A history of the application of MDS matrices in cryptography

Ana Clara Zoppi Serpa
Prof. Dr. Ricardo Dahab
Dr. Jorge Nakahara Jr.

February 3, 2022

Contents

Chapter 1

A history of the application of MDS matrices in cryptography

MDS matrices have been widely used in the construction of diffusion layers for block ciphers such as SHARK [24], SQUARE [12], BKSQ [13], KHAZAD [4], ANUBIS [3], Hierocrypt-3 [10], Rijndael (AES) [14] and Curupira [5]. They have also been applied in the design of hash functions (e.g Whirlwind [2] and Grøstl [15]). The choice is due to the fact that MDS codes provide transformations with optimal linear and differential branch numbers (see e.g [12] or [24]), thus contributing to security against Differential and Linear Cryptanalysis attacks.

When a matrix is MDS, optimal *branch number* (a measure of diffusion power) is ensured, therefore, from the theoretical security perspective, any two distinct $n \times n$ MDS matrices present equal contribution to a cipher's design in terms of diffusion power. However, their computational cost, which is a relevant practical implementation criterion, *is not* necessarily the same. This motivates not only the search for MDS matrices, but the search for *MDS matrices with low computational cost*. In this work, the computational cost of a matrix A is measured by the amount of **xor** and **xtime** operations required when multiplying a cipher's state column vector by A.

Due to the computational cost of matrix multiplication, there is an interest in finding MDS matrices with coefficients as small as possible, in order to minimize the required amount of **xor** and **xtime** operations required by the implementations. However, the complexity of finding MDS matrices through random search increases proportionally to the dimension, which led to the investigation of systematic methods to construct (or find) MDS matrices. One possible avenue is trying to find direct mathematical constructions which ensure the MDS property, and another is to impose restrictions to limit the random search space (e.g imposing the matrix should be circulant, as was done by the authors of [12]). Furthermore, there is an interest in finding involutory MDS

matrices (as pointed by [4] and [3]), so that the encryption and the decryption computational cost are the same.

It is also worth noting that, although MDS matrices are widely used in cryptographic algorithms, there are designs which prefer not to make use of them. The block ciphers Serpent [8], IDEA [18] and PRESENT [9], for instance, do not include MDS matrices in their design. The hash function Keccak [7], which was later selected by NIST to become the SHA-3 standard, also does not use MDS matrices. The computational cost can be related to this choice.

In this chapter, we aim at providing a history of the application of MDS matrices in cryptography, listing the matrices, the ciphers in which they have been applied, the respective Finite Fields (order and irreducible polynomial), and their cost (amount of **xor** and **xtime** operations).

Note: this is a partial report. It will be expanded in the future.

We assume the reader is familiar with:

- Linear branch number (see Chapter X)
- Differential branch number (see Chapter X)
- Differential Cryptanalysis (see Chapter X)
- Linear Cryptanalysis (see Chapter X)
- MDS codes (see Chapter X and, for further detail, reference [20])
- Diffusion property in cryptography (see Chapter X)
- Groups, rings and fields in abstract algebra (see Chapter X)

1.1 Notation

- $det(A)$: determinant of the matrix A
- A^{-1}: inverse matrix of A
- n, k, d: parameters of a code
- $\mathcal{C}$: a code
- G: generator matrix of a code
- I_n: the $n \times n$ identity matrix
- $[I_n B]$: matrix obtained by placing the $n \times n$ matrix B to the right of the $n \times n$ identity matrix I_n. For example, for $B = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $[I_n B] = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 3 & 4 \end{bmatrix}$

1.2 Acronyms

- MDS: Maximum Distance Separable
- AES: Advanced Encryption Standard (Rijndael's name after being chosen by NIST)
- **xor**: bitwise XOR between two bit strings
- **xtime**: refers to the multiplication by the polynomial x in the finite field GF(2^m) for an integer m

1.3 Preliminaries

1.3.1 Linear codes

Definition 1 (Hamming weight [20]) *The Hamming weight $w(x)$ of a vector x is the number of nonzero components of the vector x.*

Definition 2 (Hamming distance [20]) *The Hamming distance between two vectors x and y is $w(x - y)$, which is equal to the Hamming weight of the difference of the two vectors.*

Definition 3 (Linear code [20]) *A linear $[n, k, d]$ code over a field $\mathbb{F}$ is a k-dimensional subspace of the vector space $\mathbb{F}^n$, where any two different vectors of the subspace have a Hamming distance of at least d, and d is the largest number with this property.*

The distance d of a linear code equals the minimum weight of a non-zero codeword in the code. A linear code can be described by generator and/or parity-check matrices.

Definition 4 (Generator matrix [20]) *A generator matrix G for an $[n, k, d]$ code C is a $k \times n$ matrix whose rows form a vector space basis for C. The choice of a basis in a vector space is not unique, thus a code has many different generator matrices which can be reduced to one another by performing elementary row operations.*

Definition 5 (Parity-check matrix [20]) *A parity-check matrix H for an $[n, k, d]$ code C is an $(n - k) \times k$ matrix with the property that a vector x is a codeword of C iff $Hx^T = 0$.*

Theorem 1 (Singleton Bound [20]) *If C is an $[n, k, d]$ code, then $d \leq n - k + 1$.*

Definition 6 (MDS code [20]) *An* MDS code *is a* linear code *that meets the* Singleton bound*, i.e a linear code with $d = n - k + 1$.*

An MDS matrix associated to a $[n, k, d]$ code has *branch number* equal to d, which is the maximum possible branch number, thus providing optimal diffusion.

Definition 7 (Branch number [25]) *The branch number $\mathcal{B}$ of a linear mapping $\theta : GF(2^m)^k \to GF(2^m)^l$ is defined as:*

$$\mathcal{B}(\theta) = \min_{a \neq 0}\{w(a) + w(\theta(a))\}.$$

Note that here, $+$ denotes a XOR operation, since the fields have characteristic equal to 2.

Furthermore, given a matrix M, associated to a $[n, k, d]$ linear code, the linear mapping defined by $\theta(a) = a \cdot M$ has branch number $\mathcal{B}(\theta) = d$. When the linear code is MDS, i.e when M is MDS, the mapping is an optimal diffusion mapping.

1.3.2 Matrices

Obs: eu escrevi essas primeiras definições (matriz singular, involutória, circulante, circulante à esquerda, circulante à direita) com base no que eu lembrava de matemática mesmo, então por hora ainda não coloquei uma referência bibliográfica, já que são definições mais gerais e não chegam a ser específicas de cripto. Mas posso colocar depois se necessário.

Definition 8 (Singular matrix) *A square matrix A is singular if and only if $det(A) = 0$.*

Definition 9 (Non-singular matrix) *A is non-singular if and only if $det(A) \neq 0$.*

Definition 10 (Involutory matrix) *An $n \times n$ square matrix A is involutory if $A \times A = I_n$, where I_n is the identity matrix. In other words, A is involutory when $A = A^{-1}$.*

Definition 11 (Circulant matrix) *An $n \times n$ matrix A is circulant if each row i is formed by a cyclical shift of i positions of the same set of elements $\{a_0, a_1, a_2, ..., a_{n-1}\}$.*

Definition 12 (Left circulant matrix) *A circulant matrix in which the shift is a cyclical shift to the left, i.e*

$$A = \begin{bmatrix} a_0 & a_1 & ... & ... & a_{n-1} \\ a_1 & a_2 & ... & a_{n-1} & a_0 \\ ... & ... & ... & ... & ... \\ a_{n-1} & a_0 & ... & ... & a_{n-2} \end{bmatrix}.$$

Definition 13 (Right circulant matrix) *A circulant matrix in which the shift is a cyclical shift to the right, i.e*

$$A = \begin{bmatrix} a_0 & a_1 & ... & ... & a_{n-1} \\ a_{n-1} & a_0 & a_1 & ... & a_{n-2} \\ ... & ... & ... & ... & ... \\ a_1 & ... & a_{n-2} & a_{n-1} & a_0 \end{bmatrix}.$$

Note that circulant matrices can be defined by just one row, since all the other rows are cyclical shifts of the first. Therefore, they can be denoted as $circ(a_0, a_1, ..., a_{n-1})$. In the case of left circulant and right circulant matrices, respectively, $lcirc(a_0, ..., a_{n-1})$ and $rcirc(a_0, ..., a_{n-1})$. For example, matrices (1.12) and its inverse (1.12), used in the Rijndael cipher, can be denoted as $rcirc(02_x, 03_x, 01_x, 01_x)$ and $rcirc(0e_x, 0b_x, 0d_x, 09_x)$. Since a circulant matrix can be defined by one row only, only n elements are required, and this optimizes the process of searching for (and finding) such matrices. However, *there are no guarantees about the MDS property.* One must check whether Theorem 2 holds to ensure the obtained matrix is MDS. As an example, the circulant matrix initially employed in Whirlpool-0 [26] is not MDS, and was further replaced by an actual MDS matrix found by Shirai in [25].

Definition 14 (Transpose matrix) *The transpose of a matrix A, denoted by A^T, is the matrix such that $A^T[i][j] = A[j][i]$. In other words, it is the matrix obtained by writing the rows of A as columns. Note that, if A is an $m \times n$ matrix, then A^T will be $n \times m$.*

Definition 15 (Submatrix) *Given a matrix M, a submatrix of M is the matrix obtained after removing z rows and columns of M, $z \geq 1$, provided that there are sufficient rows (and columns) to be removed.*

Theorem 2 (MDS codes [20]) *An $[n, k, d]$-code $\mathcal{C}$ with generator matrix $G = [I_n B]$, where B is a $k \times (n-k)$ matrix, is MDS if and only if every square submatrix of B is non-singular.*

We call the B matrix of Theorem 2 the *MDS matrix* throughout this work, i.e the MDS matrices we study are the B matrices of the respective MDS codes chosen when designing them. Note that Definition 6 establishes the conditions for a code to be MDS, therefore Theorem 2 is an alternative way of evaluating a code, or a matrix, with respect to the MDS property. For further detail on matrices, determinants and linear algebra, the reader may refer to [19].

Definition 16 (Cauchy matrix) *Given $x_0, ..., x_{n-1}$ and $y_0, ..., y_{n-1}$, the matrix A where $A[i][j] = \frac{1}{x_i + y_j}$ is called a Cauchy matrix. According to [27], provided that $x_i \neq x_j$ for $0 \leq i, j \leq n-1$, that $y_i \neq y_j$ for $0 \leq i, j \leq n-1$ and that $x_i + y_j \neq 0$ for all i, j, any square submatrix of a Cauchy matrix is nonsingular over any field.*

It is worth noting that a Cauchy matrix construction directly ensures the MDS property, as can be seen in Definition 16, and it requires only $2n$ choices of elements, since the x_i and the y_i must be defined.

Definition 17 (Hadamard matrix [6]) *Given n elements $a_0, a_1, ..., a_{n-1}$, n being a power of 2, the matrix H such that $H[i][j] = a_{i \oplus j}$ is a Hadamard matrix.*

In Whirlwind[2], the authors make use of *dyadic* matrices, defining them as a matrix S such that $S[i][j] = s_{i \oplus j}$ given a set $s_0, s_1, ..., s_{n-1}$ of n elements.

This definition matches Definition 17, which is used in Anubis and Khazad, but referred as Hadamard instead of dyadic. Therefore, for dyadic matrices, the same situation described for Hadamard applies: a dyadic construction allows us to reduce the scope of the element choice, i.e only n elements must be chosen, but there is no guarantee of MDS property.

Note that a Hadamard construction, similarly to a circulant construction, requires only n elements to be defined, but it does not guarantee MDS property either. To the best of our knowledge, no proofs about Hadamard matrices being MDS have been presented in the literature at the time of writing. Furthermore, in this work, we believe we present an example of a Hadamard non-MDS matrix. See Section 1.7 for further detail on this.

Definition 18 (Vandermonde matrix [16]) *Given z elements $a_0, a_1, ..., a_{z-1}$, the $z \times n$ matrix V such that*

$$V = \begin{bmatrix} 1 & a_0 & a_0^2 & ... & a_0^{n-1} \\ 1 & a_1 & a_1^2 & ... & a_1^{n-1} \\ ... & ... & ... & ... & ... \\ 1 & a_{z-1} & a_{z-1}^2 & ... & a_{z-1}^{n-1} \end{bmatrix} \tag{1.1}$$

is a Vandermonde matrix.

Similarly to circulant and Hadamard constructions, in the case of the Vandermonde matrix, z elements are required and then we must choose the number of columns n. Not all Vandermonde matrices are square matrices, but the notion of MDS matrix applies only to square matrices. Therefore, z must be equal to n if we wish to construct a Vandermonde MDS matrix. However, again there are no guarantees about the MDS property with a Vandermonde construction. To the best of our knowledge, at the time of writing, there are no such guarantees. The matrices must be constructed and then evaluated with respect to the MDS property, e.g using Theorem 2.

A summary on the types of matrices

An $n \times n$ matrix possesses n^2 elements and thus, when constructing one e.g by selecting random elements, n^2 choices must be made. However, Cauchy, circulant, Vandermonde and Hadamard (dyadic) constructions allow us to lower the number of elements we need to select. Circulant, Vandermonde and Hadamard constructions allow us to select only n elements, whilst Cauchy constructions require selecting $2n$ elements. The Cauchy construction ensures MDS property, whilst the other constructions do not and e.g Theorem 2 must be used to evaluate MDS property. Furthermore, it is relevant to note that, albeit most matrices in this work have their dimension n be a power of two such as 4 or 8, this is not a requirement for the construction. One can construct $n \times n$ circulant (or Cauchy, or Vandermonde) matrices for any arbitrary n. The dimension n must only be a power of two for the Hadamard (dyadic) construction. Table 1.1 summarizes this information.

Type	Elements to select	MDS guarantee	n must be power of two
Circulant	n	no	no
Hadamard (dyadic)	n	no	yes
Vandermonde	n	no	no
Cauchy	$2n$	yes	no
random	n^2	no	no

Table 1.1: Matrix classification summary

1.3.3 Evaluating a matrix for MDS property

If Theorem 2 is used, the determinant of the matrix itself must be calculated, as well as the determinants of its submatrices. First, we derive a formula for the cost of calculating the determinant of an $n \times n$ matrix. Our cost unit is *the number of multiplications in a finite field*, since it is the most expensive operation.

The determinant of a 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ can be computed by means of the formula $ad - bc$, requiring therefore two multiplications.

The determinant of a 3×3 matrix can be computed by calculating cofactors of 2×2 submatrices obtained by removing a row i and a column j. For example, the determinant of $\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$ can be computed as $a \begin{vmatrix} e & f \\ h & i \end{vmatrix} + b \begin{vmatrix} d & f \\ g & i \end{vmatrix} + c \begin{vmatrix} d & e \\ g & h \end{vmatrix}$, where $\begin{vmatrix} e & f \\ h & i \end{vmatrix}$ denotes the determinant of the submatrix $\begin{bmatrix} e & f \\ h & i \end{bmatrix}$.

The cost is therefore $3 + 3t(2)$, where $t(2)$ is the number of multiplications required to compute the determinant of a 2×2 matrix. We know that $t(2) = 2$, therefore the cost to obtain the determinant of a 3×3 matrix is $3+3 \times 2 = 9$, i.e $t(3) = 9$. Extending this logic, let $t(n)$ be the cost of obtaining the determinant of an $n \times n$ matrix. Then $t(n) = n + nt(n-1) = n + n(n-1+(n-1)t(n-2)) = n+n(n-1)+n(n-1)t(n-2) = n+n(n-1)+n(n-1)(n-2)+...+n(n-1)(n-2)..2$. For example, for $n = 4$, $t(4) = 4+4 \times 3+4 \times 3 \times 2 = 4+12+24 = 40$ multiplications in a finite field.

In order to evaluate a matrix for MDS property, we must compute the determinants of all its square submatrices. Let A be an $n \times n$ matrix. A submatrix of A is obtained by removing z rows and columns of A. The possible values of z range from 1 to $n - 1$. When removing $n - 1$ rows and columns though, only single matrix elements remain. We evaluate if they are zero or not, and this does not require multiplications in the underlying finite field, only equality checks. When removing z rows and columns, $(n - z) \times (n - z)$ submatrices are obtained, and computing a determinant costs $t(n-z)$ multiplications in a finite field. There are 2^z ways of choosing which rows are to be removed, and 2^z ways of choosing which columns are to be removed. Therefore, $2^z \times 2^z = 2^{2z}$ possible $(n-z) \times (n-z)$ submatrices, totalizing 2^{2z} determinants to evaluate. The cost is therefore $2^{2z} \times t(n - z)$ multiplications for a given z. Let $t'(z) = 2^{2z} \times t(n - z)$. Since z ranges from 1 to $n - 2$, the total cost to evaluate a matrix for MDS

property will be $t'(1) + t(2) + ... + t'(n-2)$.

