix

Consider the transformation of the first two trios in the first row, and the first trio in each of the second and third rows of Table 1 (Eq. 3).

$$\begin{aligned}
[100]\begin{bmatrix} m_{11}m_{12}m_{13} \\ m_{21}m_{22}m_{23} \\ m_{31}m_{32}m_{33} \end{bmatrix} &= [111] + [i_1 i_2 i_3] \\
[001]\begin{bmatrix} m_{11}m_{12}m_{13} \\ m_{21}m_{22}m_{23} \\ m_{31}m_{32}m_{33} \end{bmatrix} &= [101] + [111] = [010] \\
[011]\begin{bmatrix} m_{11}m_{12}m_{13} \\ m_{21}m_{22}m_{23} \\ m_{31}m_{32}m_{33} \end{bmatrix} &= [100] + [i_1 i_2 i_3] \\
[110]\begin{bmatrix} m_{11}m_{12}m_{13} \\ m_{21}m_{22}m_{23} \\ m_{31}m_{32}m_{33} \end{bmatrix} &= [110] + [i_1 i_2 i_3]
\end{aligned} \tag{3}$$

[9] The + means $x + x = 0$ (and the sum of all other even number of xs = 0).

The resulting solutions are given in Eq. 4.

$$
\begin{aligned}
&m_{11} + i_1 = m_{12} + i_2 = m_{13} + i_3 = 1 \\
&m_{31} = m_{33} = 0 \\
&m_{32} = 1 \\
&m_{21} + m_{31} + i_1 = 1 \\
&m_{22} + m_{32} + i_2 = m_{23} + m_{33} + i_3 = 0 \\
&m_{11} + m_{21} + i_1 = m_{12} + m_{22} + i_2 = 1 \\
&m_{13} + m_{23} + i_3 = 0
\end{aligned}
\tag{4}
$$

Adding the equations for i_1 in the fourth and sixth rows of Eq. 4 and substituting the zero value for m_{31} from the second row, m_{11} is determined to be zero. Adding the equations for i_2 in the fifth and sixth rows and substituting the unit value for m_{32} from the third row, m_{12} is determined to be zero. Adding the equations for i_3 in the fifth and seventh rows and substituting the zero value for m_{33} from the second row, m_{13} is determined to be zero. Since matrix row one cannot be all zeros because of the nonsingularity restriction, this proves that there is no possible 3×3 matrix that will produce the required transformations.

4×4 Matrix

Consider the transformation of the leading two four-tuples in each of the three rows (the six relations shown in Eqs. 5 and 6).

$$
\begin{aligned}
&[1000]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14} \\ m_{21}m_{22}m_{23}m_{24} \\ m_{31}m_{32}m_{33}m_{34} \\ m_{41}m_{42}m_{43}m_{44} \end{bmatrix} = [1111] + [i_1 i_2 i_3 i_4] \\
&[0111]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14} \\ m_{21}m_{22}m_{23}m_{24} \\ m_{31}m_{32}m_{33}m_{34} \\ m_{41}m_{42}m_{43}m_{44} \end{bmatrix} = [1001] + [i_1 i_2 i_3 i_4] \\
&[1101]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14} \\ m_{21}m_{22}m_{23}m_{24} \\ m_{31}m_{32}m_{33}m_{34} \\ m_{41}m_{42}m_{43}m_{44} \end{bmatrix} = [1101] + [i_1 i_2 i_3 i_4]
\end{aligned}
\tag{5}
$$

$$
\begin{aligned}
[0111]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14} \\ m_{21}m_{22}m_{23}m_{24} \\ m_{31}m_{32}m_{33}m_{34} \\ m_{41}m_{42}m_{43}m_{44} \end{bmatrix} &= [0101]+[1111] \\
[1011]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14} \\ m_{21}m_{22}m_{23}m_{24} \\ m_{31}m_{32}m_{33}m_{34} \\ m_{41}m_{42}m_{43}m_{44} \end{bmatrix} &= [0010]+[1001] \\
[1011]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14} \\ m_{21}m_{22}m_{23}m_{24} \\ m_{31}m_{32}m_{33}m_{34} \\ m_{41}m_{42}m_{43}m_{44} \end{bmatrix} &= [1111]+[1101]
\end{aligned}
\tag{6}
$$

The first and fourth output bits of the second and third transformations in Eq. 6 differ, although the inputs are identical. Since this is not possible for a one-to-one transformation, it proves that there is no possible 4×4 nonsingular matrix that will produce the required transformations.

6×6 Matrix

Since the 6×6 matrix used in the original transform design provides the specified result, it is conclusive that there is at least one 6×6 matrix that will do so. It is informative to find out whether there are any others. The twelve necessary equations are given in Eqs. 7-12.

$$
\begin{aligned}
[100001]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66} \end{bmatrix} &= [111101]+[i_1i_2i_3i_4i_5i_6] \\
[110111]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66} \end{bmatrix} &= [010000]+[111101]
\end{aligned}
\tag{7}
$$

$$[001100]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66} \end{bmatrix} = [011101] + [010000]$$

$$[010110]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66} \end{bmatrix} = [111001] + [011101] \tag{8}$$

$$[011110]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66} \end{bmatrix} = [100100] + [i_1 i_2 i_3 i_4 i_5 i_6]$$

$$[110100]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66} \end{bmatrix} = [100001] + [100100] \tag{9}$$

$$[001011]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66} \end{bmatrix} = [111101] + [100001]$$

$$[100100]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66} \end{bmatrix} = [100011] + [111101] \tag{10}$$

$$[110110]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66} \end{bmatrix} = [110111] + [i_1 i_2 i_3 i_4 i_5 i_6]$$

$$[110110]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66} \end{bmatrix} = [110100] + [110111] \tag{11}$$

$$
\begin{aligned}
[110110]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66} \end{bmatrix} &= [110111]+[110100] \\
[110110]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66} \end{bmatrix} &= [110100]+[110111]
\end{aligned}
\tag{12}
$$

Since the last three matrix equations are identical, only the first 10 equations need be used for the solution. These 10 matrix equations lead to 60 equations for the 36 matrix constituents and the six initialization vector entries (60 equations containing 42 unknowns). The process used will be to describe each of six column solution families of 10 equations individually in a matrix structure shown in the following tables. The solution for the individual values can be depicted through a row-reduction process to isolate individual matrix entry solutions for each of the six matrices shown below.

<u>Matrix One for Column One</u>

Table 2. Conditions for First Column of 6×6 Matrix

m_{11}	m_{21}	m_{31}	m_{41}	m_{51}	m_{61}	i_1	bit 1
1	0	0	0	0	1	1	1
1	1	0	1	1	1	0	1
0	0	1	1	0	0	0	0
0	1	0	1	1	0	0	1
0	1	1	1	1	0	1	1
1	1	0	1	0	0	0	0
0	0	1	0	1	1	0	0
1	0	0	1	0	0	0	0
1	1	0	1	1	0	1	1
1	1	0	1	1	0	0	0

A row reduction:

m_{11}	m_{21}	m_{31}	m_{41}	m_{51}	m_{61}	i_1	bit 1
1	0	0	0	0	0	0	1
0	1	0	0	0	0	0	0

0	0	1	0	0	0	0	1
0	0	0	0	0	0	1	1
0	0	0	1	0	0	0	1
0	0	0	0	1	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	1
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

The only possible solution is that $i_1 = 1$, $m_{11} = 1$, $m_{21} = 0$, $m_{31} = 1$, $m_{41} = 1$, $m_{51} = 0$, and $m_{61} = 1$.

<u>Matrix Two for Column Two</u>

Table 3. Conditions for Second Column of 6×6 Matrix

m_{12}	m_{22}	m_{32}	m_{42}	m_{52}	m_{62}	i_2	bit 2
1	0	0	0	0	1	1	1
1	1	0	1	1	1	0	0
0	0	1	1	0	0	0	0
0	1	0	1	1	0	0	0
0	1	1	1	1	0	1	0
1	1	0	1	0	0	0	0
0	0	1	0	1	1	0	1
1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	1
1	1	0	1	1	0	0	0

A row reduction:

m_{12}	m_{22}	m_{32}	m_{42}	m_{52}	m_{62}	i_2	bit 2
1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	1
0	0	1	0	0	0	0	1
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	0	0	1	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	1

The only possible solution is that $i_2 = 1$, $m_{12} = 0$, $m_{22} = 1$, $m_{32} = 1$, $m_{42} = 1$, $m_{52} = 0$, and $m_{62} = 0$.