1.3.4 Abstract algebra

Aqui pretendo colocar definições de grupo, grupo abeliano, corpo etc. A parte de álgebra abstrata que não é específica de corpos finitos e que a gente geralmente vê na faculdade

1.3.5 Finite fields — GF(2^m)

(Finite field [14]) *A* finite field *is a field with a finite number of elements. The number of elements in the set is called the* order *of the field.*

(Characteristic and order [14]) *A field with order r exists if and only if r is a prime power, i.e $r = p^m$ for some integer m, where p is a prime integer. p is called the* characteristic *of the field. For each prime power there is exactly one finite field, denoted by GF(p^m).*

(Representing finite fields with prime order [14]) *Elements of a finite field GF(p) can be represented by the integers $0, 1, ..., p-1$, and the field operations are integer addition modulo p and integer multiplication modulo p.*

(Representing finite fields with non-prime order [14]) *For finite fields with an order $r = p^m$ that is not prime, addition and multiplication cannot be represented by addition and multiplication modulo r, and instead other representations must be used. One of the possible representations for GF(p^m) is by means of* polynomials over GF(p) with degree at most $m-1$. *Addition and multiplication are then defined modulo an* irreducible polynomial of degree m.

(Polynomial [14]) *A polynomial over a field $\mathbb{F}$ is an expression of the form*

$$b(x) = b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + ... + b_2x^2 + b_1x + b_0,$$

where x is the indeterminate *and $b_i \in \mathbb{F}$ are the coefficients. The* degree *of the polynomial equals l if $b_j = 0$ for all $j > l$ and l is the smallest number with this property.*

Note that, when using polynomials over GF(p) to represent the GF(p^m) field, the degree is at most $m-1$.

In this chapter, we focus particularly on fields with characteristic $p = 2$, due to their wide application in cryptography.

Addition and multiplication are defined on polynomials as follows.

(Polynomial addition [14]) *Summing two polynomials $a(x)$ and $b(x)$ consists of summing the coefficients with equal powers of x, with the sum occuring in the underlying field $\mathbb{F}$. The neutral element is 0 (the polynomial with all coefficients equal to 0). The inverse element can be found by replacing each coefficient by its inverse element in $\mathbb{F}$. The degree of $a(x) + b(x)$ is at most the maximum of the degrees of $a(x)$ and $b(x)$, therefore addition is closed.*

For polynomials over GF(2) stored as integers in a cryptographic software implementation, addition can be implemented with a bitwise XOR instruction.

(Polynomial multiplication [14]) *In order to make multiplication closed, we select a polynomial $p(x)$ of degree l, called the* reduction polynomial. *Multiplication of $a(x)$ and $b(x)$ is then defined as the algebraic product of the polynomials modulo the reduction polynomial $p(x)$.*

The neutral element is 1 (the polynomial of degree 0 and with coefficient of x^0 equal to 1). The inverse element of $a(x)$ is $a^{-1}(x)$ such that $a(x) \times a^{-1}(x) = 1 mod p(x)$. Note that $a^{-1}(x)$ exists only when $a(x) \neq 0$.

For polynomials over GF(2) stored as integers in a cryptographic software implementation, multiplication by x can be implemented as a logical bit shift followed by conditional XOR (i.e subtraction) of the reduction polynomial (the **xtime** operation). Multiplication by other polynomials can be implemented as a series of **xtime**.

The reduction polynomial is chosen as an irreducible polynomial.

(Irreducible polynomial [14]) *A polynomial $d(x)$ is irreducible over the field GF(p) if and only if there exist no two polynomials $a(x)$ and $b(x)$ with coefficients in GF(p) such that $d(x) = a(x) \times b(x)$, where $a(x)$ and $b(x)$ are of degree greater than 0.*

For further reference on abstract algebra and Finite Fields, the reader may refer to [21], [23] and [22].

1.3.6 Computational cost unit

Computational cost of multiplication in GF(2^8)

Consider T a state byte, which we multiply by the polynomial $2e_x = 00101110_2 = x^5 + x^3 + x^2 + x$ in GF(2^8). Note that

$$T \cdot 2e_x = T \cdot x^5 + T \cdot x^3 + T \cdot x^2 + T \cdot x = T \cdot x \cdot x \cdot x \cdot x \cdot x + T \cdot x \cdot x \cdot x + T \cdot x \cdot x + T \cdot x,$$

where $\cdot$ denotes multiplication and $+$ denotes addition (which, in GF(2^8), is equivalent to a bitwise XOR). Multiplication by the x polynomial is performed by **xtime**, and addition is performed by **xor**.

Let $T \cdot x = Y$. Then $T \cdot 2e_x = Y + Y \cdot x + Y \cdot x \cdot x + Y \cdot x \cdot x \cdot x \cdot$.

Let $Y \cdot x = W$. Then $T \cdot 2e_x = Y + W + W \cdot x + W \cdot x \cdot x \cdot x$.

Let $W \cdot x = Z$. Then $T \cdot 2e_x = Y + W + Z + Z \cdot x \cdot x$.

The total number of **xtime** operations in this process is 5 (1 to obtain Y from T, 1 to obtain W from Y, 1 to obtain Z from W, 2 to compute $Z \cdot x \cdot x$), since we can reuse intermediate **xtime** calls. The total number of **xor** operations is 3. For multiplication in GF(2^8), in the worst case, 7 **xtime** would be necessary, since the maximum degree of polynomials in GF(2^8) is 7.

Computational cost of a matrix

The computational cost of an $n \times n$ matrix A is given by the necessary **xor** and **xtime** operations when multiplying a $n \times 1$ column vector by A. As an example, we calculate the cost of matrix (1.5), used in the SQUARE [12] cipher.

A row of matrix (1.5) contains the elements $01_x = 1, 02_x = x$ and $03_x = x+1$ only. Multiplying by 01_x does not require **xtime** or **xor**, since $01_x \cdot T = T$. Computing $02_x \cdot T = x \cdot T$ requires 1 **xtime**. Computing $03_x \cdot T = (x+1) \cdot T = T \cdot x + T$ requires 1 **xtime** and 1 **xor**. Furthermore, adding the row multiplication results costs 3 **xor**. Therefore, the cost of a row is 2 **xtime** and 4 **xor**. Equation 1.2 illustrates this, with t_1, t_2, t_3 and t_4 being bytes of the state column vector.

$$\begin{bmatrix} 02_x & 01_x & 01_x & 03_x \end{bmatrix} \cdot \begin{bmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{bmatrix} = 02_x \cdot t_1 + 01_x \cdot t_2 + 01_x \cdot t_3 + 03_x \cdot t_4 \quad (1.2)$$

Note that matrix (1.5) contains 4 rows, yielding a total cost of 8 **xtime** and 16 **xor**.

1.4 MDS matrix catalogue

In Table 1.2, the **Ord** column refers to the matrix dimensions, the **Inv** column refers to whether they are involutory or not, **Use** refers to application in e.g a block cipher or hash function, **Bib** contains the bibliographic reference, **#xor** refers to the necessary amount of **xor** operations, and **#xtime** refers to the necessary amount of **xtime** operations. All finite fields of Table 1.2 have characteristic $p = 2$. The order is 2^m, with m being given by the degree of the irreducible polynomial in the column $GF(2)[x]/(p(x))$. For example, $m = 8$ for SHARK, SQUARE, BKSQ, KHAZAD, ANUBIS, Hierocrypt, Rijndael and the Cauchy matrix found by [27].

Year	Ord	Type	Inv	Use	Bib	$GF(2)[x]/(p(x))$	#xor	#xtime	Matrices
1996	8	—	no	SHARK	[24]	$x^8+x^7+x^6+x^5$ $+x^4+x^2+1$	235 223	369 393	(1.3) (1.4)
1997	4	right circulant	no	SQUARE	[12]	$x^8+x^7+x^6+x^5$ $+x^4+x^2+1$	16 40	8 48	(1.5) (1.6)
1997	8	Cauchy	yes	—	[27]	$x^8+x^4+x^3$ $+x^2+1$	240	344	(1.7)
1998	3	right circulant	no	BKSQ	[13]	$x^8+x^7+x^6+x^5$ $+x^4+x^2+1$	9 39	9 63	(1.14) (1.15)
1999	4	right circulant	no	Rijndael (AES)	[14]	$x^8+x^4+x^3$ $+x+1$	16 40	8 48	(1.12) (1.13)
2000	8	Hadamard	yes	KHAZAD	[4]	$x^8+x^4+x^3$ $+x^2+1$	112	120	(1.8)
2000	4	Hadamard	yes	ANUBIS	[3]	$x^8+x^4+x^3$ $+x^2+1$	16	20	(1.9)

2000	4	Vandermonde	no	ANUBIS key schedule	[3]	$x^8+x^4+x^3$ $+x^2+1$	20 69	32 101	(1.10) (1.11)
2000	4	right circulant	no	Hierocrypt-3, Hierocrypt-L1	[10], [11]	$x^8+x^6+x^5$ $+x+1$	52 52	108 104	(1.16) (1.17)
2000	4	right circulant	no	Hierocrypt-3	[10]	x^4+x+1	32 40	40 44	(1.18) (1.19)
2000	2	—	no	Hierocrypt-L1	[11]	x^4+x+1	8 7	10 11	(1.20) (1.21)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	72 240	88 400	(1.36) (1.50)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	80 288	80 424	(1.37) (1.51)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	72 224	88 360	(1.38) (1.52)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	80 224	72 360	(1.39) (1.53)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	80 240	88 424	(1.40) (1.54)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	88 224	80 424	(1.41) (1.55)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	80 256	88 416	(1.42) (1.56)
2003	8	right circulant	no	Whirlpool (suggestion adopted)	[25]	$x^8+x^4+x^3$ $+x^2+1$	72 224	88 360	(1.43) (1.57)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	80 224	72 360	(1.44) (1.58)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	80 256	88 416	(1.45) (1.59)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	88 224	80 424	(1.46) (1.60)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	80 240	88 424	(1.47) (1.61)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	80 288	80 424	(1.48) (1.62)
2003	8	right circulant	no	suggested by Shirai for Whirlpool-0	[25]	$x^8+x^4+x^3$ $+x^2+1$	72 240	88 400	(1.49) (1.63)
2004	4	—	no	FOX	[17]	$x^8+x^7+x^6+x^5$ $+x^4+x^3+1$	30 72	25 106	(1.22) (1.24)
2004	8	—	no	FOX	[17]	$x^8+x^7+x^6+x^5$ $+x^4+x^3+1$	141 284	169 392	(1.23) (1.25)
2007	3	—	yes	Curupira	[5]	$x^8+x^6+x^3$ $+x^2+1$	12	15	(1.26)
2007	3	right circulant	no	Curupira key schedule	[5]	$x^8+x^6+x^3$ $+x^2+1$	27 30	36 36	(1.27) (1.28)
2009	8	right circulant	no	Grøstl	[15]	$x^8+x^4+x^3$ $+x+1$	104 232	96 376	(1.29) (1.30)

Table 1.2: MDS matrices: parameters, usage and cost

Please note that matrices derived from (1.36) to (1.49) by Shirai and Shibu-

tani are also MDS, although not listed in Table 1.2. See Section 1.6 for further detail on this. Matrix (1.3) and its inverse (1.4) are used in the SHARK [24] cipher.

$$\begin{bmatrix} ce_x & 95_x & 57_x & 82_x & 8a_x & 19_x & b0_x & 01_x \\ e7_x & fe_x & 05_x & d2_x & 52_x & c1_x & 88_x & f1_x \\ b9_x & da_x & 4d_x & d1_x & 9e_x & 17_x & 83_x & 86_x \\ d0_x & 9d_x & 26_x & 2c_x & 5d_x & 9f_x & 6d_x & 75_x \\ 52_x & a9_x & 07_x & 6c_x & b9_x & 8f_x & 70_x & 17_x \\ 87_x & 28_x & 3a_x & 5a_x & f4_x & 33_x & 0b_x & 6c_x \\ 74_x & 51_x & 15_x & cf_x & 09_x & a4_x & 62_x & 09_x \\ 0b_x & 31_x & 7f_x & 86_x & be_x & 05_x & 83_x & 34_x \end{bmatrix} \tag{1.3}$$

$$\begin{bmatrix} e7_x & 30_x & 90_x & 85_x & d0_x & 4b_x & 91_x & 41_x \\ 53_x & 95_x & 9b_x & a5_x & 96_x & bc_x & a1_x & 68_x \\ 02_x & 45_x & f7_x & 65_x & 5c_x & 1f_x & b6_x & 52_x \\ a2_x & ca_x & 22_x & 94_x & 44_x & 63_x & 2a_x & a2_x \\ fc_x & 67_x & 8e_x & 10_x & 29_x & 75_x & 85_x & 71_x \\ 24_x & 45_x & a2_x & cf_x & 2f_x & 22_x & c1_x & 0e_x \\ a1_x & f1_x & 71_x & 40_x & 91_x & 27_x & 18_x & a5_x \\ 56_x & f4_x & af_x & 32_x & d2_x & a4_x & dc_x & 71_x \end{bmatrix} \tag{1.4}$$

Matrix (1.5) and its inverse (1.6) are used in the SQUARE [12] cipher. They are right-circulant.

$$\begin{bmatrix} 02_x & 01_x & 01_x & 03_x \\ 03_x & 02_x & 01_x & 01_x \\ 01_x & 03_x & 02_x & 01_x \\ 01_x & 01_x & 03_x & 02_x \end{bmatrix} \tag{1.5}$$

$$\begin{bmatrix} 0e_x & 09_x & 0d_x & 0b_x \\ 0b_x & 0e_x & 09_x & 0d_x \\ 0d_x & 0b_x & 0e_x & 09_x \\ 09_x & 0d_x & 0b_x & 0e_x \end{bmatrix} \tag{1.6}$$

Matrix (1.7) is involutory, and was obtained by [27] with a Cauchy construction.

$$\begin{bmatrix} 93_x & 13_x & 57_x & da_x & 58_x & 47_x & 0c_x & 1f_x \\ 13_x & 93_x & da_x & 57_x & 47_x & 58_x & 1f_x & 0c_x \\ 57_x & da_x & 93_x & 13_x & 0c_x & 1f_x & 58_x & 47_x \\ da_x & 57_x & 13_x & 93_x & 1f_x & 0c_x & 47_x & 58_x \\ 58_x & 47_x & 0c_x & 1f_x & 93_x & 13_x & 57_x & da_x \\ 47_x & 58_x & 1f_x & 0c_x & 13_x & 93_x & da_x & 57_x \\ 0c_x & 1f_x & 58_x & 47_x & 57_x & da_x & 93_x & 13_x \\ 1f_x & 0c_x & 47_x & 58_x & da_x & 57_x & 13_x & 93_x \end{bmatrix} \tag{1.7}$$

Matrix (1.8) is Hadamard and involutory. It is used in the KHAZAD [4] cipher.

$$\begin{bmatrix} 01_x & 03_x & 04_x & 05_x & 06_x & 08_x & 0b_x & 07_x \\ 03_x & 01_x & 05_x & 04_x & 08_x & 06_x & 07_x & 0b_x \\ 04_x & 05_x & 01_x & 03_x & 0b_x & 07_x & 06_x & 08_x \\ 05_x & 04_x & 03_x & 01_x & 07_x & 0b_x & 08_x & 06_x \\ 06_x & 08_x & 0b_x & 07_x & 01_x & 03_x & 04_x & 05_x \\ 08_x & 06_x & 07_x & 0b_x & 03_x & 01_x & 05_x & 04_x \\ 0b_x & 07_x & 06_x & 08_x & 04_x & 05_x & 01_x & 03_x \\ 07_x & 0b_x & 08_x & 06_x & 05_x & 04_x & 03_x & 01_x \end{bmatrix} \tag{1.8}$$

Matrix (1.9) is Hadamard and involutory. It is used in the ANUBIS [3] cipher.

$$\begin{bmatrix} 01_x & 02_x & 04_x & 06_x \\ 02_x & 01_x & 06_x & 04_x \\ 04_x & 06_x & 01_x & 02_x \\ 06_x & 04_x & 02_x & 01_x \end{bmatrix} \tag{1.9}$$

Still regarding the ANUBIS cipher, while (1.9) is used as its linear transformation layer, (1.10) is used in the key extraction. It is a Vandermonde construction. When $N = 4$, it is an MDS matrix (see Theorem 2). Matrix (1.11) is the inverse of (1.10).

$$\begin{bmatrix} 01_x & 01_x & 01_x & ... & 01_x \\ 01_x & 02_x & 02_x^2 & ... & 02_x^{N-1} \\ 01_x & 06_x & 06_x^2 & ... & 06_x^{N-1} \\ 01_x & 08_x & 08_x^2 & ... & 08_x^{N-1} \end{bmatrix} = \begin{bmatrix} 01_x & 01_x & 01_x & 01_x \\ 01_x & 02_x & 04_x & 08_x \\ 01_x & 06_x & 14_x & 78_x \\ 01_x & 08_x & 40_x & 3a_x \end{bmatrix} \text{ for } N = 4 \tag{1.10}$$

$$\begin{bmatrix} 71_x & 53_x & 7c_x & 5f_x \\ 8c_x & 25_x & c3_x & 6a_x \\ a3_x & ad_x & 71_x & 7f_x \\ 5f_x & db_x & ce_x & 4a_x \end{bmatrix} \tag{1.11}$$

Matrix (1.12) and its inverse (1.13) are used in the Rijndael [14] cipher, which was selected to become AES. They are right-circulant. We show the hexadecimal notation and the corresponding polynomials to emphasize that, albeit stored as integers in cryptographic software implementation, all matrix elements are actually polynomials in a Finite Field. This applies not only to the Rijndael cipher's matrices but to all matrices listed in this work.

$$\begin{bmatrix} 02_x & 03_x & 01_x & 01_x \\ 01_x & 02_x & 03_x & 01_x \\ 01_x & 01_x & 02_x & 03_x \\ 03_x & 01_x & 01_x & 02_x \end{bmatrix} = \begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix} \tag{1.12}$$

$$\begin{bmatrix} 0e_x & 0b_x & 0d_x & 09_x \\ 09_x & 0e_x & 0b_x & 0d_x \\ 0d_x & 09_x & 0e_x & 0b_x \\ 0b_x & 0d_x & 09_x & 0e_x \end{bmatrix} = \begin{bmatrix} x^3+x^2+x & x^3+x+1 & x^3+x^2+1 & x^3+1 \\ x^3+1 & x^3+x^2+x & x^3+x+1 & x^3+x^2+1 \\ x^3+x^2+1 & x^3+1 & x^3+x^2+x & x^3+x+1 \\ x^3+x+1 & x^3+x^2+1 & x^3+1 & x^3+x^2+x \end{bmatrix} \tag{1.13}$$

Furthermore, it is interesting to note that Rijndael's matrix (1.12) is the transpose of SQUARE's matrix (1.5) and this also happens to the inverses (matrix (1.6) is the transpose of (1.13)).

Matrices (1.14) and its inverse (1.15) are used in the BKSQ [13] cipher. They are right-circulant.

$$\begin{bmatrix} 03_x & 02_x & 02_x \\ 02_x & 03_x & 02_x \\ 02_x & 02_x & 03_x \end{bmatrix} \tag{1.14}$$

$$\begin{bmatrix} ac_x & ad_x & ad_x \\ ad_x & ac_x & ad_x \\ ad_x & ad_x & ac_x \end{bmatrix} \tag{1.15}$$

The Hierocrypt-3 cipher makes use of two MDS matrices, one for lower level diffusion and another for higher level diffusion on the cipher, which follows a nested Substitution Permutation Network design (for more detail the reader may refer to [10]). Matrix (1.16) and its inverse (1.17) are used for lower level diffusion. (1.18) and (1.19) (the inverse) are used for higher level diffusion. It is worth noting that, for lower level diffusion, the finite field is $GF(2^8)$, whilst, for higher level diffusion, the authors choose $GF(2^4)$.

$$\begin{bmatrix} c4_x & 65_x & c8_x & 8b_x \\ 8b_x & c4_x & 65_x & c8_x \\ c8_x & 8b_x & c4_x & 65_x \\ 65_x & c8_x & 8b_x & c4_x \end{bmatrix} \tag{1.16}$$

$$\begin{bmatrix} 82_x & c4_x & 34_x & f6_x \\ f6_x & 82_x & c4_x & 34_x \\ 34_x & f6_x & 82_x & c4_x \\ c4_x & 34_x & f6_x & 82_x \end{bmatrix} \tag{1.17}$$

$$\begin{bmatrix} 5_x & 5_x & a_x & e_x \\ e_x & 5_x & 5_x & a_x \\ a_x & e_x & 5_x & 5_x \\ 5_x & a_x & e_x & 5_x \end{bmatrix} \tag{1.18}$$

$$\begin{bmatrix} b_x & e_x & e_x & 6_x \\ 6_x & b_x & e_x & e_x \\ e_x & 6_x & b_x & e_x \\ e_x & e_x & 6_x & b_x \end{bmatrix} \tag{1.19}$$

The Hierocrypt-L1 cipher too uses matrix (1.16) and the inverse (1.17) in its lower diffusion layer. However, for the higher layer, (1.20) and (1.21) (inverse) are used. Analogously to Hierocrypt-3, the higher layer uses $GF(2^4)$.

$$\begin{bmatrix} 5_x & 7_x \\ a_x & b_x \end{bmatrix} \tag{1.20}$$

$$\begin{bmatrix} c_x & a_x \\ 5_x & b_x \end{bmatrix} \tag{1.21}$$

Matrices (1.22) (inverse: (1.24)) and (1.23) (inverse: (1.25)) are used in the FOX block cipher family, with $z = x^7+x^6+x^5+x^4+x^3+x^2+1, a = x+1, b = x^7+x, c = x, d = x^2, e = x^7+x^6+x^5+x^4+x^3+x^2$ and $f = x^6+x^5+x^4+x^3+x^2+x$.

$$\begin{bmatrix} 1 & 1 & 1 & x \\ 1 & z & x & 1 \\ z & x & 1 & 1 \\ x & 1 & z & 1 \end{bmatrix} = \begin{bmatrix} 01_x & 01_x & 01_x & 02_x \\ 01_x & fd_x & 02_x & 01_x \\ fd_x & 02_x & 01_x & 01_x \\ 02_x & 01_x & fd_x & 01_x \end{bmatrix} \tag{1.22}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & a \\ 1 & a & b & c & d & e & f & 1 \\ a & b & c & d & e & f & 1 & 1 \\ b & c & d & e & f & 1 & a & 1 \\ c & d & e & f & 1 & a & b & 1 \\ d & e & f & 1 & a & b & c & 1 \\ e & f & 1 & a & b & c & d & 1 \\ f & 1 & a & b & c & d & e & 1 \end{bmatrix} = \begin{bmatrix} 01_x & 01_x & 01_x & 01_x & 01_x & 01_x & 01_x & 03_x \\ 01_x & 03_x & 82_x & 02_x & 04_x & fc_x & 7e_x & 01_x \\ 03_x & 82_x & 02_x & 04_x & fc_x & 7e_x & 01_x & 01_x \\ 82_x & 02_x & 04_x & fc_x & 7e_x & 01_x & 03_x & 01_x \\ 02_x & 04_x & fc_x & 7e_x & 01_x & 03_x & 82_x & 01_x \\ 04_x & fc_x & 7e_x & 01_x & 03_x & 82_x & 02_x & 01_x \\ fc_x & 7e_x & 01_x & 03_x & 82_x & 02_x & 04_x & 01_x \\ 7e_x & 01_x & 03_x & 82_x & 02_x & 04_x & fc_x & 01_x \end{bmatrix} \tag{1.23}$$

$$\begin{bmatrix} 7e_x & e1_x & ad_x & b0_x \\ 7e_x & ad_x & b0_x & e1_x \\ 7e_x & b0_x & e1_x & ad_x \\ c3_x & 7e_x & 7e_x & 7e_x \end{bmatrix} \tag{1.24}$$

$$\begin{bmatrix} c6_x & fe_x & 3a_x & 73_x & 6d_x & 0c_x & d2_x & b7_x \\ c6_x & 3a_x & 73_x & 6d_x & 0c_x & d2_x & b7_x & fe_x \\ c6_x & 73_x & 6d_x & 0c_x & d2_x & b7_x & fe_x & 3a_x \\ c6_x & 6d_x & 0c_x & d2_x & b7_x & fe_x & 3a_x & 73_x \\ c6_x & 0c_x & d2_x & b7_x & fe_x & 3a_x & 73_x & 6d_x \\ c6_x & d2_x & b7_x & fe_x & 3a_x & 73_x & 6d_x & 0c_x \\ c6_x & b7_x & fe_x & 3a_x & 73_x & 6d_x & 0c_x & d2_x \\ ea_x & c6_x & c6_x & c6_x & c6_x & c6_x & c6_x & c6_x \end{bmatrix} \tag{1.25}$$

Matrix (1.26) is used in Curupira's diffusion layer. It is involutory.

$$\begin{bmatrix} 03_x & 02_x & 02_x \\ 04_x & 05_x & 04_x \\ 06_x & 06_x & 07_x \end{bmatrix} \tag{1.26}$$

Matrix (1.27) is used in Curupira's key scheduling process, with $c(x) = x^4 + x^3 + x^2$.

$$\begin{bmatrix} 1+c(x) & c(x) & c(x) \\ c(x) & 1+c(x) & c(x) \\ c(x) & c(x) & 1+c(x) \end{bmatrix} = \begin{bmatrix} 1d_x & 1c_x & 1c_x \\ 1c_x & 1d_x & 1c_x \\ 1c_x & 1c_x & 1d_x \end{bmatrix} \tag{1.27}$$

Matrix (1.28) is the inverse of (1.27).

$$\begin{bmatrix} 1c_x & 1d_x & 1d_x \\ 1d_x & 1c_x & 1d_x \\ 1d_x & 1d_x & 1c_x \end{bmatrix} \tag{1.28}$$

Matrix (1.29) is used in the Grøstl hash function. It is right-circulant. Its inverse is (1.30).

$$\begin{bmatrix} 02_x & 02_x & 03_x & 04_x & 05_x & 03_x & 05_x & 07_x \\ 07_x & 02_x & 02_x & 03_x & 04_x & 05_x & 03_x & 05_x \\ 05_x & 07_x & 02_x & 02_x & 03_x & 04_x & 05_x & 03_x \\ 03_x & 05_x & 07_x & 02_x & 02_x & 03_x & 04_x & 05_x \\ 05_x & 03_x & 05_x & 07_x & 02_x & 02_x & 03_x & 04_x \\ 04_x & 05_x & 03_x & 05_x & 07_x & 02_x & 02_x & 03_x \\ 03_x & 04_x & 05_x & 03_x & 05_x & 07_x & 02_x & 02_x \\ 02_x & 03_x & 04_x & 05_x & 03_x & 05_x & 07_x & 02_x \end{bmatrix} \tag{1.29}$$

$$\begin{bmatrix} 13_x & 5a_x & 54_x & 72_x & 50_x & df_x & 45_x & 53_x \\ 53_x & 13_x & 5a_x & 54_x & 72_x & 50_x & df_x & 45_x \\ 45_x & 53_x & 13_x & 5a_x & 54_x & 72_x & 50_x & df_x \\ df_x & 45_x & 53_x & 13_x & 5a_x & 54_x & 72_x & 50_x \\ 50_x & df_x & 45_x & 53_x & 13_x & 5a_x & 54_x & 72_x \\ 72_x & 50_x & df_x & 45_x & 53_x & 13_x & 5a_x & 54_x \\ 54_x & 72_x & 50_x & df_x & 45_x & 53_x & 13_x & 5a_x \\ 5a_x & 54_x & 72_x & 50_x & df_x & 45_x & 53_x & 13_x \end{bmatrix} \tag{1.30}$$

1.5 A note on Hierocrypt 3 and Hierocrypt-L1

In the Hierocrypt 3 and Hierocrypt-L1 ciphers, there are two different diffusion layers, referred as low level (mds_l) and high level (MDS_H) by the authors, since these ciphers follow a nested SPN structure (for more details please refer to [10] and [11]). Their high level diffusion layer is called MDS_H and is based on multiplication by matrices (1.18) (for Hierocrypt 3) and (1.20) (for Hierocrypt-L1). They are both MDS, as stated in the design rationale section of the ciphers' specification documents (see [10] and [11]). However, for the implementation, the MDS_H transformation can be equivalently expressed as multiplication by a 16×16 binary matrix (in Hierocrypt-3) which is *not MDS*, but yields the same result. For Hierocrypt-L1, a 8×8 non-MDS matrix is used. In [10], they state

> "$MDS(32,4)$ consists of eight parallel $MDS(4,4)$. When all $MDS(4,4)$ are the same, MDS_H is nothing but the combination of byte-wise XOR's and is expressed as 16×16 matrix."

In [11], they present a similar statement about the 8×8 matrix.

Matrix (1.31) is the binary matrix used for MDS_H in Hierocrypt 3. We can see that it is not MDS, since it has a zero element (see Theorem 2).

$$\begin{bmatrix}
1010101011011111 \\
1101110111100111 \\
1110111011110011 \\
0101010110101110 \\
1111101010101101 \\
0111110111011110 \\
0011111011101111 \\
1110010101011010 \\
1101111110101010 \\
1110011111011101 \\
1111001111101110 \\
1010111001010101 \\
1010110111111010 \\
1101111001111101 \\
1110111100111110 \\
0101101011100101
\end{bmatrix} \tag{1.31}$$

Matrix (1.32) is also not MDS, since it has a zero element. It is used for MDS_H in Hierocrypt L1.

$$\begin{bmatrix}
10101110 \\
11011111 \\
11100111 \\
01011101 \\
11010101 \\
11101010 \\
11111101 \\
10101011
\end{bmatrix} \tag{1.32}$$

1.6 A note on Whirlpool-0

Matrix (1.33) is used in the Whirlpool-0 hash function. The irreducible polynomial of the field is $p(x) = x^8 + x^4 + x^3 + x^2 + 1$, and the inverse matrix is (1.34).

$$\begin{bmatrix} 01_x & 01_x & 03_x & 01_x & 05_x & 08_x & 09_x & 05_x \\ 05_x & 01_x & 01_x & 03_x & 01_x & 05_x & 08_x & 09_x \\ 09_x & 05_x & 01_x & 01_x & 03_x & 01_x & 05_x & 08_x \\ 08_x & 09_x & 05_x & 01_x & 01_x & 03_x & 01_x & 05_x \\ 05_x & 08_x & 09_x & 05_x & 01_x & 01_x & 03_x & 01_x \\ 01_x & 05_x & 08_x & 09_x & 05_x & 01_x & 01_x & 03_x \\ 03_x & 01_x & 05_x & 08_x & 09_x & 05_x & 01_x & 01_x \\ 01_x & 03_x & 01_x & 05_x & 08_x & 09_x & 05_x & 01_x \end{bmatrix} \tag{1.33}$$

$$\begin{bmatrix} a5_x & 07_x & 95_x & 9e_x & 0c_x & a7_x & 01_x & ea_x \\ d1_x & b3_x & e8_x & 5a_x & 01_x & ab_x & 3d_x & 6c_x \\ f8_x & 3c_x & 8a_x & 12_x & 2e_x & 8b_x & cc_x & 5e_x \\ 73_x & 27_x & 4e_x & e0_x & bf_x & c0_x & 24_x & 4a_x \\ 85_x & 17_x & 1c_x & 47_x & 0d_x & 4e_x & 5b_x & aa_x \\ 17_x & b0_x & d6_x & 2d_x & 6c_x & 26_x & ef_x & cb_x \\ dd_x & ce_x & 15_x & da_x & 6c_x & 17_x & 03_x & fc_x \\ ec_x & 78_x & d8_x & ea_x & da_x & 21_x & 17_x & b1_x \end{bmatrix} \tag{1.34}$$

In [26], it is claimed that (1.33) is MDS. However, in [25], Shirai and Shibutani find singular submatrices, which implies that the matrix is, in fact, not MDS. They also present alternative circulant matrices which are MDS.

One of the singular submatrices found in [25] is matrix (1.35). Other singular submatrices were found, for further detail we refer the reader to [25].

$$\begin{bmatrix} 01_x & 05_x \\ 01_x & 05_x \end{bmatrix} \tag{1.35}$$

Furthermore, Shirai and Shibutani obtain 224 MDS matrices satisfying the desired conditions for Whirlpool:

- Branch number equal to 9;
- As many 1-elements as possible (namely, 3);
- Hamming weight of any element is at most 2.