Matrix Three for Column Three

Table 4. Conditions for Third Column of 6×6 Matrix

m_{13}	m_{23}	m_{33}	m_{43}	m_{53}	m_{63}	i_3	bit 3
1	0	0	0	0	1	1	1
1	1	0	1	1	1	0	1
0	0	1	1	0	0	0	1
0	1	0	1	1	0	0	0
0	1	1	1	1	0	1	0
1	1	0	1	0	0	0	0
0	0	1	0	1	1	0	1
1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	0
1	1	0	1	1	0	0	0

A row reduction:

m_{13}	m_{23}	m_{33}	m_{43}	m_{53}	m_{63}	i_3	bit 3
1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	1
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	1
0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0

The only possible solution is that $i_3 = 0$, $m_{13} = 0$, $m_{23} = 1$, $m_{33} = 0$, $m_{43} = 1$, $m_{53} = 0$, and $m_{63} = 1$.

Matrix Four for Column Four

Table 5. Conditions for Fourth Column of 6×6 Matrix

m_{14}	m_{24}	m_{34}	m_{44}	m_{54}	m_{64}	i_4	bit 4
1	0	0	0	0	1	1	1
1	1	0	1	1	1	0	1
0	0	1	1	0	0	0	1
0	1	0	1	1	0	0	1
0	1	1	1	1	0	1	1

1	1	0	1	0	0	0	1
0	0	1	0	1	1	0	1
1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	1
1	1	0	1	1	0	0	0

A row reduction:

m_{14}	m_{24}	m_{34}	m_{44}	m_{54}	m_{64}	i_4	bit 4
1	0	0	0	0	0	0	1
0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	1
0	0	0	0	0	0	1	1
0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	1
0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	1
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

The only possible solution is that $i_4 = 1$, $m_{14} = 1$, $m_{24} = 0$, $m_{34} = 1$, $m_{44} = 0$, $m_{54} = 1$, and $m_{64} = 1$.

<u>Matrix Five for Column Five</u>

Table 6. Conditions for Fifth Column of 6×6 Matrix

m_{15}	m_{25}	m_{35}	m_{45}	m_{55}	m_{65}	i_5	bit 5
1	0	0	0	0	1	1	0
1	1	0	1	1	1	0	0
0	0	1	1	0	0	0	0
0	1	0	1	1	0	0	0
0	1	1	1	1	0	1	0
1	1	0	1	0	0	0	0
0	0	1	0	1	1	0	0
1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	1
1	1	0	1	1	0	0	1

A row reduction:

m_{15}	m_{25}	m_{35}	m_{45}	m_{55}	m_{65}	i_5	bit 5
1	0	0	0	0	0	0	1
0	1	0	0	0	0	0	1
0	0	1	0	0	0	0	0

0	0	0	0	0	0	1	0
0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	1
0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	1
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

The only possible solution is that $i_5 = 0$, $m_{15} = 1$, $m_{25} = 1$, $m_{35} = 0$, $m_{45} = 0$, $m_{55} = 1$, and $m_{65} = 1$.

<u>Matrix Six for Column Six</u>

Table 7. Conditions for Sixth Column of 6×6 Matrix

m_{16}	m_{26}	m_{36}	m_{46}	m_{56}	m_{66}	i_6	bit 6
1	0	0	0	0	1	1	1
1	1	0	1	1	1	0	1
0	0	1	1	0	0	0	1
0	1	0	1	1	0	0	0
0	1	1	1	1	0	1	0
1	1	0	1	0	0	0	1
0	0	1	0	1	1	0	0
1	0	0	1	0	0	0	0
1	1	0	1	1	0	1	1
1	1	0	1	1	0	0	1

A row reduction:

m_{16}	m_{26}	m_{36}	m_{46}	m_{56}	m_{66}	i_6	bit 6
1	0	0	0	0	0	0	1
0	1	0	0	0	0	0	1
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0

The only possible solution is that $i_6 = 0$, $m_{16} = 1$, $m_{26} = 1$, $m_{36} = 0$, $m_{46} = 1$, $m_{56} = 0$, and $m_{66} = 0$.

In conclusion for the 6×6 matrix size, the exact initialization vector and matrix now used in the Level-Two one-way transformation are the only solution possible for a chained 6×6 nonsingular matrix that will give the required input/output sequence pairs. This matrix, its inverse, and the initialization vector are:

$$M_6 = \begin{bmatrix} 100111 \\ 011011 \\ 110100 \\ 111001 \\ 000110 \\ 101110 \end{bmatrix} \quad M_6^{-1} = \begin{bmatrix} 111011 \\ 011110 \\ 111000 \\ 101101 \\ 101111 \\ 011001 \end{bmatrix} \quad i = 110100 \tag{13}$$

One way to compute the matrix multiplication one event at a time is shown in Ref. 3.

8×8 Matrix

The matrix equations for transforming the three eight-tuples for each of the three sequences are given in Eqs. 14 through 22.

$$[10000111]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68} \\ m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78} \\ m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88} \end{bmatrix} = [11110101] + [i_1 i_2 i_3 i_4 i_5 i_6 i_7 i_8] \tag{14}$$

$$[01111011]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68} \\ m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78} \\ m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88} \end{bmatrix} = [10010010] + [i_1 i_2 i_3 i_4 i_5 i_6 i_7 i_8] \tag{15}$$

$$[11011011]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68} \\ m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78} \\ m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88} \end{bmatrix} = [11011111] + [i_1 i_2 i_3 i_4 i_5 i_6 i_7 i_8] \qquad (16)$$

$$[01110011]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68} \\ m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78} \\ m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88} \end{bmatrix} = [00000111] + [11110101] \qquad (17)$$

$$[01000010]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68} \\ m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78} \\ m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88} \end{bmatrix} = [00011111] + [10010010] \qquad (18)$$

$$[01101101]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68} \\ m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78} \\ m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88} \end{bmatrix} = [01001101] + [11011111] \qquad (19)$$

$$[00010110]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68} \\ m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78} \\ m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88} \end{bmatrix} = [01111001] + [00000111] \tag{20}$$

$$[11100100]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68} \\ m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78} \\ m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88} \end{bmatrix} = [01100011] + [00011111] \tag{21}$$

$$[10110110]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68} \\ m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78} \\ m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88} \end{bmatrix} = [11110100] + [01001101] \tag{22}$$

<u>Matrix One for Column One</u>

Table 8. Conditions for First Column of 8×8 Matrix

m_{11}	m_{21}	m_{31}	m_{41}	m_{51}	m_{61}	m_{71}	m_{81}	i_1	Bit 1
1	0	0	0	0	1	1	1	1	1
0	1	1	1	1	0	1	1	1	1
1	1	0	1	1	0	1	1	1	1
0	1	1	1	0	0	1	1	0	1

0	1	0	0	0	0	1	0	0	1
0	1	1	0	1	1	0	1	0	1
0	0	0	1	0	1	1	0	0	0
1	1	1	0	0	1	0	0	0	0
1	0	1	1	0	1	1	0	0	1

A row-reduced matrix:

m_{11}	m_{21}	m_{31}	m_{41}	m_{51}	m_{61}	m_{71}	m_{81}	i_1	Bit 1
1	0	0	0	0	0	0	1	0	1
0	1	0	0	0	0	1	0	0	1
0	0	1	0	0	0	0	1	0	1
0	0	0	0	1	0	0	0	0	1
0	0	0	1	0	0	0	0	0	1
0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0	1	1
0	0	0	0	0	1	1	0	0	1
0	0	0	0	0	0	0	0	0	1

The sixth and ninth rows of the row-reduced matrix could only be satisfied if 0 = 1, so this proves that there is no possible 8×8 matrix that will produce the required transformations. Since the connection between this row-reduction proof and the corresponding equations may not be as clear as in the preceding examples, an equation proof is given below. The sum of the equations represented by the first, third, fourth, fifth, and sixth rows of the original "matrix one for column one" is:

$$\begin{aligned}
&m_{11} + m_{61} + m_{71} + m_{81} + i_1 = 1 \\
&+ m_{11} + m_{21} + m_{41} + m_{51} + m_{71} + m_{81} + i_1 = 1 \\
&+ m_{21} + m_{31} + m_{41} + m_{71} + m_{81} = 1 \\
&+ m_{21} + m_{71} = 1 \\
&+ m_{21} + m_{31} + m_{51} + m_{61} + m_{81} = 1
\end{aligned} \tag{23}$$

which sums to: 0 = 1, thereby verifying the conclusion derived from the row reduction matrix.