Matrices from (1.36) to (1.49) are the ones obtained by Shirai. They point out that, reversing elements and applying rotations to each of the C_i, it is possible to obtain additional MDS matrices, totalizing thus 224 MDS matrices. For further detail please refer to [25]. The authors of Whirlpool decided to replace the non-MDS matrix by Shirai's C_7 matrix, and therefore Whirlpool-0 refers to the version with the non-MDS matrix, prior to the correction, and Whirlpool refers to the corrected version, with the MDS matrix. For further detail on the history and the updates of Whirlpool, the reader may refer to the Whirlpool web page [1].

$$C_0 = rcirc(01_x, 01_x, 02_x, 01_x, 05_x, 08_x, 09_x, 04_x) \tag{1.36}$$
$$C_1 = rcirc(01_x, 01_x, 02_x, 01_x, 06_x, 09_x, 08_x, 03_x) \tag{1.37}$$
$$C_2 = rcirc(01_x, 01_x, 02_x, 01_x, 08_x, 09_x, 04_x, 05_x) \tag{1.38}$$
$$C_3 = rcirc(01_x, 01_x, 02_x, 01_x, 09_x, 06_x, 04_x, 03_x) \tag{1.39}$$
$$C_4 = rcirc(01_x, 01_x, 02_x, 06_x, 05_x, 09_x, 01_x, 08_x) \tag{1.40}$$
$$C_5 = rcirc(01_x, 01_x, 03_x, 01_x, 04_x, 09_x, 05_x, 06_x) \tag{1.41}$$
$$C_6 = rcirc(01_x, 01_x, 03_x, 01_x, 08_x, 04_x, 09_x, 06_x) \tag{1.42}$$
$$C_7 = rcirc(01_x, 01_x, 04_x, 01_x, 08_x, 05_x, 02_x, 09_x) \tag{1.43}$$
$$C_8 = rcirc(01_x, 01_x, 04_x, 01_x, 09_x, 03_x, 02_x, 06_x) \tag{1.44}$$
$$C_9 = rcirc(01_x, 01_x, 04_x, 03_x, 06_x, 08_x, 01_x, 09_x) \tag{1.45}$$
$$C_{10} = rcirc(01_x, 01_x, 05_x, 01_x, 04_x, 06_x, 03_x, 09_x) \tag{1.46}$$
$$C_{11} = rcirc(01_x, 01_x, 05_x, 08_x, 02_x, 09_x, 01_x, 06_x) \tag{1.47}$$
$$C_{12} = rcirc(01_x, 01_x, 08_x, 01_x, 06_x, 03_x, 02_x, 09_x) \tag{1.48}$$
$$C_{13} = rcirc(01_x, 01_x, 08_x, 02_x, 04_x, 05_x, 01_x, 09_x) \tag{1.49}$$

The inverses of Shirai's matrices from C_0 to C_{13} are the following.

$$C_0^{-1} = rcirc(b5_x, 98_x, 23_x, fa_x, 23_x, a5_x, b6_x, 30_x) \tag{1.50}$$
$$C_1^{-1} = rcirc(bb_x, de_x, a0_x, df_x, 4a_x, 55_x, 7a_x, c5_x) \tag{1.51}$$
$$C_2^{-1} = rcirc(04_x, a4_x, cb_x, af_x, c2_x, 3e_x, 0e_x, c2_x) \tag{1.52}$$
$$C_3^{-1} = rcirc(4f_x, aa_x, 2c_x, 0c_x, 84_x, 76_x, 14_x, bb_x) \tag{1.53}$$
$$C_4^{-1} = rcirc(5b_x, e8_x, ed_x, e2_x, 33_x, 98_x, 82_x, 94_x) \tag{1.54}$$
$$C_5^{-1} = rcirc(87_x, d4_x, 76_x, 80_x, 9d_x, e4_x, 24_x, c5_x) \tag{1.55}$$
$$C_6^{-1} = rcirc(ad_x, ef_x, 44_x, 71_x, a8_x, e2_x, 42_x, 7e_x) \tag{1.56}$$
$$C_7^{-1} = rcirc(04_x, af_x, 0e_x, a4_x, c2_x, c2_x, cb_x, 3e_x) \tag{1.57}$$
$$C_8^{-1} = rcirc(4f_x, 0c_x, 14_x, aa_x, 84_x, bb_x, 2c_x, 76_x) \tag{1.58}$$
$$C_9^{-1} = rcirc(e2_x, 44_x, 7e_x, a8_x, ef_x, 42_x, 71_x, ad_x) \tag{1.59}$$
$$C_{10}^{-1} = rcirc(87_x, 80_x, 24_x, d4_x, 9d_x, c5_x, 76_x, e4_x) \tag{1.60}$$
$$C_{11}^{-1} = rcirc(ed_x, 98_x, 5b_x, e2_x, 82_x, e8_x, 33_x, 94_x) \tag{1.61}$$
$$C_{12}^{-1} = rcirc(bb_x, df_x, 7a_x, de_x, 4a_x, c5_x, a0_x, 55_x) \tag{1.62}$$
$$C_{13}^{-1} = rcirc(a5_x, 23_x, 30_x, 23_x, 98_x, b6_x, fa_x, b5_x) \tag{1.63}$$
$$\tag{1.64}$$

1.7 About Whirlwind and its (possibly) non-MDS matrix

Matrices (1.67) and (1.69) are used in the Whirlwind hash function, with the irreducible polynomial $p(x) = x^4 + x + 1$. The inverses are, respectively, (1.68) and (1.70). In [2], it is claimed that the matrix is MDS. However, in our work, we have found singular submatrices, which leads us to believe, according to Theorem 2, that it is not MDS.

For example, the smallest singular submatrix we have found (matrix (1.65)) for (1.67) is 2×2. It is clear that the determinant is $(x+1)(x^2+x)-x(x^2+1) = x^3 + x^2 + x^2 + x - (x^3 + x) = x^3 + x - x^3 - x = 0$.

$$\begin{bmatrix} 3_x & 5_x \\ 2_x & 6_x \end{bmatrix} = \begin{bmatrix} x+1 & x^2+1 \\ x & x^2+x \end{bmatrix} \tag{1.65}$$

There are too many singular submatrices to list, therefore, we list which rows and columns should be removed from the original matrix in order to obtain them, in Table 1.3. Our row/column index starts at 0 and ends at 7.

Rows to be removed	**Columns to be removed**
(0, 3)	(0, 7)
(0, 3)	(3, 4)
(0, 5)	(0, 7)
(0, 5)	(2, 5)
(0, 6)	(2, 5)
(0, 6)	(3, 4)
(0, 7)	(0, 3)
(0, 7)	(0, 5)
(0, 7)	(2, 4)
(0, 7)	(2, 7)
(0, 7)	(3, 5)
(0, 7)	(4, 7)
(1, 2)	(1, 6)
(1, 2)	(2, 5)
(1, 4)	(1, 6)
(1, 4)	(3, 4)
(1, 6)	(1, 2)
(1, 6)	(1, 4)
(1, 6)	(2, 4)
(1, 6)	(3, 5)
(1, 6)	(3, 6)
(1, 6)	(5, 6)
(1, 7)	(2, 5)
(1, 7)	(3, 4)
(2, 4)	(0, 7)
(2, 4)	(1, 6)
(2, 5)	(0, 5)
(2, 5)	(0, 6)
(2, 5)	(1, 2)
(2, 5)	(1, 7)
(2, 5)	(2, 7)
(2, 5)	(5, 6)

(2, 7)	(0, 7)
(2, 7)	(2, 5)
(3, 4)	(0, 3)
(3, 4)	(0, 6)
(3, 4)	(1, 4)
(3, 4)	(1, 7)
(3, 4)	(3, 6)
(3, 4)	(4, 7)
(3, 5)	(0, 7)
(3, 5)	(1, 6)
(3, 6)	(1, 6)
(3, 6)	(3, 4)
(4, 7)	(0, 7)
(4, 7)	(3, 4)
(5, 6)	(1, 6)
(5, 6)	(2, 5)
(0, 1, 2)	(0, 3, 7)
(0, 1, 2)	(3, 4, 6)
(0, 1, 3)	(1, 2, 6)
(0, 1, 3)	(2, 5, 7)
(0, 1, 4)	(1, 3, 7)
(0, 1, 5)	(0, 2, 6)
(0, 1, 6)	(0, 5, 7)
(0, 1, 6)	(1, 2, 4)
(0, 1, 6)	(3, 5, 6)
(0, 1, 7)	(0, 3, 5)
(0, 1, 7)	(1, 4, 6)
(0, 1, 7)	(2, 4, 7)
(0, 2, 3)	(1, 2, 5)
(0, 2, 3)	(1, 4, 6)
(0, 2, 4)	(1, 2, 4)
(0, 2, 4)	(2, 3, 7)
(0, 2, 5)	(0, 5, 6)
(0, 2, 5)	(1, 2, 7)
(0, 2, 5)	(3, 4, 5)
(0, 2, 5)	(4, 6, 7)
(0, 2, 6)	(0, 1, 5)
(0, 2, 6)	(0, 3, 6)
(0, 2, 7)	(0, 3, 5)
(0, 2, 7)	(1, 6, 7)
(0, 2, 7)	(2, 4, 7)
(0, 2, 7)	(4, 5, 6)
(0, 3, 4)	(0, 3, 6)
(0, 3, 4)	(1, 2, 3)
(0, 3, 4)	(1, 4, 7)
(0, 3, 5)	(0, 1, 7)
(0, 3, 5)	(0, 2, 7)
(0, 3, 5)	(0, 3, 7)
(0, 3, 5)	(0, 4, 7)
(0, 3, 5)	(0, 5, 7)
(0, 3, 5)	(0, 6, 7)
(0, 3, 5)	(1, 3, 5)
(0, 3, 6)	(0, 2, 6)
(0, 3, 6)	(0, 3, 4)

(0, 3, 6)	(1, 3, 4)
(0, 3, 6)	(2, 3, 4)
(0, 3, 6)	(3, 4, 5)
(0, 3, 6)	(3, 4, 6)
(0, 3, 6)	(3, 4, 7)
(0, 3, 7)	(0, 1, 2)
(0, 3, 7)	(0, 3, 5)
(0, 3, 7)	(2, 4, 7)
(0, 4, 5)	(3, 5, 7)
(0, 4, 6)	(0, 5, 6)
(0, 4, 6)	(3, 6, 7)
(0, 4, 7)	(0, 3, 5)
(0, 4, 7)	(2, 4, 7)
(0, 4, 7)	(5, 6, 7)
(0, 5, 6)	(0, 2, 5)
(0, 5, 6)	(0, 4, 6)
(0, 5, 6)	(1, 2, 5)
(0, 5, 6)	(2, 3, 5)
(0, 5, 6)	(2, 4, 5)
(0, 5, 6)	(2, 5, 6)
(0, 5, 6)	(2, 5, 7)
(0, 5, 7)	(0, 1, 6)
(0, 5, 7)	(0, 3, 5)
(0, 5, 7)	(1, 2, 3)
(0, 5, 7)	(2, 4, 7)
(0, 6, 7)	(0, 3, 5)
(0, 6, 7)	(1, 3, 6)
(0, 6, 7)	(2, 4, 7)
(1, 2, 3)	(0, 3, 4)
(1, 2, 3)	(0, 5, 7)
(1, 2, 4)	(0, 1, 6)
(1, 2, 4)	(0, 2, 4)
(1, 2, 4)	(1, 2, 6)
(1, 2, 4)	(1, 3, 6)
(1, 2, 4)	(1, 4, 6)
(1, 2, 4)	(1, 5, 6)
(1, 2, 4)	(1, 6, 7)
(1, 2, 5)	(0, 2, 3)
(1, 2, 5)	(0, 5, 6)
(1, 2, 5)	(1, 2, 7)
(1, 2, 6)	(0, 1, 3)
(1, 2, 6)	(1, 2, 4)
(1, 2, 6)	(3, 5, 6)
(1, 2, 7)	(0, 2, 5)
(1, 2, 7)	(1, 2, 5)
(1, 2, 7)	(1, 3, 7)
(1, 2, 7)	(2, 3, 5)
(1, 2, 7)	(2, 4, 5)
(1, 2, 7)	(2, 5, 6)
(1, 2, 7)	(2, 5, 7)
(1, 3, 4)	(0, 3, 6)
(1, 3, 4)	(1, 4, 7)
(1, 3, 4)	(2, 4, 5)
(1, 3, 4)	(5, 6, 7)

(1, 3, 5)	(0, 3, 5)
(1, 3, 5)	(2, 3, 6)
(1, 3, 6)	(0, 6, 7)
(1, 3, 6)	(1, 2, 4)
(1, 3, 6)	(3, 5, 6)
(1, 3, 6)	(4, 5, 7)
(1, 3, 7)	(0, 1, 4)
(1, 3, 7)	(1, 2, 7)
(1, 4, 5)	(2, 4, 6)
(1, 4, 6)	(0, 1, 7)
(1, 4, 6)	(0, 2, 3)
(1, 4, 6)	(1, 2, 4)
(1, 4, 6)	(3, 5, 6)
(1, 4, 7)	(0, 3, 4)
(1, 4, 7)	(1, 3, 4)
(1, 4, 7)	(1, 5, 7)
(1, 4, 7)	(2, 3, 4)
(1, 4, 7)	(3, 4, 5)
(1, 4, 7)	(3, 4, 6)
(1, 4, 7)	(3, 4, 7)
(1, 5, 6)	(1, 2, 4)
(1, 5, 6)	(3, 5, 6)
(1, 5, 6)	(4, 6, 7)
(1, 5, 7)	(1, 4, 7)
(1, 5, 7)	(2, 6, 7)
(1, 6, 7)	(0, 2, 7)
(1, 6, 7)	(1, 2, 4)
(1, 6, 7)	(3, 5, 6)
(2, 3, 4)	(0, 3, 6)
(2, 3, 4)	(1, 4, 7)
(2, 3, 4)	(2, 5, 7)
(2, 3, 5)	(0, 5, 6)
(2, 3, 5)	(1, 2, 7)
(2, 3, 5)	(3, 4, 6)
(2, 3, 6)	(1, 3, 5)
(2, 3, 7)	(0, 2, 4)
(2, 4, 5)	(0, 5, 6)
(2, 4, 5)	(1, 2, 7)
(2, 4, 5)	(1, 3, 4)
(2, 4, 6)	(1, 4, 5)
(2, 4, 6)	(2, 4, 7)
(2, 4, 7)	(0, 1, 7)
(2, 4, 7)	(0, 2, 7)
(2, 4, 7)	(0, 3, 7)
(2, 4, 7)	(0, 4, 7)
(2, 4, 7)	(0, 5, 7)
(2, 4, 7)	(0, 6, 7)
(2, 4, 7)	(2, 4, 6)
(2, 5, 6)	(0, 5, 6)
(2, 5, 6)	(1, 2, 7)
(2, 5, 6)	(4, 5, 7)
(2, 5, 7)	(0, 1, 3)
(2, 5, 7)	(0, 5, 6)
(2, 5, 7)	(1, 2, 7)

(2, 5, 7)	(2, 3, 4)
(2, 6, 7)	(1, 5, 7)
(3, 4, 5)	(0, 2, 5)
(3, 4, 5)	(0, 3, 6)
(3, 4, 5)	(1, 4, 7)
(3, 4, 6)	(0, 1, 2)
(3, 4, 6)	(0, 3, 6)
(3, 4, 6)	(1, 4, 7)
(3, 4, 6)	(2, 3, 5)
(3, 4, 7)	(0, 3, 6)
(3, 4, 7)	(1, 4, 7)
(3, 4, 7)	(4, 5, 6)
(3, 5, 6)	(0, 1, 6)
(3, 5, 6)	(1, 2, 6)
(3, 5, 6)	(1, 3, 6)
(3, 5, 6)	(1, 4, 6)
(3, 5, 6)	(1, 5, 6)
(3, 5, 6)	(1, 6, 7)
(3, 5, 6)	(3, 5, 7)
(3, 5, 7)	(0, 4, 5)
(3, 5, 7)	(3, 5, 6)
(3, 6, 7)	(0, 4, 6)
(4, 5, 6)	(0, 2, 7)
(4, 5, 6)	(3, 4, 7)
(4, 5, 7)	(1, 3, 6)
(4, 5, 7)	(2, 5, 6)
(4, 6, 7)	(0, 2, 5)
(4, 6, 7)	(1, 5, 6)
(5, 6, 7)	(0, 4, 7)
(5, 6, 7)	(1, 3, 4)
(0, 1, 2, 3)	(0, 3, 5, 6)
(0, 1, 2, 3)	(1, 2, 4, 7)
(0, 1, 2, 4)	(0, 4, 6, 7)
(0, 1, 2, 4)	(2, 4, 5, 6)
(0, 1, 2, 5)	(1, 2, 4, 6)
(0, 1, 2, 5)	(1, 3, 5, 6)
(0, 1, 2, 6)	(0, 4, 5, 6)
(0, 1, 2, 6)	(1, 3, 4, 5)
(0, 1, 2, 6)	(2, 3, 5, 7)
(0, 1, 2, 6)	(2, 4, 6, 7)
(0, 1, 3, 4)	(0, 2, 4, 7)
(0, 1, 3, 4)	(0, 3, 5, 7)
(0, 1, 3, 5)	(1, 5, 6, 7)
(0, 1, 3, 5)	(3, 4, 5, 7)
(0, 1, 3, 7)	(0, 2, 4, 5)
(0, 1, 3, 7)	(1, 4, 5, 7)
(0, 1, 3, 7)	(2, 3, 4, 6)
(0, 1, 3, 7)	(3, 5, 6, 7)
(0, 1, 4, 6)	(1, 2, 3, 5)
(0, 1, 4, 6)	(3, 4, 5, 7)
(0, 1, 4, 7)	(0, 2, 5, 6)
(0, 1, 4, 7)	(0, 3, 6, 7)
(0, 1, 4, 7)	(1, 3, 5, 6)
(0, 1, 5, 6)	(0, 2, 4, 7)

(0, 1, 5, 6)	(1, 2, 6, 7)
(0, 1, 5, 6)	(1, 3, 4, 7)
(0, 1, 5, 7)	(0, 2, 3, 4)
(0, 1, 5, 7)	(2, 4, 5, 6)
(0, 2, 3, 4)	(0, 1, 5, 7)
(0, 2, 3, 4)	(0, 4, 5, 6)
(0, 2, 3, 4)	(1, 3, 6, 7)
(0, 2, 3, 4)	(2, 4, 6, 7)
(0, 2, 3, 6)	(0, 4, 6, 7)
(0, 2, 3, 6)	(2, 4, 5, 6)
(0, 2, 3, 7)	(0, 3, 4, 6)
(0, 2, 3, 7)	(1, 3, 4, 7)
(0, 2, 4, 5)	(0, 1, 3, 7)
(0, 2, 4, 5)	(1, 5, 6, 7)
(0, 2, 4, 6)	(0, 3, 4, 7)
(0, 2, 4, 6)	(1, 2, 5, 6)
(0, 2, 4, 7)	(0, 1, 3, 4)
(0, 2, 4, 7)	(0, 1, 5, 6)
(0, 2, 4, 7)	(2, 3, 5, 6)
(0, 2, 4, 7)	(3, 4, 6, 7)
(0, 2, 5, 6)	(0, 1, 4, 7)
(0, 2, 5, 6)	(1, 2, 3, 6)
(0, 2, 5, 6)	(1, 4, 5, 6)
(0, 2, 5, 6)	(2, 3, 4, 7)
(0, 2, 6, 7)	(1, 2, 3, 5)
(0, 2, 6, 7)	(3, 4, 5, 7)
(0, 3, 4, 5)	(1, 2, 4, 6)
(0, 3, 4, 5)	(1, 2, 5, 7)
(0, 3, 4, 5)	(2, 3, 4, 7)
(0, 3, 4, 6)	(0, 2, 3, 7)
(0, 3, 4, 6)	(0, 4, 5, 7)
(0, 3, 4, 6)	(1, 2, 4, 5)
(0, 3, 4, 6)	(1, 2, 6, 7)
(0, 3, 4, 7)	(0, 2, 4, 6)
(0, 3, 4, 7)	(1, 3, 5, 7)
(0, 3, 5, 6)	(0, 1, 2, 3)
(0, 3, 5, 6)	(4, 5, 6, 7)
(0, 3, 5, 7)	(0, 1, 3, 4)
(0, 3, 5, 7)	(1, 2, 4, 5)
(0, 3, 5, 7)	(1, 2, 6, 7)
(0, 3, 5, 7)	(3, 4, 6, 7)
(0, 3, 6, 7)	(0, 1, 4, 7)
(0, 3, 6, 7)	(1, 2, 4, 6)
(0, 3, 6, 7)	(1, 2, 5, 7)
(0, 4, 5, 6)	(0, 1, 2, 6)
(0, 4, 5, 6)	(0, 2, 3, 4)
(0, 4, 5, 7)	(0, 3, 4, 6)
(0, 4, 5, 7)	(1, 3, 4, 7)
(0, 4, 6, 7)	(0, 1, 2, 4)
(0, 4, 6, 7)	(0, 2, 3, 6)
(0, 4, 6, 7)	(1, 3, 4, 5)
(0, 4, 6, 7)	(2, 3, 5, 7)
(1, 2, 3, 5)	(0, 1, 4, 6)
(1, 2, 3, 5)	(0, 2, 6, 7)

(1, 2, 3, 5)	(1, 4, 5, 7)
(1, 2, 3, 5)	(3, 5, 6, 7)
(1, 2, 3, 6)	(0, 2, 5, 6)
(1, 2, 3, 6)	(1, 2, 5, 7)
(1, 2, 3, 7)	(1, 5, 6, 7)
(1, 2, 3, 7)	(3, 4, 5, 7)
(1, 2, 4, 5)	(0, 3, 4, 6)
(1, 2, 4, 5)	(0, 3, 5, 7)
(1, 2, 4, 5)	(2, 3, 5, 6)
(1, 2, 4, 6)	(0, 1, 2, 5)
(1, 2, 4, 6)	(0, 3, 4, 5)
(1, 2, 4, 6)	(0, 3, 6, 7)
(1, 2, 4, 6)	(2, 5, 6, 7)
(1, 2, 4, 7)	(0, 1, 2, 3)
(1, 2, 4, 7)	(4, 5, 6, 7)
(1, 2, 5, 6)	(0, 2, 4, 6)
(1, 2, 5, 6)	(1, 3, 5, 7)
(1, 2, 5, 7)	(0, 3, 4, 5)
(1, 2, 5, 7)	(0, 3, 6, 7)
(1, 2, 5, 7)	(1, 2, 3, 6)
(1, 2, 5, 7)	(1, 4, 5, 6)
(1, 2, 6, 7)	(0, 1, 5, 6)
(1, 2, 6, 7)	(0, 3, 4, 6)
(1, 2, 6, 7)	(0, 3, 5, 7)
(1, 3, 4, 5)	(0, 1, 2, 6)
(1, 3, 4, 5)	(0, 4, 6, 7)
(1, 3, 4, 7)	(0, 1, 5, 6)
(1, 3, 4, 7)	(0, 2, 3, 7)
(1, 3, 4, 7)	(0, 4, 5, 7)
(1, 3, 4, 7)	(2, 3, 5, 6)
(1, 3, 5, 6)	(0, 1, 2, 5)
(1, 3, 5, 6)	(0, 1, 4, 7)
(1, 3, 5, 6)	(2, 3, 4, 7)
(1, 3, 5, 6)	(2, 5, 6, 7)
(1, 3, 5, 7)	(0, 3, 4, 7)
(1, 3, 5, 7)	(1, 2, 5, 6)
(1, 3, 6, 7)	(0, 2, 3, 4)
(1, 3, 6, 7)	(2, 4, 5, 6)
(1, 4, 5, 6)	(0, 2, 5, 6)
(1, 4, 5, 6)	(1, 2, 5, 7)
(1, 4, 5, 7)	(0, 1, 3, 7)
(1, 4, 5, 7)	(1, 2, 3, 5)
(1, 5, 6, 7)	(0, 1, 3, 5)
(1, 5, 6, 7)	(0, 2, 4, 5)
(1, 5, 6, 7)	(1, 2, 3, 7)
(1, 5, 6, 7)	(2, 3, 4, 6)
(2, 3, 4, 6)	(0, 1, 3, 7)
(2, 3, 4, 6)	(1, 5, 6, 7)
(2, 3, 4, 7)	(0, 2, 5, 6)
(2, 3, 4, 7)	(0, 3, 4, 5)
(2, 3, 4, 7)	(1, 3, 5, 6)
(2, 3, 5, 6)	(0, 2, 4, 7)
(2, 3, 5, 6)	(1, 2, 4, 5)
(2, 3, 5, 6)	(1, 3, 4, 7)

(2, 3, 5, 7)	(0, 1, 2, 6)
(2, 3, 5, 7)	(0, 4, 6, 7)
(2, 4, 5, 6)	(0, 1, 2, 4)
(2, 4, 5, 6)	(0, 1, 5, 7)
(2, 4, 5, 6)	(0, 2, 3, 6)
(2, 4, 5, 6)	(1, 3, 6, 7)
(2, 4, 6, 7)	(0, 1, 2, 6)
(2, 4, 6, 7)	(0, 2, 3, 4)
(2, 5, 6, 7)	(1, 2, 4, 6)
(2, 5, 6, 7)	(1, 3, 5, 6)
(3, 4, 5, 7)	(0, 1, 3, 5)
(3, 4, 5, 7)	(0, 1, 4, 6)
(3, 4, 5, 7)	(0, 2, 6, 7)
(3, 4, 5, 7)	(1, 2, 3, 7)
(3, 4, 6, 7)	(0, 2, 4, 7)
(3, 4, 6, 7)	(0, 3, 5, 7)
(3, 5, 6, 7)	(0, 1, 3, 7)
(3, 5, 6, 7)	(1, 2, 3, 5)
(4, 5, 6, 7)	(0, 3, 5, 6)
(4, 5, 6, 7)	(1, 2, 4, 7)
(0, 1, 2, 3, 4)	(0, 2, 5, 6, 7)
(0, 1, 2, 3, 4)	(1, 2, 3, 5, 6)
(0, 1, 2, 3, 5)	(0, 2, 3, 4, 7)
(0, 1, 2, 3, 5)	(1, 3, 4, 6, 7)
(0, 1, 2, 3, 6)	(0, 1, 3, 4, 7)
(0, 1, 2, 3, 6)	(0, 2, 4, 5, 7)
(0, 1, 2, 3, 7)	(0, 1, 2, 5, 6)
(0, 1, 2, 3, 7)	(1, 3, 4, 5, 6)
(0, 1, 2, 4, 5)	(1, 2, 3, 5, 7)
(0, 1, 2, 4, 6)	(0, 1, 2, 4, 7)
(0, 1, 2, 4, 6)	(1, 2, 3, 6, 7)
(0, 1, 2, 4, 7)	(0, 1, 2, 4, 6)
(0, 1, 2, 4, 7)	(0, 2, 3, 4, 5)
(0, 1, 2, 4, 7)	(0, 2, 3, 4, 7)
(0, 1, 2, 4, 7)	(0, 2, 3, 5, 7)
(0, 1, 2, 4, 7)	(0, 2, 4, 5, 7)
(0, 1, 2, 4, 7)	(0, 3, 4, 5, 7)
(0, 1, 2, 4, 7)	(2, 3, 4, 5, 7)
(0, 1, 2, 5, 6)	(0, 1, 2, 3, 7)
(0, 1, 2, 5, 6)	(0, 2, 3, 5, 6)
(0, 1, 2, 5, 6)	(1, 2, 4, 5, 7)
(0, 1, 2, 5, 7)	(0, 1, 4, 6, 7)
(0, 1, 2, 5, 7)	(0, 2, 3, 5, 6)
(0, 1, 2, 5, 7)	(1, 2, 4, 5, 7)
(0, 1, 2, 5, 7)	(3, 4, 5, 6, 7)
(0, 1, 2, 6, 7)	(0, 2, 3, 5, 6)
(0, 1, 2, 6, 7)	(1, 2, 4, 5, 7)
(0, 1, 2, 6, 7)	(1, 3, 4, 6, 7)
(0, 1, 3, 4, 5)	(0, 2, 3, 4, 6)
(0, 1, 3, 4, 6)	(0, 1, 5, 6, 7)
(0, 1, 3, 4, 6)	(0, 3, 4, 5, 6)
(0, 1, 3, 4, 6)	(1, 2, 3, 4, 7)
(0, 1, 3, 4, 6)	(2, 4, 5, 6, 7)
(0, 1, 3, 4, 7)	(0, 1, 2, 3, 6)

(0, 1, 3, 4, 7)	(0, 3, 4, 5, 6)
(0, 1, 3, 4, 7)	(1, 2, 3, 4, 7)
(0, 1, 3, 5, 6)	(0, 1, 3, 5, 7)
(0, 1, 3, 5, 6)	(1, 2, 3, 4, 5)
(0, 1, 3, 5, 6)	(1, 2, 3, 4, 6)
(0, 1, 3, 5, 6)	(1, 2, 3, 5, 6)
(0, 1, 3, 5, 6)	(1, 2, 4, 5, 6)
(0, 1, 3, 5, 6)	(1, 3, 4, 5, 6)
(0, 1, 3, 5, 6)	(2, 3, 4, 5, 6)
(0, 1, 3, 5, 7)	(0, 1, 3, 5, 6)
(0, 1, 3, 5, 7)	(0, 2, 3, 6, 7)
(0, 1, 3, 6, 7)	(0, 2, 5, 6, 7)
(0, 1, 3, 6, 7)	(0, 3, 4, 5, 6)
(0, 1, 3, 6, 7)	(1, 2, 3, 4, 7)
(0, 1, 4, 5, 6)	(1, 3, 5, 6, 7)
(0, 1, 4, 5, 7)	(0, 2, 4, 6, 7)
(0, 1, 4, 6, 7)	(0, 1, 2, 5, 7)
(0, 1, 4, 6, 7)	(0, 3, 4, 5, 6)
(0, 1, 4, 6, 7)	(1, 2, 3, 4, 7)
(0, 1, 5, 6, 7)	(0, 1, 3, 4, 6)
(0, 1, 5, 6, 7)	(0, 2, 3, 5, 6)
(0, 1, 5, 6, 7)	(1, 2, 4, 5, 7)
(0, 2, 3, 4, 5)	(0, 1, 2, 4, 7)
(0, 2, 3, 4, 5)	(0, 3, 5, 6, 7)
(0, 2, 3, 4, 5)	(1, 3, 4, 5, 6)
(0, 2, 3, 4, 6)	(0, 1, 3, 4, 5)
(0, 2, 3, 4, 6)	(0, 2, 3, 5, 6)
(0, 2, 3, 4, 7)	(0, 1, 2, 3, 5)
(0, 2, 3, 4, 7)	(0, 1, 2, 4, 7)
(0, 2, 3, 4, 7)	(0, 3, 5, 6, 7)
(0, 2, 3, 5, 6)	(0, 1, 2, 5, 6)
(0, 2, 3, 5, 6)	(0, 1, 2, 5, 7)
(0, 2, 3, 5, 6)	(0, 1, 2, 6, 7)
(0, 2, 3, 5, 6)	(0, 1, 5, 6, 7)
(0, 2, 3, 5, 6)	(0, 2, 3, 4, 6)
(0, 2, 3, 5, 6)	(0, 2, 5, 6, 7)
(0, 2, 3, 5, 6)	(1, 2, 5, 6, 7)
(0, 2, 3, 5, 7)	(0, 1, 2, 4, 7)
(0, 2, 3, 5, 7)	(0, 3, 5, 6, 7)
(0, 2, 3, 5, 7)	(1, 4, 5, 6, 7)
(0, 2, 3, 5, 7)	(2, 3, 4, 5, 6)
(0, 2, 3, 6, 7)	(0, 1, 3, 5, 7)
(0, 2, 4, 5, 6)	(0, 3, 4, 5, 6)
(0, 2, 4, 5, 6)	(2, 3, 5, 6, 7)
(0, 2, 4, 5, 7)	(0, 1, 2, 3, 6)
(0, 2, 4, 5, 7)	(0, 1, 2, 4, 7)
(0, 2, 4, 5, 7)	(0, 3, 5, 6, 7)
(0, 2, 4, 5, 7)	(1, 2, 3, 4, 5)
(0, 2, 4, 6, 7)	(0, 1, 4, 5, 7)
(0, 2, 4, 6, 7)	(1, 2, 4, 6, 7)
(0, 2, 5, 6, 7)	(0, 1, 2, 3, 4)
(0, 2, 5, 6, 7)	(0, 1, 3, 6, 7)
(0, 2, 5, 6, 7)	(0, 2, 3, 5, 6)
(0, 2, 5, 6, 7)	(1, 2, 4, 5, 7)