12×12 Matrix

A 12×12 matrix solution might be presumed likely, since a 6×6 matrix is known to be possible and since six divides 12. However, two problematic constraints can be seen from the properties of the third row in Table 1. If the transformation is expressed as:

$$y = x[M] + i \tag{24}$$

where x is a 12-bit input vector, M is a 12×12 transformation matrix, and i represents both the initialization vector for the first 12 bits and the previous output vector for the second 12 bits. This leads to two results (transformation of first 12 bits and transformation of second 12 bits) for the third row of Table 1:

$$\begin{aligned} y_1 &= x_1[M] + i = 110111110100 \\ y_2 &= x_2[M] + y_1 = 110111110100 \end{aligned} \tag{25}$$

Since $y_1 = y_2$ and $x_1 = x_2$, then it is necessary that $i = y_1$. In other words, there is no more than one initialization vector that can be used for a 12×12 transformation that will satisfy the constraints given in Table 1, and if such a chained transformation exists, it must use the initialization vector 110111110100. Also, since $y_1 = y_2$ and $i = y_1$, then $x_1[M] = x_2[M] = 0$. The only way to assure this for a nonsingular matrix M is if x_1 and x_2 are zero vectors, which is not the case for the inputs in Table 1. This proves that there is no 12×12 matrix that will meet the requirements.

24×24 Matrix

There is a somewhat obvious solution for a 24×24 matrix that meets the specifications. A 24×24 matrix can be obtained recursively from ten 6×6 matrices. The reason that this can be done with a dimension that six divides while it could not be done with a 12×12 matrix is related to the chaining. Since the 6×6 chaining uses values derived from previous 6×6 matrices (excepting the initialization vector), and since these values were generated by previous inputs, the 24 inputs can be grouped into four sections, each processed by 6×6 matrix multiplication. This approach is appropriate for a single 24×24 matrix multiplication, but cannot be successful for matrices (e.g., 12×12) that have to be recursively chained. In addition, the approach gives an existence proof, but does not exhaust other possible 24×24 matrices that might also meet the conditions of Table 1. The 24×24 initialization vector is four replications of the 6×6 initialization vector, mathematically expressed as $2^{18}\, i + 2^{12}\, i + 2^{6}\, i + i$. The construction is shown in Eq. 26.

$$\begin{aligned} M_{24} &= \begin{bmatrix} M_6 M_6 M_6 M_6 \\ M_0 M_6 M_6 M_6 \\ M_0 M_0 M_6 M_6 \\ M_0 M_0 M_0 M_6 \end{bmatrix} \\ M_{24}^{-1} &= \begin{bmatrix} M_6^{-1} M_6^{-1} M_0 M_0 \\ M_0 M_6^{-1} M_6^{-1} M_0 \\ M_0 M_0 M_6^{-1} M_6^{-1} \\ M_0 M_0 M_0 M_6^{-1} \end{bmatrix} \end{aligned} \tag{26}$$

Here, M_{24} and M_{24}^{-1} are the 24×24 one-way transformation matrix and its inverse, M_6 and M_6^{-1} are the 6×6 one-way transformation matrix and its inverse, and M_0 is an all-zero 6×6 matrix. For example, the first row of Table 1 is computed as:

$$
\begin{aligned}
y = 100001110111001100010110 & \begin{bmatrix}
100111100111100111100111 \\
011011011011011011011011 \\
110100110100110100110100 \\
111001111001111001111001 \\
000110000110000110000110 \\
101110101110101110101110 \\
000000100111100111100111 \\
000000011011011011011011 \\
000000110100110100110100 \\
000000111001111001111001 \\
000000000110000110000110 \\
000000101110101110101110 \\
000000000000100111100111 \\
000000000000011011011011 \\
000000000000110100110100 \\
000000000000111001111001 \\
000000000000000110000110 \\
000000000000101110101110 \\
000000000000000000100111 \\
000000000000000000011011 \\
000000000000000000110100 \\
000000000000000000111001 \\
000000000000000000000110 \\
000000000000000000101110
\end{bmatrix} \\
+ 110100110100110100110100 = 111101010000011101111001 &
\end{aligned}
\tag{27}
$$

Although the existence of this 24×24 matrix shows that the Level-Two one-way transform can be inverted in a different manner than previously known (by applying M_{24}^{-1}) there are no obvious weaknesses related to this discovery. The 24×24 inversion process requires approximately ten times as much information as required to invert the 6×6 matrix, and this information would be subject to the same restrictions against intentional storage as those for the Unique Signal patterns. For this reason, matrix dimensions significantly higher than six are not of significant interest as threats for inadvertent inversion. However, since there are numerous 24×24 matrices that meet the

requirements, some of these have been examined for inversion weaknesses and this investigation will continue as resources allow. An example of an inversion matrix found that is less complex than that indicated by Eq. 26 is shown below in Eq. 28.

$$(output + 010100110100110100110100) \times \begin{bmatrix} 110101110110110101110110 \\ 101011010111110111000101 \\ 010101100101010000101101 \\ 000100000000000000000000 \\ 000010000000000000000000 \\ 000001000000000000000000 \\ 000000100000000000000000 \\ 000000010000000000000000 \\ 000000001000000000000000 \\ 000000000100000000000000 \\ 000000000010000000000000 \\ 000000000001000000000000 \\ 000000000000100000000000 \\ 000000000000010000000000 \\ 000000000000001000000000 \\ 000000000000000100000000 \\ 000000000000000010000000 \\ 000000000000000001000000 \\ 000000000000000000100000 \\ 000000000000000000010000 \\ 000000000000000000001000 \\ 000000000000000000000100 \\ 000000000000000000000010 \\ 000000000000000000000001 \end{bmatrix} = input \tag{28}$$

Although of relatively low complexity, accidental construction of this matrix and initialization vector does not appear to be trivial.

Conclusions

The stated intent was met, where all possible nonsingular chained one-way transformation dimensions that meet the System 2 requirements and divide 24 were investigated. The mathematical results proved that there is only one possible additional transformation dimension (other than the 6×6 Level-Two transform currently in use) under the stated constraints, where the matrix dimension is 24 or a divisor of 24. That

matrix size is 24×24. Furthermore, the existing 6×6 transformation was proved to be the only dimension-six solution possible that meets the constraints. It is noteworthy that new solutions for 24×24 matrices that give equivalent results to the existing 6×6 transformation matrix were derived. Dimensions that divide 48 are of less practical interest, but these were also investigated, and the results are provided in Appendix A. Here, there were 48×48 matrices found that met the required conditions, and they are indicated in Appendix A. Included in Appendix B are some inversion matrices that can be used to derive Unique Signal patterns from pre-arm information without meeting the constraints of safe information. This part of the investigation will continue. However, no inversion weaknesses or concerns have been revealed through this work.

Appendix A: Matrix Dimensions that Divide 48

In this appendix, the dimensions 16 and 48, which divide 48, but not 24, are addressed.

16×16 Matrix

The six matrix equations for transforming the three 16-tuples for each of the two 48-bit sequences[10] indicated by Table 1 are:

$$[1000011101110011]\begin{bmatrix}
m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18}m_{19}m_{1,10}m_{1,11}m_{1,12}m_{1,13}m_{1,14}m_{1,15}m_{1,16} \\
m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28}m_{29}m_{2,10}m_{2,11}m_{2,12}m_{2,13}m_{2,14}m_{2,15}m_{2,16} \\
m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38}m_{39}m_{3,10}m_{3,11}m_{3,12}m_{3,13}m_{3,14}m_{3,15}m_{3,16} \\
m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48}m_{49}m_{4,10}m_{4,11}m_{4,12}m_{4,13}m_{4,14}m_{4,15}m_{4,16} \\
m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58}m_{59}m_{5,10}m_{5,11}m_{5,12}m_{5,13}m_{5,14}m_{5,15}m_{5,16} \\
m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68}m_{69}m_{6,10}m_{6,11}m_{6,12}m_{6,13}m_{6,14}m_{6,15}m_{6,16} \\
m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78}m_{79}m_{7,10}m_{7,11}m_{7,12}m_{7,13}m_{7,14}m_{7,15}m_{7,16} \\
m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88}m_{89}m_{8,10}m_{8,11}m_{8,12}m_{8,13}m_{8,14}m_{8,15}m_{8,16} \\
m_{91}m_{92}m_{93}m_{94}m_{95}m_{96}m_{97}m_{98}m_{99}m_{9,10}m_{9,11}m_{9,12}m_{9,13}m_{9,14}m_{9,15}m_{9,16} \\
m_{10,1}m_{10,2}m_{10,3}m_{10,4}m_{10,5}m_{10,6}m_{10,7}m_{10,8}m_{10,9}m_{10,10}m_{10,11}m_{10,12}m_{10,13}m_{10,14}m_{10,15}m_{10,16} \\
m_{11,1}m_{11,2}m_{11,3}m_{11,4}m_{11,5}m_{11,6}m_{11,7}m_{11,8}m_{11,9}m_{11,10}m_{11,11}m_{11,12}m_{11,13}m_{11,14}m_{11,15}m_{11,16} \\
m_{12,1}m_{12,2}m_{12.3}m_{12,4}m_{12,5}m_{12,6}m_{12,7}m_{12,8}m_{12,9}m_{12,10}m_{12,11}m_{12,12}m_{12,13}m_{12,14}m_{12,15}m_{12,16} \\
m_{13,1}m_{13,2}m_{13,3}m_{13.4}m_{13,5}m_{13,6}m_{13,7}m_{13,8}m_{13,9}m_{13,10}m_{13,11}m_{13,12}m_{13,13}m_{13,14}m_{13,15}m_{13,16} \\
m_{14,1}m_{14,2}m_{14,3}m_{14,4}m_{14,5}m_{14,6}m_{14,7}m_{14,8}m_{14,9}m_{14,10}m_{14,11}m_{14,12}m_{14,13}m_{14,14}m_{14,15}m_{14,16} \\
m_{15,1}m_{15,2}m_{15,3}m_{15,4}m_{15,5}m_{15,6}m_{15,7}m_{15,8}m_{15,9}m_{15,10}m_{15,11}m_{15,12}m_{15,13}m_{15,14}m_{15,15}m_{15,16} \\
m_{16,1}m_{16,2}m_{16,3}m_{16,4}m_{16,5}m_{16,6}m_{16,7}m_{16,8}m_{16,9}m_{16,10}m_{16,11}m_{16,12}m_{16,13}m_{16,14}m_{16,15}m_{16,16}
\end{bmatrix}$$