(0, 3, 4, 5, 6)	(0, 1, 3, 4, 6)
(0, 3, 4, 5, 6)	(0, 1, 3, 4, 7)
(0, 3, 4, 5, 6)	(0, 1, 3, 6, 7)
(0, 3, 4, 5, 6)	(0, 1, 4, 6, 7)
(0, 3, 4, 5, 6)	(0, 2, 4, 5, 6)
(0, 3, 4, 5, 6)	(0, 3, 4, 6, 7)
(0, 3, 4, 5, 6)	(1, 3, 4, 6, 7)
(0, 3, 4, 5, 7)	(0, 1, 2, 4, 7)
(0, 3, 4, 5, 7)	(0, 3, 5, 6, 7)
(0, 3, 4, 5, 7)	(2, 4, 5, 6, 7)
(0, 3, 4, 6, 7)	(0, 3, 4, 5, 6)
(0, 3, 4, 6, 7)	(1, 2, 3, 4, 7)
(0, 3, 4, 6, 7)	(1, 4, 5, 6, 7)
(0, 3, 5, 6, 7)	(0, 2, 3, 4, 5)
(0, 3, 5, 6, 7)	(0, 2, 3, 4, 7)
(0, 3, 5, 6, 7)	(0, 2, 3, 5, 7)
(0, 3, 5, 6, 7)	(0, 2, 4, 5, 7)
(0, 3, 5, 6, 7)	(0, 3, 4, 5, 7)
(0, 3, 5, 6, 7)	(1, 3, 5, 6, 7)
(0, 3, 5, 6, 7)	(2, 3, 4, 5, 7)
(0, 4, 5, 6, 7)	(1, 2, 3, 4, 6)
(0, 4, 5, 6, 7)	(1, 2, 5, 6, 7)
(1, 2, 3, 4, 5)	(0, 1, 3, 5, 6)
(1, 2, 3, 4, 5)	(0, 2, 4, 5, 7)
(1, 2, 3, 4, 5)	(1, 2, 4, 6, 7)
(1, 2, 3, 4, 6)	(0, 1, 3, 5, 6)
(1, 2, 3, 4, 6)	(0, 4, 5, 6, 7)
(1, 2, 3, 4, 6)	(1, 2, 4, 6, 7)
(1, 2, 3, 4, 6)	(2, 3, 4, 5, 7)
(1, 2, 3, 4, 7)	(0, 1, 3, 4, 6)
(1, 2, 3, 4, 7)	(0, 1, 3, 4, 7)
(1, 2, 3, 4, 7)	(0, 1, 3, 6, 7)
(1, 2, 3, 4, 7)	(0, 1, 4, 6, 7)
(1, 2, 3, 4, 7)	(0, 3, 4, 6, 7)
(1, 2, 3, 4, 7)	(1, 2, 3, 5, 7)
(1, 2, 3, 4, 7)	(1, 3, 4, 6, 7)
(1, 2, 3, 5, 6)	(0, 1, 2, 3, 4)
(1, 2, 3, 5, 6)	(0, 1, 3, 5, 6)
(1, 2, 3, 5, 6)	(1, 2, 4, 6, 7)
(1, 2, 3, 5, 7)	(0, 1, 2, 4, 5)
(1, 2, 3, 5, 7)	(1, 2, 3, 4, 7)
(1, 2, 3, 6, 7)	(0, 1, 2, 4, 6)
(1, 2, 4, 5, 6)	(0, 1, 3, 5, 6)
(1, 2, 4, 5, 6)	(1, 2, 4, 6, 7)
(1, 2, 4, 5, 6)	(3, 4, 5, 6, 7)
(1, 2, 4, 5, 7)	(0, 1, 2, 5, 6)
(1, 2, 4, 5, 7)	(0, 1, 2, 5, 7)
(1, 2, 4, 5, 7)	(0, 1, 2, 6, 7)
(1, 2, 4, 5, 7)	(0, 1, 5, 6, 7)
(1, 2, 4, 5, 7)	(0, 2, 5, 6, 7)
(1, 2, 4, 5, 7)	(1, 2, 5, 6, 7)
(1, 2, 4, 5, 7)	(1, 3, 4, 5, 7)
(1, 2, 4, 6, 7)	(0, 2, 4, 6, 7)
(1, 2, 4, 6, 7)	(1, 2, 3, 4, 5)

(1, 2, 4, 6, 7)	(1, 2, 3, 4, 6)
(1, 2, 4, 6, 7)	(1, 2, 3, 5, 6)
(1, 2, 4, 6, 7)	(1, 2, 4, 5, 6)
(1, 2, 4, 6, 7)	(1, 3, 4, 5, 6)
(1, 2, 4, 6, 7)	(2, 3, 4, 5, 6)
(1, 2, 5, 6, 7)	(0, 2, 3, 5, 6)
(1, 2, 5, 6, 7)	(0, 4, 5, 6, 7)
(1, 2, 5, 6, 7)	(1, 2, 4, 5, 7)
(1, 3, 4, 5, 6)	(0, 1, 2, 3, 7)
(1, 3, 4, 5, 6)	(0, 1, 3, 5, 6)
(1, 3, 4, 5, 6)	(0, 2, 3, 4, 5)
(1, 3, 4, 5, 6)	(1, 2, 4, 6, 7)
(1, 3, 4, 5, 7)	(1, 2, 4, 5, 7)
(1, 3, 4, 5, 7)	(2, 3, 4, 6, 7)
(1, 3, 4, 6, 7)	(0, 1, 2, 3, 5)
(1, 3, 4, 6, 7)	(0, 1, 2, 6, 7)
(1, 3, 4, 6, 7)	(0, 3, 4, 5, 6)
(1, 3, 4, 6, 7)	(1, 2, 3, 4, 7)
(1, 3, 5, 6, 7)	(0, 1, 4, 5, 6)
(1, 3, 5, 6, 7)	(0, 3, 5, 6, 7)
(1, 4, 5, 6, 7)	(0, 2, 3, 5, 7)
(1, 4, 5, 6, 7)	(0, 3, 4, 6, 7)
(2, 3, 4, 5, 6)	(0, 1, 3, 5, 6)
(2, 3, 4, 5, 6)	(0, 2, 3, 5, 7)
(2, 3, 4, 5, 6)	(1, 2, 4, 6, 7)
(2, 3, 4, 5, 7)	(0, 1, 2, 4, 7)
(2, 3, 4, 5, 7)	(0, 3, 5, 6, 7)
(2, 3, 4, 5, 7)	(1, 2, 3, 4, 6)
(2, 3, 4, 6, 7)	(1, 3, 4, 5, 7)
(2, 3, 5, 6, 7)	(0, 2, 4, 5, 6)
(2, 4, 5, 6, 7)	(0, 1, 3, 4, 6)
(2, 4, 5, 6, 7)	(0, 3, 4, 5, 7)
(3, 4, 5, 6, 7)	(0, 1, 2, 5, 7)
(3, 4, 5, 6, 7)	(1, 2, 4, 5, 6)
(0, 1, 2, 3, 4, 7)	(0, 1, 3, 4, 6, 7)
(0, 1, 2, 3, 4, 7)	(0, 2, 3, 4, 5, 7)
(0, 1, 2, 3, 5, 6)	(0, 1, 2, 5, 6, 7)
(0, 1, 2, 3, 5, 6)	(1, 2, 3, 4, 5, 6)
(0, 1, 2, 4, 5, 7)	(0, 1, 2, 5, 6, 7)
(0, 1, 2, 4, 5, 7)	(0, 2, 3, 4, 5, 7)
(0, 1, 2, 4, 6, 7)	(0, 2, 3, 4, 5, 7)
(0, 1, 2, 4, 6, 7)	(1, 2, 3, 4, 5, 6)
(0, 1, 2, 5, 6, 7)	(0, 1, 2, 3, 5, 6)
(0, 1, 2, 5, 6, 7)	(0, 1, 2, 4, 5, 7)
(0, 1, 2, 5, 6, 7)	(0, 2, 3, 4, 5, 6)
(0, 1, 2, 5, 6, 7)	(0, 2, 3, 5, 6, 7)
(0, 1, 2, 5, 6, 7)	(1, 2, 3, 4, 5, 7)
(0, 1, 2, 5, 6, 7)	(1, 2, 4, 5, 6, 7)
(0, 1, 3, 4, 5, 6)	(0, 1, 3, 4, 6, 7)
(0, 1, 3, 4, 5, 6)	(1, 2, 3, 4, 5, 6)
(0, 1, 3, 4, 6, 7)	(0, 1, 2, 3, 4, 7)
(0, 1, 3, 4, 6, 7)	(0, 1, 3, 4, 5, 6)
(0, 1, 3, 4, 6, 7)	(0, 2, 3, 4, 5, 6)
(0, 1, 3, 4, 6, 7)	(0, 3, 4, 5, 6, 7)

(0, 1, 3, 4, 6, 7)	(1, 2, 3, 4, 5, 7)
(0, 1, 3, 4, 6, 7)	(1, 2, 3, 4, 6, 7)
(0, 1, 3, 5, 6, 7)	(0, 2, 3, 4, 5, 7)
(0, 1, 3, 5, 6, 7)	(1, 2, 3, 4, 5, 6)
(0, 2, 3, 4, 5, 6)	(0, 1, 2, 5, 6, 7)
(0, 2, 3, 4, 5, 6)	(0, 1, 3, 4, 6, 7)
(0, 2, 3, 4, 5, 7)	(0, 1, 2, 3, 4, 7)
(0, 2, 3, 4, 5, 7)	(0, 1, 2, 4, 5, 7)
(0, 2, 3, 4, 5, 7)	(0, 1, 2, 4, 6, 7)
(0, 2, 3, 4, 5, 7)	(0, 1, 3, 5, 6, 7)
(0, 2, 3, 4, 5, 7)	(0, 2, 3, 5, 6, 7)
(0, 2, 3, 4, 5, 7)	(0, 3, 4, 5, 6, 7)
(0, 2, 3, 5, 6, 7)	(0, 1, 2, 5, 6, 7)
(0, 2, 3, 5, 6, 7)	(0, 2, 3, 4, 5, 7)
(0, 3, 4, 5, 6, 7)	(0, 1, 3, 4, 6, 7)
(0, 3, 4, 5, 6, 7)	(0, 2, 3, 4, 5, 7)
(1, 2, 3, 4, 5, 6)	(0, 1, 2, 3, 5, 6)
(1, 2, 3, 4, 5, 6)	(0, 1, 2, 4, 6, 7)
(1, 2, 3, 4, 5, 6)	(0, 1, 3, 4, 5, 6)
(1, 2, 3, 4, 5, 6)	(0, 1, 3, 5, 6, 7)
(1, 2, 3, 4, 5, 6)	(1, 2, 3, 4, 6, 7)
(1, 2, 3, 4, 5, 6)	(1, 2, 4, 5, 6, 7)
(1, 2, 3, 4, 5, 7)	(0, 1, 2, 5, 6, 7)
(1, 2, 3, 4, 5, 7)	(0, 1, 3, 4, 6, 7)
(1, 2, 3, 4, 6, 7)	(0, 1, 3, 4, 6, 7)
(1, 2, 3, 4, 6, 7)	(1, 2, 3, 4, 5, 6)
(1, 2, 4, 5, 6, 7)	(0, 1, 2, 5, 6, 7)
(1, 2, 4, 5, 6, 7)	(1, 2, 3, 4, 5, 6)

Table 1.3: Whirlwind m_0 (1.67) singular submatrices

For (1.69), an example of singular submatrix is (1.66), and the list of rows and columns to be removed to yield all singular submatrices is given by Table 1.4.

$$\begin{bmatrix} 8_x & 7_x \\ 3_x & e_x \end{bmatrix} = \begin{bmatrix} x^3 & x^2+x+1 \\ x+1 & x^3+x^2+x \end{bmatrix} \tag{1.66}$$

Rows to be removed	**Columns to be removed**
(0, 2)	(1, 5)
(0, 2)	(3, 7)
(0, 4)	(0, 5)
(0, 4)	(0, 7)
(0, 4)	(1, 3)
(0, 4)	(1, 4)
(0, 4)	(3, 4)
(0, 4)	(5, 7)
(0, 5)	(0, 4)
(0, 5)	(1, 5)
(0, 7)	(0, 4)
(0, 7)	(3, 7)
(1, 3)	(0, 4)

(1, 3)	(2, 6)
(1, 4)	(0, 4)
(1, 4)	(1, 5)
(1, 5)	(0, 2)
(1, 5)	(0, 5)
(1, 5)	(1, 4)
(1, 5)	(1, 6)
(1, 5)	(2, 5)
(1, 5)	(4, 6)
(1, 6)	(1, 5)
(1, 6)	(2, 6)
(2, 5)	(1, 5)
(2, 5)	(2, 6)
(2, 6)	(1, 3)
(2, 6)	(1, 6)
(2, 6)	(2, 5)
(2, 6)	(2, 7)
(2, 6)	(3, 6)
(2, 6)	(5, 7)
(2, 7)	(2, 6)
(2, 7)	(3, 7)
(3, 4)	(0, 4)
(3, 4)	(3, 7)
(3, 6)	(2, 6)
(3, 6)	(3, 7)
(3, 7)	(0, 2)
(3, 7)	(0, 7)
(3, 7)	(2, 7)
(3, 7)	(3, 4)
(3, 7)	(3, 6)
(3, 7)	(4, 6)
(4, 6)	(1, 5)
(4, 6)	(3, 7)
(5, 7)	(0, 4)
(5, 7)	(2, 6)
(0, 1, 2)	(0, 3, 5)
(0, 1, 2)	(0, 3, 6)
(0, 1, 2)	(0, 5, 6)
(0, 1, 2)	(1, 2, 4)
(0, 1, 2)	(1, 2, 7)
(0, 1, 2)	(1, 4, 7)
(0, 1, 2)	(2, 4, 7)
(0, 1, 2)	(3, 5, 6)
(0, 1, 3)	(0, 3, 5)
(0, 1, 3)	(0, 3, 6)
(0, 1, 3)	(0, 5, 6)
(0, 1, 3)	(1, 2, 4)
(0, 1, 3)	(1, 2, 7)
(0, 1, 3)	(1, 4, 7)
(0, 1, 3)	(2, 4, 7)
(0, 1, 3)	(3, 5, 6)
(0, 1, 4)	(0, 5, 7)
(0, 1, 4)	(1, 3, 4)
(0, 1, 5)	(0, 2, 5)

(0, 1, 5)	(1, 4, 6)
(0, 1, 6)	(3, 5, 7)
(0, 1, 7)	(2, 4, 6)
(0, 2, 3)	(0, 3, 5)
(0, 2, 3)	(0, 3, 6)
(0, 2, 3)	(0, 5, 6)
(0, 2, 3)	(1, 2, 4)
(0, 2, 3)	(1, 2, 7)
(0, 2, 3)	(1, 4, 7)
(0, 2, 3)	(2, 4, 7)
(0, 2, 3)	(3, 5, 6)
(0, 2, 4)	(0, 5, 7)
(0, 2, 4)	(1, 3, 4)
(0, 2, 4)	(1, 6, 7)
(0, 2, 4)	(2, 5, 6)
(0, 2, 5)	(0, 1, 5)
(0, 2, 5)	(1, 2, 5)
(0, 2, 5)	(1, 3, 5)
(0, 2, 5)	(1, 4, 5)
(0, 2, 5)	(1, 5, 6)
(0, 2, 5)	(1, 5, 7)
(0, 2, 6)	(0, 4, 7)
(0, 2, 6)	(1, 3, 6)
(0, 2, 6)	(2, 5, 7)
(0, 2, 6)	(3, 4, 5)
(0, 2, 7)	(0, 3, 7)
(0, 2, 7)	(1, 3, 7)
(0, 2, 7)	(2, 3, 7)
(0, 2, 7)	(3, 4, 7)
(0, 2, 7)	(3, 5, 7)
(0, 2, 7)	(3, 6, 7)
(0, 3, 4)	(0, 5, 7)
(0, 3, 4)	(1, 3, 4)
(0, 3, 4)	(2, 4, 6)
(0, 3, 5)	(0, 1, 2)
(0, 3, 5)	(0, 1, 3)
(0, 3, 5)	(0, 2, 3)
(0, 3, 5)	(1, 2, 3)
(0, 3, 5)	(4, 5, 6)
(0, 3, 5)	(4, 5, 7)
(0, 3, 5)	(4, 6, 7)
(0, 3, 5)	(5, 6, 7)
(0, 3, 6)	(0, 1, 2)
(0, 3, 6)	(0, 1, 3)
(0, 3, 6)	(0, 2, 3)
(0, 3, 6)	(1, 2, 3)
(0, 3, 6)	(4, 5, 6)
(0, 3, 6)	(4, 5, 7)
(0, 3, 6)	(4, 6, 7)
(0, 3, 6)	(5, 6, 7)
(0, 3, 7)	(0, 2, 7)
(0, 3, 7)	(1, 5, 7)
(0, 3, 7)	(3, 4, 6)
(0, 4, 5)	(0, 5, 7)