$$= [1111010100000111] + [i_1 i_2 i_3 i_4 i_5 i_6 i_7 i_8 i_9 i_{10} i_{11} i_{12} i_{13} i_{14} i_{15} i_{16}]$$

[10] For denoting 48-bit processing, the third row of Table 1 must be repeated.

$$
[0001011001111011]\begin{bmatrix}
m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18}m_{19}m_{1,10}m_{1,11}m_{1,12}m_{1,13}m_{1,14}m_{1,15}m_{1,16} \\
m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28}m_{29}m_{2,10}m_{2,11}m_{2,12}m_{2,13}m_{2,14}m_{2,15}m_{2,16} \\
m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38}m_{39}m_{3,10}m_{3,11}m_{3,12}m_{3,13}m_{3,14}m_{3,15}m_{3,16} \\
m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48}m_{49}m_{4,10}m_{4,11}m_{4,12}m_{4,13}m_{4,14}m_{4,15}m_{4,16} \\
m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58}m_{59}m_{5,10}m_{5,11}m_{5,12}m_{5,13}m_{5,14}m_{5,15}m_{5,16} \\
m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68}m_{69}m_{6,10}m_{6,11}m_{6,12}m_{6,13}m_{6,14}m_{6,15}m_{6,16} \\
m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78}m_{79}m_{7,10}m_{7,11}m_{7,12}m_{7,13}m_{7,14}m_{7,15}m_{7,16} \\
m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88}m_{89}m_{8,10}m_{8,11}m_{8,12}m_{8,13}m_{8,14}m_{8,15}m_{8,16} \\
m_{91}m_{92}m_{93}m_{94}m_{95}m_{96}m_{97}m_{98}m_{99}m_{9,10}m_{9,11}m_{9,12}m_{9,13}m_{9,14}m_{9,15}m_{9,16} \\
m_{10,1}m_{10,2}m_{10,3}m_{10,4}m_{10,5}m_{10,6}m_{10,7}m_{10,8}m_{10,9}m_{10,10}m_{10,11}m_{10,12}m_{10,13}m_{10,14}m_{10,15}m_{10,16} \\
m_{11,1}m_{11,2}m_{11,3}m_{11,4}m_{11,5}m_{11,6}m_{11,7}m_{11,8}m_{11,9}m_{11,10}m_{11,11}m_{11,12}m_{11,13}m_{11,14}m_{11,15}m_{11,16} \\
m_{12,1}m_{12,2}m_{12.3}m_{12,4}m_{12,5}m_{12,6}m_{12,7}m_{12,8}m_{12,9}m_{12,10}m_{12,11}m_{12,12}m_{12,13}m_{12,14}m_{12,15}m_{12,16} \\
m_{13,1}m_{13,2}m_{13,3}m_{13.4}m_{13,5}m_{13,6}m_{13,7}m_{13,8}m_{13,9}m_{13,10}m_{13,11}m_{13,12}m_{13,13}m_{13,14}m_{13,15}m_{13,16} \\
m_{14,1}m_{14,2}m_{14,3}m_{14,4}m_{14,5}m_{14,6}m_{14,7}m_{14,8}m_{14,9}m_{14,10}m_{14,11}m_{14,12}m_{14,13}m_{14,14}m_{14,15}m_{14,16} \\
m_{15,1}m_{15,2}m_{15,3}m_{15,4}m_{15,5}m_{15,6}m_{15,7}m_{15,8}m_{15,9}m_{15,10}m_{15,11}m_{15,12}m_{15,13}m_{15,14}m_{15,15}m_{15,16} \\
m_{16,1}m_{16,2}m_{16,3}m_{16,4}m_{16,5}m_{16,6}m_{16,7}m_{16,8}m_{16,9}m_{16,10}m_{16,11}m_{16,12}m_{16,13}m_{16,14}m_{16,15}m_{16,16}
\end{bmatrix}
$$

$$
=[0111100110010010]+[1111010100000111]
$$

$$
[0100001011100100]\begin{bmatrix}
m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18}m_{19}m_{1,10}m_{1,11}m_{1,12}m_{1,13}m_{1,14}m_{1,15}m_{1,16} \\
m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28}m_{29}m_{2,10}m_{2,11}m_{2,12}m_{2,13}m_{2,14}m_{2,15}m_{2,16} \\
m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38}m_{39}m_{3,10}m_{3,11}m_{3,12}m_{3,13}m_{3,14}m_{3,15}m_{3,16} \\
m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48}m_{49}m_{4,10}m_{4,11}m_{4,12}m_{4,13}m_{4,14}m_{4,15}m_{4,16} \\
m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58}m_{59}m_{5,10}m_{5,11}m_{5,12}m_{5,13}m_{5,14}m_{5,15}m_{5,16} \\
m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68}m_{69}m_{6,10}m_{6,11}m_{6,12}m_{6,13}m_{6,14}m_{6,15}m_{6,16} \\
m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78}m_{79}m_{7,10}m_{7,11}m_{7,12}m_{7,13}m_{7,14}m_{7,15}m_{7,16} \\
m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88}m_{89}m_{8,10}m_{8,11}m_{8,12}m_{8,13}m_{8,14}m_{8,15}m_{8,16} \\
m_{91}m_{92}m_{93}m_{94}m_{95}m_{96}m_{97}m_{98}m_{99}m_{9,10}m_{9,11}m_{9,12}m_{9,13}m_{9,14}m_{9,15}m_{9,16} \\
m_{10,1}m_{10,2}m_{10,3}m_{10,4}m_{10,5}m_{10,6}m_{10,7}m_{10,8}m_{10,9}m_{10,10}m_{10,11}m_{10,12}m_{10,13}m_{10,14}m_{10,15}m_{10,16} \\
m_{11,1}m_{11,2}m_{11,3}m_{11,4}m_{11,5}m_{11,6}m_{11,7}m_{11,8}m_{11,9}m_{11,10}m_{11,11}m_{11,12}m_{11,13}m_{11,14}m_{11,15}m_{11,16} \\
m_{12,1}m_{12,2}m_{12.3}m_{12,4}m_{12,5}m_{12,6}m_{12,7}m_{12,8}m_{12,9}m_{12,10}m_{12,11}m_{12,12}m_{12,13}m_{12,14}m_{12,15}m_{12,16} \\
m_{13,1}m_{13,2}m_{13,3}m_{13.4}m_{13,5}m_{13,6}m_{13,7}m_{13,8}m_{13,9}m_{13,10}m_{13,11}m_{13,12}m_{13,13}m_{13,14}m_{13,15}m_{13,16} \\
m_{14,1}m_{14,2}m_{14,3}m_{14,4}m_{14,5}m_{14,6}m_{14,7}m_{14,8}m_{14,9}m_{14,10}m_{14,11}m_{14,12}m_{14,13}m_{14,14}m_{14,15}m_{14,16} \\
m_{15,1}m_{15,2}m_{15,3}m_{15,4}m_{15,5}m_{15,6}m_{15,7}m_{15,8}m_{15,9}m_{15,10}m_{15,11}m_{15,12}m_{15,13}m_{15,14}m_{15,15}m_{15,16} \\
m_{16,1}m_{16,2}m_{16,3}m_{16,4}m_{16,5}m_{16,6}m_{16,7}m_{16,8}m_{16,9}m_{16,10}m_{16,11}m_{16,12}m_{16,13}m_{16,14}m_{16,15}m_{16,16}
\end{bmatrix}
$$