(0, 4, 5)	(1, 3, 4)
(0, 4, 6)	(0, 5, 7)
(0, 4, 6)	(1, 2, 6)
(0, 4, 6)	(1, 3, 4)
(0, 4, 6)	(2, 3, 5)
(0, 4, 7)	(0, 2, 6)
(0, 4, 7)	(0, 5, 7)
(0, 4, 7)	(1, 3, 4)
(0, 5, 6)	(0, 1, 2)
(0, 5, 6)	(0, 1, 3)
(0, 5, 6)	(0, 2, 3)
(0, 5, 6)	(1, 2, 3)
(0, 5, 6)	(4, 5, 6)
(0, 5, 6)	(4, 5, 7)
(0, 5, 6)	(4, 6, 7)
(0, 5, 6)	(5, 6, 7)
(0, 5, 7)	(0, 1, 4)
(0, 5, 7)	(0, 2, 4)
(0, 5, 7)	(0, 3, 4)
(0, 5, 7)	(0, 4, 5)
(0, 5, 7)	(0, 4, 6)
(0, 5, 7)	(0, 4, 7)
(0, 6, 7)	(1, 3, 5)
(1, 2, 3)	(0, 3, 5)
(1, 2, 3)	(0, 3, 6)
(1, 2, 3)	(0, 5, 6)
(1, 2, 3)	(1, 2, 4)
(1, 2, 3)	(1, 2, 7)
(1, 2, 3)	(1, 4, 7)
(1, 2, 3)	(2, 4, 7)
(1, 2, 3)	(3, 5, 6)
(1, 2, 4)	(0, 1, 2)
(1, 2, 4)	(0, 1, 3)
(1, 2, 4)	(0, 2, 3)
(1, 2, 4)	(1, 2, 3)
(1, 2, 4)	(4, 5, 6)
(1, 2, 4)	(4, 5, 7)
(1, 2, 4)	(4, 6, 7)
(1, 2, 4)	(5, 6, 7)
(1, 2, 5)	(0, 2, 5)
(1, 2, 5)	(1, 4, 6)
(1, 2, 5)	(3, 5, 7)
(1, 2, 6)	(0, 4, 6)
(1, 2, 6)	(1, 3, 6)
(1, 2, 6)	(2, 5, 7)
(1, 2, 7)	(0, 1, 2)
(1, 2, 7)	(0, 1, 3)
(1, 2, 7)	(0, 2, 3)
(1, 2, 7)	(1, 2, 3)
(1, 2, 7)	(4, 5, 6)
(1, 2, 7)	(4, 5, 7)
(1, 2, 7)	(4, 6, 7)
(1, 2, 7)	(5, 6, 7)
(1, 3, 4)	(0, 1, 4)

(1, 3, 4)	(0, 2, 4)
(1, 3, 4)	(0, 3, 4)
(1, 3, 4)	(0, 4, 5)
(1, 3, 4)	(0, 4, 6)
(1, 3, 4)	(0, 4, 7)
(1, 3, 5)	(0, 2, 5)
(1, 3, 5)	(0, 6, 7)
(1, 3, 5)	(1, 4, 6)
(1, 3, 5)	(3, 4, 7)
(1, 3, 6)	(0, 2, 6)
(1, 3, 6)	(1, 2, 6)
(1, 3, 6)	(2, 3, 6)
(1, 3, 6)	(2, 4, 6)
(1, 3, 6)	(2, 5, 6)
(1, 3, 6)	(2, 6, 7)
(1, 3, 7)	(0, 2, 7)
(1, 3, 7)	(1, 5, 6)
(1, 3, 7)	(2, 4, 5)
(1, 3, 7)	(3, 4, 6)
(1, 4, 5)	(0, 2, 5)
(1, 4, 5)	(1, 4, 6)
(1, 4, 6)	(0, 1, 5)
(1, 4, 6)	(1, 2, 5)
(1, 4, 6)	(1, 3, 5)
(1, 4, 6)	(1, 4, 5)
(1, 4, 6)	(1, 5, 6)
(1, 4, 6)	(1, 5, 7)
(1, 4, 7)	(0, 1, 2)
(1, 4, 7)	(0, 1, 3)
(1, 4, 7)	(0, 2, 3)
(1, 4, 7)	(1, 2, 3)
(1, 4, 7)	(4, 5, 6)
(1, 4, 7)	(4, 5, 7)
(1, 4, 7)	(4, 6, 7)
(1, 4, 7)	(5, 6, 7)
(1, 5, 6)	(0, 2, 5)
(1, 5, 6)	(1, 3, 7)
(1, 5, 6)	(1, 4, 6)
(1, 5, 7)	(0, 2, 5)
(1, 5, 7)	(0, 3, 7)
(1, 5, 7)	(1, 4, 6)
(1, 5, 7)	(2, 3, 4)
(1, 6, 7)	(0, 2, 4)
(2, 3, 4)	(1, 5, 7)
(2, 3, 5)	(0, 4, 6)
(2, 3, 6)	(1, 3, 6)
(2, 3, 6)	(2, 5, 7)
(2, 3, 7)	(0, 2, 7)
(2, 3, 7)	(3, 4, 6)
(2, 4, 5)	(1, 3, 7)
(2, 4, 6)	(0, 1, 7)
(2, 4, 6)	(0, 3, 4)
(2, 4, 6)	(1, 3, 6)
(2, 4, 6)	(2, 5, 7)

(2, 4, 7)	(0, 1, 2)
(2, 4, 7)	(0, 1, 3)
(2, 4, 7)	(0, 2, 3)
(2, 4, 7)	(1, 2, 3)
(2, 4, 7)	(4, 5, 6)
(2, 4, 7)	(4, 5, 7)
(2, 4, 7)	(4, 6, 7)
(2, 4, 7)	(5, 6, 7)
(2, 5, 6)	(0, 2, 4)
(2, 5, 6)	(1, 3, 6)
(2, 5, 6)	(2, 5, 7)
(2, 5, 7)	(0, 2, 6)
(2, 5, 7)	(1, 2, 6)
(2, 5, 7)	(2, 3, 6)
(2, 5, 7)	(2, 4, 6)
(2, 5, 7)	(2, 5, 6)
(2, 5, 7)	(2, 6, 7)
(2, 6, 7)	(1, 3, 6)
(2, 6, 7)	(2, 5, 7)
(3, 4, 5)	(0, 2, 6)
(3, 4, 6)	(0, 3, 7)
(3, 4, 6)	(1, 3, 7)
(3, 4, 6)	(2, 3, 7)
(3, 4, 6)	(3, 4, 7)
(3, 4, 6)	(3, 5, 7)
(3, 4, 6)	(3, 6, 7)
(3, 4, 7)	(0, 2, 7)
(3, 4, 7)	(1, 3, 5)
(3, 4, 7)	(3, 4, 6)
(3, 5, 6)	(0, 1, 2)
(3, 5, 6)	(0, 1, 3)
(3, 5, 6)	(0, 2, 3)
(3, 5, 6)	(1, 2, 3)
(3, 5, 6)	(4, 5, 6)
(3, 5, 6)	(4, 5, 7)
(3, 5, 6)	(4, 6, 7)
(3, 5, 6)	(5, 6, 7)
(3, 5, 7)	(0, 1, 6)
(3, 5, 7)	(0, 2, 7)
(3, 5, 7)	(1, 2, 5)
(3, 5, 7)	(3, 4, 6)
(3, 6, 7)	(0, 2, 7)
(3, 6, 7)	(3, 4, 6)
(4, 5, 6)	(0, 3, 5)
(4, 5, 6)	(0, 3, 6)
(4, 5, 6)	(0, 5, 6)
(4, 5, 6)	(1, 2, 4)
(4, 5, 6)	(1, 2, 7)
(4, 5, 6)	(1, 4, 7)
(4, 5, 6)	(2, 4, 7)
(4, 5, 6)	(3, 5, 6)
(4, 5, 7)	(0, 3, 5)
(4, 5, 7)	(0, 3, 6)
(4, 5, 7)	(0, 5, 6)

(4, 5, 7)	(1, 2, 4)
(4, 5, 7)	(1, 2, 7)
(4, 5, 7)	(1, 4, 7)
(4, 5, 7)	(2, 4, 7)
(4, 5, 7)	(3, 5, 6)
(4, 6, 7)	(0, 3, 5)
(4, 6, 7)	(0, 3, 6)
(4, 6, 7)	(0, 5, 6)
(4, 6, 7)	(1, 2, 4)
(4, 6, 7)	(1, 2, 7)
(4, 6, 7)	(1, 4, 7)
(4, 6, 7)	(2, 4, 7)
(4, 6, 7)	(3, 5, 6)
(5, 6, 7)	(0, 3, 5)
(5, 6, 7)	(0, 3, 6)
(5, 6, 7)	(0, 5, 6)
(5, 6, 7)	(1, 2, 4)
(5, 6, 7)	(1, 2, 7)
(5, 6, 7)	(1, 4, 7)
(5, 6, 7)	(2, 4, 7)
(5, 6, 7)	(3, 5, 6)
(0, 1, 2, 3)	(0, 1, 2, 4)
(0, 1, 2, 3)	(0, 1, 2, 7)
(0, 1, 2, 3)	(0, 1, 3, 5)
(0, 1, 2, 3)	(0, 1, 3, 6)
(0, 1, 2, 3)	(0, 1, 4, 7)
(0, 1, 2, 3)	(0, 1, 5, 6)
(0, 1, 2, 3)	(0, 2, 3, 5)
(0, 1, 2, 3)	(0, 2, 3, 6)
(0, 1, 2, 3)	(0, 2, 4, 7)
(0, 1, 2, 3)	(0, 2, 5, 6)
(0, 1, 2, 3)	(0, 3, 4, 5)
(0, 1, 2, 3)	(0, 3, 4, 6)
(0, 1, 2, 3)	(0, 3, 5, 6)
(0, 1, 2, 3)	(0, 3, 5, 7)
(0, 1, 2, 3)	(0, 3, 6, 7)
(0, 1, 2, 3)	(0, 4, 5, 6)
(0, 1, 2, 3)	(0, 5, 6, 7)
(0, 1, 2, 3)	(1, 2, 3, 4)
(0, 1, 2, 3)	(1, 2, 3, 7)
(0, 1, 2, 3)	(1, 2, 4, 5)
(0, 1, 2, 3)	(1, 2, 4, 6)
(0, 1, 2, 3)	(1, 2, 4, 7)
(0, 1, 2, 3)	(1, 2, 5, 7)
(0, 1, 2, 3)	(1, 2, 6, 7)
(0, 1, 2, 3)	(1, 3, 4, 7)
(0, 1, 2, 3)	(1, 3, 5, 6)
(0, 1, 2, 3)	(1, 4, 5, 7)
(0, 1, 2, 3)	(1, 4, 6, 7)
(0, 1, 2, 3)	(2, 3, 4, 7)
(0, 1, 2, 3)	(2, 3, 5, 6)
(0, 1, 2, 3)	(2, 4, 5, 7)
(0, 1, 2, 3)	(2, 4, 6, 7)
(0, 1, 2, 3)	(3, 4, 5, 6)

(0, 1, 2, 3)	(3, 5, 6, 7)
(0, 1, 2, 4)	(0, 1, 2, 3)
(0, 1, 2, 4)	(0, 1, 4, 5)
(0, 1, 2, 4)	(0, 2, 4, 6)
(0, 1, 2, 4)	(0, 3, 5, 6)
(0, 1, 2, 4)	(1, 2, 4, 7)
(0, 1, 2, 4)	(1, 3, 5, 7)
(0, 1, 2, 4)	(2, 3, 6, 7)
(0, 1, 2, 4)	(4, 5, 6, 7)
(0, 1, 2, 5)	(0, 3, 5, 6)
(0, 1, 2, 5)	(1, 2, 4, 7)
(0, 1, 2, 5)	(2, 5, 6, 7)
(0, 1, 2, 6)	(0, 1, 2, 6)
(0, 1, 2, 6)	(0, 3, 5, 6)
(0, 1, 2, 6)	(1, 2, 4, 7)
(0, 1, 2, 7)	(0, 1, 2, 3)
(0, 1, 2, 7)	(0, 1, 6, 7)
(0, 1, 2, 7)	(0, 2, 5, 7)
(0, 1, 2, 7)	(0, 3, 5, 6)
(0, 1, 2, 7)	(1, 2, 4, 7)
(0, 1, 2, 7)	(1, 3, 4, 6)
(0, 1, 2, 7)	(2, 3, 4, 5)
(0, 1, 2, 7)	(4, 5, 6, 7)
(0, 1, 3, 4)	(0, 3, 5, 6)
(0, 1, 3, 4)	(1, 2, 4, 7)
(0, 1, 3, 4)	(3, 4, 6, 7)
(0, 1, 3, 5)	(0, 1, 2, 3)
(0, 1, 3, 5)	(0, 1, 4, 5)
(0, 1, 3, 5)	(0, 2, 4, 6)
(0, 1, 3, 5)	(0, 3, 5, 6)
(0, 1, 3, 5)	(1, 2, 4, 7)
(0, 1, 3, 5)	(1, 3, 5, 7)
(0, 1, 3, 5)	(2, 3, 6, 7)
(0, 1, 3, 5)	(4, 5, 6, 7)
(0, 1, 3, 6)	(0, 1, 2, 3)
(0, 1, 3, 6)	(0, 1, 6, 7)
(0, 1, 3, 6)	(0, 2, 5, 7)
(0, 1, 3, 6)	(0, 3, 5, 6)
(0, 1, 3, 6)	(1, 2, 4, 7)
(0, 1, 3, 6)	(1, 3, 4, 6)
(0, 1, 3, 6)	(2, 3, 4, 5)
(0, 1, 3, 6)	(4, 5, 6, 7)
(0, 1, 3, 7)	(0, 1, 3, 7)
(0, 1, 3, 7)	(0, 3, 5, 6)
(0, 1, 3, 7)	(1, 2, 4, 7)
(0, 1, 4, 5)	(0, 1, 2, 4)
(0, 1, 4, 5)	(0, 1, 3, 5)
(0, 1, 4, 5)	(0, 1, 6, 7)
(0, 1, 4, 5)	(0, 2, 3, 6)
(0, 1, 4, 5)	(0, 4, 5, 6)
(0, 1, 4, 5)	(1, 2, 3, 7)
(0, 1, 4, 5)	(1, 4, 5, 7)
(0, 1, 4, 5)	(2, 3, 4, 5)
(0, 1, 4, 5)	(2, 4, 6, 7)

(0, 1, 4, 5)	(3, 5, 6, 7)
(0, 1, 4, 6)	(0, 2, 4, 7)
(0, 1, 4, 6)	(0, 2, 5, 6)
(0, 1, 4, 7)	(0, 1, 2, 3)
(0, 1, 4, 7)	(4, 5, 6, 7)
(0, 1, 5, 6)	(0, 1, 2, 3)
(0, 1, 5, 6)	(4, 5, 6, 7)
(0, 1, 5, 7)	(1, 3, 4, 7)
(0, 1, 5, 7)	(1, 3, 5, 6)
(0, 1, 6, 7)	(0, 1, 2, 7)
(0, 1, 6, 7)	(0, 1, 3, 6)
(0, 1, 6, 7)	(0, 1, 4, 5)
(0, 1, 6, 7)	(0, 2, 3, 5)
(0, 1, 6, 7)	(0, 5, 6, 7)
(0, 1, 6, 7)	(1, 2, 3, 4)
(0, 1, 6, 7)	(1, 4, 6, 7)
(0, 1, 6, 7)	(2, 3, 6, 7)
(0, 1, 6, 7)	(2, 4, 5, 7)
(0, 1, 6, 7)	(3, 4, 5, 6)
(0, 2, 3, 4)	(0, 2, 3, 4)
(0, 2, 3, 4)	(0, 3, 5, 6)
(0, 2, 3, 4)	(1, 2, 4, 7)
(0, 2, 3, 5)	(0, 1, 2, 3)
(0, 2, 3, 5)	(0, 1, 6, 7)
(0, 2, 3, 5)	(0, 2, 5, 7)
(0, 2, 3, 5)	(0, 3, 5, 6)
(0, 2, 3, 5)	(1, 2, 4, 7)
(0, 2, 3, 5)	(1, 3, 4, 6)
(0, 2, 3, 5)	(2, 3, 4, 5)
(0, 2, 3, 5)	(4, 5, 6, 7)
(0, 2, 3, 6)	(0, 1, 2, 3)
(0, 2, 3, 6)	(0, 1, 4, 5)
(0, 2, 3, 6)	(0, 2, 4, 6)
(0, 2, 3, 6)	(0, 3, 5, 6)
(0, 2, 3, 6)	(1, 2, 4, 7)
(0, 2, 3, 6)	(1, 3, 5, 7)
(0, 2, 3, 6)	(2, 3, 6, 7)
(0, 2, 3, 6)	(4, 5, 6, 7)
(0, 2, 3, 7)	(0, 3, 5, 6)
(0, 2, 3, 7)	(0, 4, 5, 7)
(0, 2, 3, 7)	(1, 2, 4, 7)
(0, 2, 4, 5)	(0, 3, 4, 6)
(0, 2, 4, 5)	(1, 2, 4, 6)
(0, 2, 4, 6)	(0, 1, 2, 4)
(0, 2, 4, 6)	(0, 1, 3, 5)
(0, 2, 4, 6)	(0, 2, 3, 6)
(0, 2, 4, 6)	(0, 4, 5, 6)
(0, 2, 4, 6)	(1, 2, 3, 7)
(0, 2, 4, 6)	(1, 4, 5, 7)
(0, 2, 4, 6)	(2, 4, 6, 7)
(0, 2, 4, 6)	(3, 5, 6, 7)
(0, 2, 4, 7)	(0, 1, 2, 3)
(0, 2, 4, 7)	(0, 1, 4, 6)
(0, 2, 4, 7)	(2, 3, 4, 6)