$$
=[0001111101100011]+[0111100110010010]
$$

$$
[1101101101101101]\begin{bmatrix}
m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18}m_{19}m_{1,10}m_{1,11}m_{1,12}m_{1,13}m_{1,14}m_{1,15}m_{1,16} \\
m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28}m_{29}m_{2,10}m_{2,11}m_{2,12}m_{2,13}m_{2,14}m_{2,15}m_{2,16} \\
m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38}m_{39}m_{3,10}m_{3,11}m_{3,12}m_{3,13}m_{3,14}m_{3,15}m_{3,16} \\
m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48}m_{49}m_{4,10}m_{4,11}m_{4,12}m_{4,13}m_{4,14}m_{4,15}m_{4,16} \\
m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58}m_{59}m_{5,10}m_{5,11}m_{5,12}m_{5,13}m_{5,14}m_{5,15}m_{5,16} \\
m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68}m_{69}m_{6,10}m_{6,11}m_{6,12}m_{6,13}m_{6,14}m_{6,15}m_{6,16} \\
m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78}m_{79}m_{7,10}m_{7,11}m_{7,12}m_{7,13}m_{7,14}m_{7,15}m_{7,16} \\
m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88}m_{89}m_{8,10}m_{8,11}m_{8,12}m_{8,13}m_{8,14}m_{8,15}m_{8,16} \\
m_{91}m_{92}m_{93}m_{94}m_{95}m_{96}m_{97}m_{98}m_{99}m_{9,10}m_{9,11}m_{9,12}m_{9,13}m_{9,14}m_{9,15}m_{9,16} \\
m_{10,1}m_{10,2}m_{10,3}m_{10,4}m_{10,5}m_{10,6}m_{10,7}m_{10,8}m_{10,9}m_{10,10}m_{10,11}m_{10,12}m_{10,13}m_{10,14}m_{10,15}m_{10,16} \\
m_{11,1}m_{11,2}m_{11,3}m_{11,4}m_{11,5}m_{11,6}m_{11,7}m_{11,8}m_{11,9}m_{11,10}m_{11,11}m_{11,12}m_{11,13}m_{11,14}m_{11,15}m_{11,16} \\
m_{12,1}m_{12,2}m_{12.3}m_{12,4}m_{12,5}m_{12,6}m_{12,7}m_{12,8}m_{12,9}m_{12,10}m_{12,11}m_{12,12}m_{12,13}m_{12,14}m_{12,15}m_{12,16} \\
m_{13,1}m_{13,2}m_{13,3}m_{13.4}m_{13,5}m_{13,6}m_{13,7}m_{13,8}m_{13,9}m_{13,10}m_{13,11}m_{13,12}m_{13,13}m_{13,14}m_{13,15}m_{13,16} \\
m_{14,1}m_{14,2}m_{14,3}m_{14,4}m_{14,5}m_{14,6}m_{14,7}m_{14,8}m_{14,9}m_{14,10}m_{14,11}m_{14,12}m_{14,13}m_{14,14}m_{14,15}m_{14,16} \\
m_{15,1}m_{15,2}m_{15,3}m_{15,4}m_{15,5}m_{15,6}m_{15,7}m_{15,8}m_{15,9}m_{15,10}m_{15,11}m_{15,12}m_{15,13}m_{15,14}m_{15,15}m_{15,16} \\
m_{16,1}m_{16,2}m_{16,3}m_{16,4}m_{16,5}m_{16,6}m_{16,7}m_{16,8}m_{16,9}m_{16,10}m_{16,11}m_{16,12}m_{16,13}m_{16,14}m_{16,15}m_{16,16}
\end{bmatrix}
$$

$$
=[1101111101001101]+[i_1 i_2 i_3 i_4 i_5 i_6 i_7 i_8 i_9 i_{10} i_{11} i_{12} i_{13} i_{14} i_{15} i_{16}]
$$

$$
[1011011011011011]\begin{bmatrix}
m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18}m_{19}m_{1,10}m_{1,11}m_{1,12}m_{1,13}m_{1,14}m_{1,15}m_{1,16} \\
m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28}m_{29}m_{2,10}m_{2,11}m_{2,12}m_{2,13}m_{2,14}m_{2,15}m_{2,16} \\
m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38}m_{39}m_{3,10}m_{3,11}m_{3,12}m_{3,13}m_{3,14}m_{3,15}m_{3,16} \\
m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48}m_{49}m_{4,10}m_{4,11}m_{4,12}m_{4,13}m_{4,14}m_{4,15}m_{4,16} \\
m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58}m_{59}m_{5,10}m_{5,11}m_{5,12}m_{5,13}m_{5,14}m_{5,15}m_{5,16} \\
m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68}m_{69}m_{6,10}m_{6,11}m_{6,12}m_{6,13}m_{6,14}m_{6,15}m_{6,16} \\
m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78}m_{79}m_{7,10}m_{7,11}m_{7,12}m_{7,13}m_{7,14}m_{7,15}m_{7,16} \\
m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88}m_{89}m_{8,10}m_{8,11}m_{8,12}m_{8,13}m_{8,14}m_{8,15}m_{8,16} \\
m_{91}m_{92}m_{93}m_{94}m_{95}m_{96}m_{97}m_{98}m_{99}m_{9,10}m_{9,11}m_{9,12}m_{9,13}m_{9,14}m_{9,15}m_{9,16} \\
m_{10,1}m_{10,2}m_{10,3}m_{10,4}m_{10,5}m_{10,6}m_{10,7}m_{10,8}m_{10,9}m_{10,10}m_{10,11}m_{10,12}m_{10,13}m_{10,14}m_{10,15}m_{10,16} \\
m_{11,1}m_{11,2}m_{11,3}m_{11,4}m_{11,5}m_{11,6}m_{11,7}m_{11,8}m_{11,9}m_{11,10}m_{11,11}m_{11,12}m_{11,13}m_{11,14}m_{11,15}m_{11,16} \\
m_{12,1}m_{12,2}m_{12.3}m_{12,4}m_{12,5}m_{12,6}m_{12,7}m_{12,8}m_{12,9}m_{12,10}m_{12,11}m_{12,12}m_{12,13}m_{12,14}m_{12,15}m_{12,16} \\
m_{13,1}m_{13,2}m_{13,3}m_{13.4}m_{13,5}m_{13,6}m_{13,7}m_{13,8}m_{13,9}m_{13,10}m_{13,11}m_{13,12}m_{13,13}m_{13,14}m_{13,15}m_{13,16} \\
m_{14,1}m_{14,2}m_{14,3}m_{14,4}m_{14,5}m_{14,6}m_{14,7}m_{14,8}m_{14,9}m_{14,10}m_{14,11}m_{14,12}m_{14,13}m_{14,14}m_{14,15}m_{14,16} \\
m_{15,1}m_{15,2}m_{15,3}m_{15,4}m_{15,5}m_{15,6}m_{15,7}m_{15,8}m_{15,9}m_{15,10}m_{15,11}m_{15,12}m_{15,13}m_{15,14}m_{15,15}m_{15,16} \\
m_{16,1}m_{16,2}m_{16,3}m_{16,4}m_{16,5}m_{16,6}m_{16,7}m_{16,8}m_{16,9}m_{16,10}m_{16,11}m_{16,12}m_{16,13}m_{16,14}m_{16,15}m_{16,16}
\end{bmatrix}
$$

$$
=[1111010011011111]+[1101111101001101]
$$

$$[0110110110110110]\begin{bmatrix} m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}m_{17}m_{18}m_{19}m_{1,10}m_{1,11}m_{1,12}m_{1,13}m_{1,14}m_{1,15}m_{1,16} \\ m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}m_{27}m_{28}m_{29}m_{2,10}m_{2,11}m_{2,12}m_{2,13}m_{2,14}m_{2,15}m_{2,16} \\ m_{31}m_{32}m_{33}m_{34}m_{35}m_{36}m_{37}m_{38}m_{39}m_{3,10}m_{3,11}m_{3,12}m_{3,13}m_{3,14}m_{3,15}m_{3,16} \\ m_{41}m_{42}m_{43}m_{44}m_{45}m_{46}m_{47}m_{48}m_{49}m_{4,10}m_{4,11}m_{4,12}m_{4,13}m_{4,14}m_{4,15}m_{4,16} \\ m_{51}m_{52}m_{53}m_{54}m_{55}m_{56}m_{57}m_{58}m_{59}m_{5,10}m_{5,11}m_{5,12}m_{5,13}m_{5,14}m_{5,15}m_{5,16} \\ m_{61}m_{62}m_{63}m_{64}m_{65}m_{66}m_{67}m_{68}m_{69}m_{6,10}m_{6,11}m_{6,12}m_{6,13}m_{6,14}m_{6,15}m_{6,16} \\ m_{71}m_{72}m_{73}m_{74}m_{75}m_{76}m_{77}m_{78}m_{79}m_{7,10}m_{7,11}m_{7,12}m_{7,13}m_{7,14}m_{7,15}m_{7,16} \\ m_{81}m_{82}m_{83}m_{84}m_{85}m_{86}m_{87}m_{88}m_{89}m_{8,10}m_{8,11}m_{8,12}m_{8,13}m_{8,14}m_{8,15}m_{8,16} \\ m_{91}m_{92}m_{93}m_{94}m_{95}m_{96}m_{97}m_{98}m_{99}m_{9,10}m_{9,11}m_{9,12}m_{9,13}m_{9,14}m_{9,15}m_{9,16} \\ m_{10,1}m_{10,2}m_{10,3}m_{10,4}m_{10,5}m_{10,6}m_{10,7}m_{10,8}m_{10,9}m_{10,10}m_{10,11}m_{10,12}m_{10,13}m_{10,14}m_{10,15}m_{10,16} \\ m_{11,1}m_{11,2}m_{11,3}m_{11,4}m_{11,5}m_{11,6}m_{11,7}m_{11,8}m_{11,9}m_{11,10}m_{11,11}m_{11,12}m_{11,13}m_{11,14}m_{11,15}m_{11,16} \\ m_{12,1}m_{12,2}m_{12.3}m_{12,4}m_{12,5}m_{12,6}m_{12,7}m_{12,8}m_{12,9}m_{12,10}m_{12,11}m_{12,12}m_{12,13}m_{12,14}m_{12,15}m_{12,16} \\ m_{13,1}m_{13,2}m_{13,3}m_{13.4}m_{13,5}m_{13,6}m_{13,7}m_{13,8}m_{13,9}m_{13,10}m_{13,11}m_{13,12}m_{13,13}m_{13,14}m_{13,15}m_{13,16} \\ m_{14,1}m_{14,2}m_{14,3}m_{14,4}m_{14,5}m_{14,6}m_{14,7}m_{14,8}m_{14,9}m_{14,10}m_{14,11}m_{14,12}m_{14,13}m_{14,14}m_{14,15}m_{14,16} \\ m_{15,1}m_{15,2}m_{15,3}m_{15,4}m_{15,5}m_{15,6}m_{15,7}m_{15,8}m_{15,9}m_{15,10}m_{15,11}m_{15,12}m_{15,13}m_{15,14}m_{15,15}m_{15,16} \\ m_{16,1}m_{16,2}m_{16,3}m_{16,4}m_{16,5}m_{16,6}m_{16,7}m_{16,8}m_{16,9}m_{16,10}m_{16,11}m_{16,12}m_{16,13}m_{16,14}m_{16,15}m_{16,16} \end{bmatrix}$$

$$=[0100110111110100]+[1111010011011111]$$

The corresponding matrix representations for the 16 matrix columns are:

<u>Matrix One for Column One</u>

Table 9. Conditions for First Column of 16×16 Matrix

m_{11}	m_{21}	m_{31}	m_{41}	m_{51}	m_{61}	m_{71}	m_{81}	m_{91}	$m_{10,1}$	$m_{11,1}$	$m_{12,1}$	$m_{13,1}$	$m_{14,1}$	$m_{15,1}$	$m_{16,1}$	i_1	bit 1
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1

A row-reduced matrix:

m_{11}	m_{21}	m_{31}	m_{41}	m_{51}	m_{61}	m_{71}	m_{81}	m_{91}	$m_{10,1}$	$m_{11,1}$	$m_{12,1}$	$m_{13,1}$	$m_{14,1}$	$m_{15,1}$	$m_{16,1}$	i_1	bit 1
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	1
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

<u>Matrix Two for Column Two</u>

Table 10. Conditions for Second Column of 16×16 Matrix

m_{12}	m_{22}	m_{32}	m_{42}	m_{52}	m_{62}	m_{72}	m_{82}	m_{92}	$m_{10,2}$	$m_{11,2}$	$m_{12,2}$	$m_{13,2}$	$m_{14,2}$	$m_{15,2}$	$m_{16,2}$	i_2	bit 2
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	0

A row-reduced matrix:

m_{12}	m_{22}	m_{32}	m_{42}	m_{52}	m_{62}	m_{72}	m_{82}	m_{92}	$m_{10,2}$	$m_{11,2}$	$m_{12,2}$	$m_{13,2}$	$m_{14,2}$	$m_{15,2}$	$m_{16,2}$	i_2	bit 2
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	1
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

<u>Matrix Three for Column Three</u>

Table 11. Conditions for Third Column of 16×16 Matrix

m_{13}	m_{23}	m_{33}	m_{43}	m_{53}	m_{63}	m_{73}	m_{83}	m_{93}	$m_{10,3}$	$m_{11,3}$	$m_{12,3}$	$m_{13,3}$	$m_{14,3}$	$m_{15,3}$	$m_{16,3}$	i_3	bit 3
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1

A row-reduced matrix:

m_{13}	m_{23}	m_{33}	m_{43}	m_{53}	m_{63}	m_{73}	m_{83}	m_{93}	$m_{10,3}$	$m_{11,3}$	$m_{12,3}$	$m_{13,3}$	$m_{14,3}$	$m_{15,3}$	$m_{16,3}$	i_3	bit 3
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

<u>Matrix Four for Column Four</u>

Table 12. Conditions for Fourth Column of 16×16 Matrix

m_{14}	m_{24}	m_{34}	m_{44}	m_{54}	m_{64}	m_{74}	m_{84}	m_{94}	$m_{10,4}$	$m_{11,4}$	$m_{12,4}$	$m_{13,4}$	$m_{14,4}$	$m_{15,4}$	$m_{16,4}$	i_4	bit 4
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1

A row-reduced matrix:

m_{14}	m_{24}	m_{34}	m_{44}	m_{54}	m_{64}	m_{74}	m_{84}	m_{94}	$m_{10,4}$	$m_{11,4}$	$m_{12,4}$	$m_{13,4}$	$m_{14,4}$	$m_{15,4}$	$m_{16,4}$	i_4	bit 4
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

<u>Matrix Five for Column Five</u>

Table 13. Conditions for Fifth Column of 16×16 Matrix

m_{15}	m_{25}	m_{35}	m_{45}	m_{55}	m_{65}	m_{75}	m_{85}	m_{95}	$m_{10,5}$	$m_{11,5}$	$m_{12,5}$	$m_{13,5}$	$m_{14,5}$	$m_{15,5}$	$m_{16,5}$	i_5	bit 5
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	0

A row-reduced matrix:

m_{15}	m_{25}	m_{35}	m_{45}	m_{55}	m_{65}	m_{75}	m_{85}	m_{95}	$m_{10,5}$	$m_{11,5}$	$m_{12,5}$	$m_{13,5}$	$m_{14,5}$	$m_{15,5}$	$m_{16,5}$	i_5	bit 5
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

Matrix Six for Column Six

Table 14. Conditions for Sixth Column of 16×16 Matrix

m_{16}	m_{26}	m_{36}	m_{46}	m_{56}	m_{66}	m_{76}	m_{86}	m_{96}	$m_{10,6}$	$m_{11,6}$	$m_{12,6}$	$m_{13,6}$	$m_{14,6}$	$m_{15,6}$	$m_{16,6}$	i_6	bit 6
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	0

A row-reduced matrix:

m_{16}	m_{26}	m_{36}	m_{46}	m_{56}	m_{66}	m_{76}	m_{86}	m_{96}	$m_{10,6}$	$m_{11,6}$	$m_{12,6}$	$m_{13,6}$	$m_{14,6}$	$m_{15,6}$	$m_{16,6}$	i_6	bit 6
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

Matrix Seven for Column Seven

Table 15. Conditions for Seventh Column of 16×16 Matrix

m_{17}	m_{27}	m_{37}	m_{47}	m_{57}	m_{67}	m_{77}	m_{87}	m_{97}	$m_{10,7}$	$m_{11,7}$	$m_{12,7}$	$m_{13,7}$	$m_{14,7}$	$m_{15,7}$	$m_{16,7}$	i_7	bit 7
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1

A row-reduced matrix:

m_{17}	m_{27}	m_{37}	m_{47}	m_{57}	m_{67}	m_{77}	m_{87}	m_{97}	$m_{10,7}$	$m_{11,7}$	$m_{12,7}$	$m_{13,7}$	$m_{14,7}$	$m_{15,7}$	$m_{16,7}$	i_7	bit 7
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

Matrix Eight for Column Eight

Table 16. Conditions for Eighth Column of 16×16 Matrix

m_{18}	m_{28}	m_{38}	m_{48}	m_{58}	m_{68}	m_{78}	m_{88}	m_{98}	$m_{10,8}$	$m_{11,8}$	$m_{12,8}$	$m_{13,8}$	$m_{14,8}$	$m_{15,8}$	$m_{16,8}$	i	bit 8
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1

A row-reduced matrix:

m_{18}	m_{28}	m_{38}	m_{48}	m_{58}	m_{68}	m_{78}	m_{88}	m_{98}	$m_{10,8}$	$m_{11,8}$	$m_{12,8}$	$m_{13,8}$	$m_{14,8}$	$m_{15,8}$	$m_{16,8}$	i_8	bit 8
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

Matrix Nine for Column Nine

Table 17. Conditions for Ninth Column of 16×16 Matrix

m_{19}	m_{29}	m_{39}	m_{49}	m_{59}	m_{69}	m_{79}	m_{89}	m_{99}	$m_{10,9}$	$m_{11,9}$	$m_{12,9}$	$m_{13,9}$	$m_{14,9}$	$m_{15,9}$	$m_{16,9}$	i_9	bit 9
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	0

A row-reduced matrix:

m_{19}	m_{29}	m_{39}	m_{49}	m_{59}	m_{69}	m_{79}	m_{89}	m_{99}	$m_{10,9}$	$m_{11,9}$	$m_{12,9}$	$m_{13,9}$	$m_{14,9}$	$m_{15,9}$	$m_{16,9}$	i_9	bit 9
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

<u>Matrix Ten for Column Ten</u>

Table 18. Conditions for Tenth Column of 16×16 Matrix

$m_{1,10}$	$m_{2,10}$	$m_{3,10}$	$m_{4,10}$	$m_{5,10}$	$m_{6,10}$	$m_{7,10}$	$m_{8,10}$	$m_{9,10}$	$m_{10,10}$	$m_{11,10}$	$m_{12,10}$	$m_{13,10}$	$m_{14,10}$	$m_{15,10}$	$m_{16,10}$	i_{10}	bit 10
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	0

A row-reduced matrix:

$m_{1,10}$	$m_{2,10}$	$m_{3,10}$	$m_{4,10}$	$m_{5,10}$	$m_{6,10}$	$m_{7,10}$	$m_{8,10}$	$m_{9,10}$	$m_{10,10}$	$m_{11,10}$	$m_{12,10}$	$m_{13,10}$	$m_{14,10}$	$m_{15,10}$	$m_{16,10}$	i_{10}	bit 10
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

<u>Matrix Eleven for Column Eleven</u>

Table 19. Conditions for Eleventh Column of 16×16 Matrix

$m_{1,11}$	$m_{2,11}$	$m_{3,11}$	$m_{4,11}$	$m_{5,11}$	$m_{6,11}$	$m_{7,11}$	$m_{8,11}$	$m_{9,11}$	$m_{10,11}$	$m_{11,11}$	$m_{12,11}$	$m_{13,11}$	$m_{14,11}$	$m_{15,11}$	$m_{16,11}$	i_{11}	bit 11
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1

A row-reduced matrix:

$m_{1,11}$	$m_{2,11}$	$m_{3,11}$	$m_{4,11}$	$m_{5,11}$	$m_{6,11}$	$m_{7,11}$	$m_{8,11}$	$m_{9,11}$	$m_{10,11}$	$m_{11,11}$	$m_{12,11}$	$m_{13,11}$	$m_{14,11}$	$m_{15,11}$	$m_{16,11}$	i_{11}	bit 11
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	1
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

<u>Matrix Twelve for Column Twelve</u>

Table 20. Conditions for Twelfth Column of 16×16 Matrix

$m_{1,12}$	$m_{2,12}$	$m_{3,12}$	$m_{4,12}$	$m_{5,12}$	$m_{6,12}$	$m_{7,12}$	$m_{8,12}$	$m_{9,12}$	$m_{10,12}$	$m_{11,12}$	$m_{12,12}$	$m_{13,12}$	$m_{14,12}$	$m_{15,12}$	$m_{16,12}$	i_{12}	bit 12
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	0

A row-reduced matrix:

$m_{1,12}$	$m_{2,12}$	$M_{3,12}$	$m_{4,12}$	$m_{5,12}$	$m_{6,12}$	$m_{7,12}$	$m_{8,12}$	$m_{9,12}$	$m_{10,12}$	$m_{11,12}$	$m_{12,12}$	$m_{13,12}$	$m_{14,12}$	$m_{15,12}$	$m_{16,12}$	i_{12}	bit 12
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

<u>Matrix Thirteen for Column Thirteen</u>

Table 21. Conditions for Thirteenth Column of 16×16 Matrix

$m_{1,13}$	$m_{2,13}$	$m_{3,13}$	$m_{4,13}$	$m_{5,13}$	$m_{6,13}$	$m_{7,13}$	$m_{8,13}$	$m_{9,13}$	$m_{10,13}$	$m_{11,13}$	$m_{12,13}$	$m_{13,13}$	$m_{14,13}$	$m_{15,13}$	$m_{16,13}$	i_{13}	bit 13
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1

A row-reduced matrix:

$m_{1,13}$	$m_{2,13}$	$m_{3,13}$	$m_{4,13}$	$m_{5,13}$	$m_{6,13}$	$m_{7,13}$	$m_{8,13}$	$m_{9,13}$	$m_{10,13}$	$m_{11,13}$	$m_{12,13}$	$m_{13,13}$	$m_{14,13}$	$m_{15,13}$	$m_{16,13}$	i_{13}	bit 13
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	1
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

<u>Matrix Fourteen for Column Fourteen</u>

Table 22. Conditions for Fourteenth Column of 16×16 Matrix

$m_{1,14}$	$m_{2,14}$	$m_{3,14}$	$m_{4,14}$	$m_{5,14}$	$m_{6,14}$	$m_{7,14}$	$m_{8,14}$	$m_{9,14}$	$m_{10,14}$	$m_{11,14}$	$m_{12,14}$	$m_{13,14}$	$m_{14,14}$	$m_{15,14}$	$m_{16,14}$	i_{14}	bit 14
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	0

A row-reduced matrix:

$m_{1,14}$	$m_{2,14}$	$m_{3,14}$	$m_{4,14}$	$m_{5,14}$	$m_{6,14}$	$m_{7,14}$	$m_{8,14}$	$m_{9,14}$	$m_{10,14}$	$m_{11,14}$	$m_{12,14}$	$m_{13,14}$	$m_{14,14}$	$m_{15,14}$	$m_{16,14}$	i_{14}	bit 14
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	1
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

<u>Matrix Fifteen for Column Fifteen</u>

Table 23. Conditions for Fifteenth Column of 16×16 Matrix

$m_{1,15}$	$m_{2,15}$	$m_{3,15}$	$m_{4,15}$	$m_{5,15}$	$m_{6,15}$	$m_{7,15}$	$m_{8,15}$	$m_{9,15}$	$m_{10,15}$	$m_{11,15}$	$m_{12,15}$	$m_{13,15}$	$m_{14,15}$	$m_{15,15}$	$m_{16,15}$	i_{15}	bit 15
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1

A row-reduced matrix:

$m_{1,15}$	$m_{2,15}$	$m_{3,15}$	$m_{4,15}$	$m_{5,15}$	$m_{6,15}$	$m_{7,15}$	$m_{8,15}$	$m_{9,15}$	$m_{10,15}$	$m_{11,15}$	$m_{12,15}$	$m_{13,15}$	$m_{14,15}$	$m_{15,15}$	$m_{16,15}$	i_{15}	bit 15
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	1
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

<u>Matrix Sixteen for Column Sixteen</u>

Table 24. Conditions for Sixteenth Column of 16×16 Matrix

$m_{1,16}$	$m_{2,16}$	$m_{3,16}$	$m_{4,16}$	$m_{5,16}$	$m_{6,16}$	$m_{7,16}$	$m_{8,16}$	$m_{9,16}$	$m_{10,16}$	$m_{11,16}$	$m_{12,16}$	$m_{13,16}$	$m_{14,16}$	$m_{15,16}$	$m_{16,16}$	i_{16}	bit 16
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1

A row-reduced matrix:

$m_{1,16}$	$m_{2,16}$	$m_{3,16}$	$m_{4,16}$	$m_{5,16}$	$m_{6,16}$	$m_{7,16}$	$m_{8,16}$	$m_{9,16}$	$m_{10,16}$	$m_{11,16}$	$m_{12,16}$	$m_{13,16}$	$m_{14,16}$	$m_{15,16}$	$m_{16,16}$	i_{16}	bit 16
1	0	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	0
0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0	1
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	1
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

The 96 equations implied by Tables 9 through 24 have 256 unknown matrix entries and 16 initialization vector entries, along with the nonsingularity restriction. The row-reduced matrices imply solutions for the upper five matrix rows as functions of the bottom 11 matrix rows. However, the nonsingularity requirement cannot be met. To see a reason, start with a deterministic solution for the initialization vector from the right-most bottom row pair in the row-reduced matrices. This result is 0100000101100001. Since the sum of the first 16 positions in the last three rows of Table 1 is all-zero, the chained transformations must sum to an all-zero vector. Knowledge of the initialization vector permits this computation to be made as shown in the following set of computations.

Row	Input Vector	Output vector
4	1101101101101101	1101111101001101
Initialization vector:		0100000101100001
Sum_1 (result of matrix multiplication)		1001111000101100
5	1011011011011011	1111010011011111
Previous result:		1101111101001101
Sum_2 (result of matrix multiplication)		0010101110010010
6	0110110110110110	0100110111110100
Previous result:		1111010011011111
Sum_3 (result of matrix multiplication)		1011100100101011
$Sum_1 + Sum_2 + Sum_3$:		0000110010010101

The final summation vector should be all-zero to support nonsingularity, and it is not. This contradicts the computation for the initialization vector, and the result proves that no nonsingular 16×16 matrix can meet the input/output requirements.

48×48 Matrix

There are solutions for 48×48 nonsingular matrices that meet the requirements. This is known because they can be based on the solutions for the 24×24 matrices previously derived. The construction of the solutions is based on the decomposition shown below:

$$M_{48} = \begin{bmatrix} M_{24} M_0 \\ M_0 M_{24} \end{bmatrix}$$

$$M_{48}^{-1} = \begin{bmatrix} M_{24}^{-1} M_0 \\ M_0 M_{24}^{-1} \end{bmatrix}$$

Here, M_{48} is the new matrix, M_{24} is a previously derived 24×24 matrix, M_{24}^{-1} is its inverse, and M_0 represents 24×24 all-zero matrices. The initialization vector can be constructed by replicating the 24-bit transform initialization vectors. For example, the initialization vector corresponding to that used in Eq. 27 is expressed mathematically as:

$$2^{42}\, i + 2^{36}\, i + 2^{30}\, i + 2^{24}\, i + 2^{18}\, i + 2^{12}\, i + 2^{6}\, i + i.$$

Here, i is the 6×6 initialization vector. The proof that this construction meets the pertinent requirements is that the first 24 bits will generate the same result as that obtained for M_{24} for the first 24 output bits and will contribute nothing to the second 24 output bits. Note that the first 24 input/output pairs are independent of each other, since there is no chaining between the two segments. The second 24 input bits will not contribute to the first 24 output bits because of the all-zero matrix in the lower left. These 24 bits will generate the same result as that obtained for M_{24} for the second 24 output bits, since there is no other contribution excepting the initialization vector.

Appendix B: Additional Pre-Arm Inversion Ranks that Divide 24

Table 1 indicates the conditions that must be met for compliance with the current System 2 specification. However, it is also of interest to investigate correspondence with the "Pre-Arm" portion of the System 2 specification, which is limited to the first two rows of Table 1. This is because inverting the Pre-Arm information to obtain Unique Signal information must not be easy to generate accidentally by any matrix. For this reason, the study described in this Appendix was undertaken, and work on inversion ranks that divide 24 will continue as resources allow.

An example of one of the most straightforward inversion matrices that hase been found so far (and which meets the conditions of the first two rows of Table 1) is:

$$(output + 011100010101110001000111) \times \begin{bmatrix} 100000000000000000000000 \\ 110000000000000000000000 \\ 001110000000000000000000 \\ 000110000000000000000000 \\ 000010000000000000000000 \\ 000001110000000000000000 \\ 000000100000000000000000 \\ 000000010000000000000000 \\ 000000001000000000000000 \\ 000000000100000000000000 \\ 000000000010000000000000 \\ 000000000001000000000000 \\ 000000000000100000000000 \\ 000000000000010000000000 \\ 000000000000001000000000 \\ 000000000000000100000000 \\ 000000000000000110000000 \\ 000000000000000111000000 \\ 000000000000000111100000 \\ 000000000000000000010000 \\ 000000000000000000001000 \\ 000000000000000000000100 \\ 000000000000000111101010 \\ 000000000000000000000001 \end{bmatrix} = input$$

References

1. Air Force AMAC POG "System 2 Basic Interface Specification," Specification Standard No. SYS 2001-02, 22 September 2004.
2. Spray, Stanley, and Arlin Cooper, "The Unique Signal Concept for Detonation Safety in Nuclear Weapons," SAND91-1269, June 1993.
3. Cooper, J. A., "Implementation of Unique Signal and Related Components," DG 10276/A, June 2003.
4. Cooper, J. A., "Techniques for Digital Data Transmission and Monitoring," *National Aerospace and Electronics Conference Proceedings*, May 1978.
5. Stone, Harold S. *Discrete Mathematical Structures and their Applications*, Science Research Associates Press 1973.
6. Cooper, J. A., "One-Way Transformations: Analysis and Applications," SAND86-0425, April 1986.
7. Cooper, J. A., "The Application of Chained One-Way Transformations to Intent Unique Signal Transmission and Verification," SAND87-2741, February 1988.

DISTRIBUTION:

Carlson, David D.	0200	MS 0428	
Rogulich, Andrew J.	0225	MS 0136	
Novotny, George C.	2001	MS 0457	
Hartwig, Ronald C.	2100	MS 0437	
Clements, David	2111	MS 0447	
Wirth, Joel	2123	MS 0482	
Slezak, Scott	2132	MS 0481	
Dalton, Larry J.	2622	MS 0860	
McCaughey, Kathleen	2700	MS 0868	
McGlaun, Michael	2830	MS 0437	
Anderson, Arden	2912	MS 0647	
Stevenson, Larry	2912	MS 0647	
McCallister, Gary	2912	MS 0647	
Molley, Perry A.	5351	MS 0537	
Brandt, Dale J.	5351	MS 0537	
Deming, Douglas	5339	MS 0503	
Shephard, Les	6000	MS 0724	
Tatro, Marjorie L.	6200	MS 0741	
Covan, John M.	6202	MS 0755	
Kuswa, Glen W.	6202	MS 0755	
Robinett III, Rush D.	6210	MS 0741	
Veers, Paul	6214	MS 0708	
Mitchiner, John	6220	MS 1138	
Snyder, Lillian	6222	MS 1138	
Rogers, Karen	6223	MS 1138	
Stubblefield, William	6223	MS 1137	
Cooper, J. Arlin	6252	MS 0615	(10)
Roach, Dennis	6252	MS 0615	
Wyss, Gregory D.	6442	MS 0757	
Allen, Mark	6861	MS 0748	
Brewer, Jeffrey	6861	MS 0748	
Robinson, David G.	6861	MS 0748	
Ringland, James T.	8112	MS 9201	
Henson, Doug	8200	MS 9153	
DeVay, Michael	8221	MS 9034	
Talbot, Edward B.	8222	MS 9154	
Bryson, Phil	8222	MS 9154	
Rorke, William	8226	MS 9106	
Sauls, Ronald	8231	MS 9013	
Mayer, Laurence	8232	MS 9154	
Gehmlich, Douglas	8241	MS 9014	
Hardin, Daniel	8241	MS 9014	
Johnson, Alice J.	8241	MS 9014	
Molle, Raphael	8241	MS 9014	
Talso, Warner	10326	MS 1091	

Sanders, Gary A.	10800	MS 0938	
D'Antonio, Perry E.	10827	MS 0942	
Knapp, Corey	12300	MS 0521	
Jones, Todd R.	12300	MS 0428	
Spray, Stanley D.	12300	MS 0428	
Mickelsen, Brad	12332	MS 0492	
Chen, Ken	12332	MS 0492	
Donnell, Alton	12332	MS 0492	
Fuentes, Marty	12332	MS 0492	
McLean, Mike	12332	MS 0492	
Mahn, Jeff	12332	MS 0492	
Maloney, Kevin	12332	MS 0492	
Pelligrino, Traci	12332	MS 0492	
Schriner, Heather	12332	MS 0492	(10)
Summers, Dan	12332	MS 0492	
Diegert, Kathleen	12335	MS 0830	
Sjulin, Janet M.	12337	MS 0829	
Johnson, Victor J.	12340	MS 0428	
Hoffman, John P. Jr.	12345	MS 0491	
Kreutzfeld, Richard E.	12346	MS 0405	
Camp, Susan E.	12346	MS 0405	
Kerschen, Matt	12346	MS 0405	
Merewether, Kim	12346	MS 0405	
Pedersen, Ronald D.	12346	MS 0405	
Rice, Glenn	12346	MS 0405	
Sobolik, Keri	12346	MS 0405	
Sype, Teresa	12346	MS 0405	
Stevenson, Martin	12347	MS 0405	
Waters, Bob	12347	MS 0405	
Central Technical Files	8945-1	MS 9018	(2)
Technical Library	4536	MS 0899	(2)