(0, 2, 4, 7)	(4, 5, 6, 7)
(0, 2, 5, 6)	(0, 1, 2, 3)
(0, 2, 5, 6)	(0, 1, 4, 6)
(0, 2, 5, 6)	(2, 3, 4, 6)
(0, 2, 5, 6)	(4, 5, 6, 7)
(0, 2, 5, 7)	(0, 1, 2, 7)
(0, 2, 5, 7)	(0, 1, 3, 6)
(0, 2, 5, 7)	(0, 2, 3, 5)
(0, 2, 5, 7)	(0, 5, 6, 7)
(0, 2, 5, 7)	(1, 2, 3, 4)
(0, 2, 5, 7)	(1, 4, 6, 7)
(0, 2, 5, 7)	(2, 4, 5, 7)
(0, 2, 5, 7)	(3, 4, 5, 6)
(0, 2, 6, 7)	(0, 3, 4, 6)
(0, 2, 6, 7)	(1, 2, 4, 6)
(0, 3, 4, 5)	(0, 1, 2, 3)
(0, 3, 4, 5)	(4, 5, 6, 7)
(0, 3, 4, 6)	(0, 1, 2, 3)
(0, 3, 4, 6)	(0, 2, 4, 5)
(0, 3, 4, 6)	(0, 2, 6, 7)
(0, 3, 4, 6)	(4, 5, 6, 7)
(0, 3, 5, 6)	(0, 1, 2, 3)
(0, 3, 5, 6)	(0, 1, 2, 4)
(0, 3, 5, 6)	(0, 1, 2, 5)
(0, 3, 5, 6)	(0, 1, 2, 6)
(0, 3, 5, 6)	(0, 1, 2, 7)
(0, 3, 5, 6)	(0, 1, 3, 4)
(0, 3, 5, 6)	(0, 1, 3, 5)
(0, 3, 5, 6)	(0, 1, 3, 6)
(0, 3, 5, 6)	(0, 1, 3, 7)
(0, 3, 5, 6)	(0, 2, 3, 4)
(0, 3, 5, 6)	(0, 2, 3, 5)
(0, 3, 5, 6)	(0, 2, 3, 6)
(0, 3, 5, 6)	(0, 2, 3, 7)
(0, 3, 5, 6)	(0, 4, 5, 6)
(0, 3, 5, 6)	(0, 4, 5, 7)
(0, 3, 5, 6)	(0, 4, 6, 7)
(0, 3, 5, 6)	(0, 5, 6, 7)
(0, 3, 5, 6)	(1, 2, 3, 4)
(0, 3, 5, 6)	(1, 2, 3, 5)
(0, 3, 5, 6)	(1, 2, 3, 6)
(0, 3, 5, 6)	(1, 2, 3, 7)
(0, 3, 5, 6)	(1, 4, 5, 6)
(0, 3, 5, 6)	(1, 4, 5, 7)
(0, 3, 5, 6)	(1, 4, 6, 7)
(0, 3, 5, 6)	(1, 5, 6, 7)
(0, 3, 5, 6)	(2, 4, 5, 6)
(0, 3, 5, 6)	(2, 4, 5, 7)
(0, 3, 5, 6)	(2, 4, 6, 7)
(0, 3, 5, 6)	(2, 5, 6, 7)
(0, 3, 5, 6)	(3, 4, 5, 6)
(0, 3, 5, 6)	(3, 4, 5, 7)
(0, 3, 5, 6)	(3, 4, 6, 7)
(0, 3, 5, 6)	(3, 5, 6, 7)

(0, 3, 5, 6)	(4, 5, 6, 7)
(0, 3, 5, 7)	(0, 1, 2, 3)
(0, 3, 5, 7)	(1, 3, 4, 5)
(0, 3, 5, 7)	(1, 3, 6, 7)
(0, 3, 5, 7)	(4, 5, 6, 7)
(0, 3, 6, 7)	(0, 1, 2, 3)
(0, 3, 6, 7)	(4, 5, 6, 7)
(0, 4, 5, 6)	(0, 1, 2, 3)
(0, 4, 5, 6)	(0, 1, 4, 5)
(0, 4, 5, 6)	(0, 2, 4, 6)
(0, 4, 5, 6)	(0, 3, 5, 6)
(0, 4, 5, 6)	(1, 2, 4, 7)
(0, 4, 5, 6)	(1, 3, 5, 7)
(0, 4, 5, 6)	(2, 3, 6, 7)
(0, 4, 5, 6)	(4, 5, 6, 7)
(0, 4, 5, 7)	(0, 2, 3, 7)
(0, 4, 5, 7)	(0, 3, 5, 6)
(0, 4, 5, 7)	(1, 2, 4, 7)
(0, 4, 6, 7)	(0, 3, 5, 6)
(0, 4, 6, 7)	(0, 4, 6, 7)
(0, 4, 6, 7)	(1, 2, 4, 7)
(0, 5, 6, 7)	(0, 1, 2, 3)
(0, 5, 6, 7)	(0, 1, 6, 7)
(0, 5, 6, 7)	(0, 2, 5, 7)
(0, 5, 6, 7)	(0, 3, 5, 6)
(0, 5, 6, 7)	(1, 2, 4, 7)
(0, 5, 6, 7)	(1, 3, 4, 6)
(0, 5, 6, 7)	(2, 3, 4, 5)
(0, 5, 6, 7)	(4, 5, 6, 7)
(1, 2, 3, 4)	(0, 1, 2, 3)
(1, 2, 3, 4)	(0, 1, 6, 7)
(1, 2, 3, 4)	(0, 2, 5, 7)
(1, 2, 3, 4)	(0, 3, 5, 6)
(1, 2, 3, 4)	(1, 2, 4, 7)
(1, 2, 3, 4)	(1, 3, 4, 6)
(1, 2, 3, 4)	(2, 3, 4, 5)
(1, 2, 3, 4)	(4, 5, 6, 7)
(1, 2, 3, 5)	(0, 3, 5, 6)
(1, 2, 3, 5)	(1, 2, 3, 5)
(1, 2, 3, 5)	(1, 2, 4, 7)
(1, 2, 3, 6)	(0, 3, 5, 6)
(1, 2, 3, 6)	(1, 2, 4, 7)
(1, 2, 3, 6)	(1, 4, 5, 6)
(1, 2, 3, 7)	(0, 1, 2, 3)
(1, 2, 3, 7)	(0, 1, 4, 5)
(1, 2, 3, 7)	(0, 2, 4, 6)
(1, 2, 3, 7)	(0, 3, 5, 6)
(1, 2, 3, 7)	(1, 2, 4, 7)
(1, 2, 3, 7)	(1, 3, 5, 7)
(1, 2, 3, 7)	(2, 3, 6, 7)
(1, 2, 3, 7)	(4, 5, 6, 7)
(1, 2, 4, 5)	(0, 1, 2, 3)
(1, 2, 4, 5)	(4, 5, 6, 7)
(1, 2, 4, 6)	(0, 1, 2, 3)

(1, 2, 4, 6)	(0, 2, 4, 5)
(1, 2, 4, 6)	(0, 2, 6, 7)
(1, 2, 4, 6)	(4, 5, 6, 7)
(1, 2, 4, 7)	(0, 1, 2, 3)
(1, 2, 4, 7)	(0, 1, 2, 4)
(1, 2, 4, 7)	(0, 1, 2, 5)
(1, 2, 4, 7)	(0, 1, 2, 6)
(1, 2, 4, 7)	(0, 1, 2, 7)
(1, 2, 4, 7)	(0, 1, 3, 4)
(1, 2, 4, 7)	(0, 1, 3, 5)
(1, 2, 4, 7)	(0, 1, 3, 6)
(1, 2, 4, 7)	(0, 1, 3, 7)
(1, 2, 4, 7)	(0, 2, 3, 4)
(1, 2, 4, 7)	(0, 2, 3, 5)
(1, 2, 4, 7)	(0, 2, 3, 6)
(1, 2, 4, 7)	(0, 2, 3, 7)
(1, 2, 4, 7)	(0, 4, 5, 6)
(1, 2, 4, 7)	(0, 4, 5, 7)
(1, 2, 4, 7)	(0, 4, 6, 7)
(1, 2, 4, 7)	(0, 5, 6, 7)
(1, 2, 4, 7)	(1, 2, 3, 4)
(1, 2, 4, 7)	(1, 2, 3, 5)
(1, 2, 4, 7)	(1, 2, 3, 6)
(1, 2, 4, 7)	(1, 2, 3, 7)
(1, 2, 4, 7)	(1, 4, 5, 6)
(1, 2, 4, 7)	(1, 4, 5, 7)
(1, 2, 4, 7)	(1, 4, 6, 7)
(1, 2, 4, 7)	(1, 5, 6, 7)
(1, 2, 4, 7)	(2, 4, 5, 6)
(1, 2, 4, 7)	(2, 4, 5, 7)
(1, 2, 4, 7)	(2, 4, 6, 7)
(1, 2, 4, 7)	(2, 5, 6, 7)
(1, 2, 4, 7)	(3, 4, 5, 6)
(1, 2, 4, 7)	(3, 4, 5, 7)
(1, 2, 4, 7)	(3, 4, 6, 7)
(1, 2, 4, 7)	(3, 5, 6, 7)
(1, 2, 4, 7)	(4, 5, 6, 7)
(1, 2, 5, 7)	(0, 1, 2, 3)
(1, 2, 5, 7)	(1, 3, 4, 5)
(1, 2, 5, 7)	(1, 3, 6, 7)
(1, 2, 5, 7)	(4, 5, 6, 7)
(1, 2, 6, 7)	(0, 1, 2, 3)
(1, 2, 6, 7)	(4, 5, 6, 7)
(1, 3, 4, 5)	(0, 3, 5, 7)
(1, 3, 4, 5)	(1, 2, 5, 7)
(1, 3, 4, 6)	(0, 1, 2, 7)
(1, 3, 4, 6)	(0, 1, 3, 6)
(1, 3, 4, 6)	(0, 2, 3, 5)
(1, 3, 4, 6)	(0, 5, 6, 7)
(1, 3, 4, 6)	(1, 2, 3, 4)
(1, 3, 4, 6)	(1, 4, 6, 7)
(1, 3, 4, 6)	(2, 4, 5, 7)
(1, 3, 4, 6)	(3, 4, 5, 6)
(1, 3, 4, 7)	(0, 1, 2, 3)

(1, 3, 4, 7)	(0, 1, 5, 7)
(1, 3, 4, 7)	(2, 3, 5, 7)
(1, 3, 4, 7)	(4, 5, 6, 7)
(1, 3, 5, 6)	(0, 1, 2, 3)
(1, 3, 5, 6)	(0, 1, 5, 7)
(1, 3, 5, 6)	(2, 3, 5, 7)
(1, 3, 5, 6)	(4, 5, 6, 7)
(1, 3, 5, 7)	(0, 1, 2, 4)
(1, 3, 5, 7)	(0, 1, 3, 5)
(1, 3, 5, 7)	(0, 2, 3, 6)
(1, 3, 5, 7)	(0, 4, 5, 6)
(1, 3, 5, 7)	(1, 2, 3, 7)
(1, 3, 5, 7)	(1, 4, 5, 7)
(1, 3, 5, 7)	(2, 4, 6, 7)
(1, 3, 5, 7)	(3, 5, 6, 7)
(1, 3, 6, 7)	(0, 3, 5, 7)
(1, 3, 6, 7)	(1, 2, 5, 7)
(1, 4, 5, 6)	(0, 3, 5, 6)
(1, 4, 5, 6)	(1, 2, 3, 6)
(1, 4, 5, 6)	(1, 2, 4, 7)
(1, 4, 5, 7)	(0, 1, 2, 3)
(1, 4, 5, 7)	(0, 1, 4, 5)
(1, 4, 5, 7)	(0, 2, 4, 6)
(1, 4, 5, 7)	(0, 3, 5, 6)
(1, 4, 5, 7)	(1, 2, 4, 7)
(1, 4, 5, 7)	(1, 3, 5, 7)
(1, 4, 5, 7)	(2, 3, 6, 7)
(1, 4, 5, 7)	(4, 5, 6, 7)
(1, 4, 6, 7)	(0, 1, 2, 3)
(1, 4, 6, 7)	(0, 1, 6, 7)
(1, 4, 6, 7)	(0, 2, 5, 7)
(1, 4, 6, 7)	(0, 3, 5, 6)
(1, 4, 6, 7)	(1, 2, 4, 7)
(1, 4, 6, 7)	(1, 3, 4, 6)
(1, 4, 6, 7)	(2, 3, 4, 5)
(1, 4, 6, 7)	(4, 5, 6, 7)
(1, 5, 6, 7)	(0, 3, 5, 6)
(1, 5, 6, 7)	(1, 2, 4, 7)
(1, 5, 6, 7)	(1, 5, 6, 7)
(2, 3, 4, 5)	(0, 1, 2, 7)
(2, 3, 4, 5)	(0, 1, 3, 6)
(2, 3, 4, 5)	(0, 1, 4, 5)
(2, 3, 4, 5)	(0, 2, 3, 5)
(2, 3, 4, 5)	(0, 5, 6, 7)
(2, 3, 4, 5)	(1, 2, 3, 4)
(2, 3, 4, 5)	(1, 4, 6, 7)
(2, 3, 4, 5)	(2, 3, 6, 7)
(2, 3, 4, 5)	(2, 4, 5, 7)
(2, 3, 4, 5)	(3, 4, 5, 6)
(2, 3, 4, 6)	(0, 2, 4, 7)
(2, 3, 4, 6)	(0, 2, 5, 6)
(2, 3, 4, 7)	(0, 1, 2, 3)
(2, 3, 4, 7)	(4, 5, 6, 7)
(2, 3, 5, 6)	(0, 1, 2, 3)

(2, 3, 5, 6)	(4, 5, 6, 7)
(2, 3, 5, 7)	(1, 3, 4, 7)
(2, 3, 5, 7)	(1, 3, 5, 6)
(2, 3, 6, 7)	(0, 1, 2, 4)
(2, 3, 6, 7)	(0, 1, 3, 5)
(2, 3, 6, 7)	(0, 1, 6, 7)
(2, 3, 6, 7)	(0, 2, 3, 6)
(2, 3, 6, 7)	(0, 4, 5, 6)
(2, 3, 6, 7)	(1, 2, 3, 7)
(2, 3, 6, 7)	(1, 4, 5, 7)
(2, 3, 6, 7)	(2, 3, 4, 5)
(2, 3, 6, 7)	(2, 4, 6, 7)
(2, 3, 6, 7)	(3, 5, 6, 7)
(2, 4, 5, 6)	(0, 3, 5, 6)
(2, 4, 5, 6)	(1, 2, 4, 7)
(2, 4, 5, 6)	(2, 4, 5, 6)
(2, 4, 5, 7)	(0, 1, 2, 3)
(2, 4, 5, 7)	(0, 1, 6, 7)
(2, 4, 5, 7)	(0, 2, 5, 7)
(2, 4, 5, 7)	(0, 3, 5, 6)
(2, 4, 5, 7)	(1, 2, 4, 7)
(2, 4, 5, 7)	(1, 3, 4, 6)
(2, 4, 5, 7)	(2, 3, 4, 5)
(2, 4, 5, 7)	(4, 5, 6, 7)
(2, 4, 6, 7)	(0, 1, 2, 3)
(2, 4, 6, 7)	(0, 1, 4, 5)
(2, 4, 6, 7)	(0, 2, 4, 6)
(2, 4, 6, 7)	(0, 3, 5, 6)
(2, 4, 6, 7)	(1, 2, 4, 7)
(2, 4, 6, 7)	(1, 3, 5, 7)
(2, 4, 6, 7)	(2, 3, 6, 7)
(2, 4, 6, 7)	(4, 5, 6, 7)
(2, 5, 6, 7)	(0, 1, 2, 5)
(2, 5, 6, 7)	(0, 3, 5, 6)
(2, 5, 6, 7)	(1, 2, 4, 7)
(3, 4, 5, 6)	(0, 1, 2, 3)
(3, 4, 5, 6)	(0, 1, 6, 7)
(3, 4, 5, 6)	(0, 2, 5, 7)
(3, 4, 5, 6)	(0, 3, 5, 6)
(3, 4, 5, 6)	(1, 2, 4, 7)
(3, 4, 5, 6)	(1, 3, 4, 6)
(3, 4, 5, 6)	(2, 3, 4, 5)
(3, 4, 5, 6)	(4, 5, 6, 7)
(3, 4, 5, 7)	(0, 3, 5, 6)
(3, 4, 5, 7)	(1, 2, 4, 7)
(3, 4, 5, 7)	(3, 4, 5, 7)
(3, 4, 6, 7)	(0, 1, 3, 4)
(3, 4, 6, 7)	(0, 3, 5, 6)
(3, 4, 6, 7)	(1, 2, 4, 7)
(3, 5, 6, 7)	(0, 1, 2, 3)
(3, 5, 6, 7)	(0, 1, 4, 5)
(3, 5, 6, 7)	(0, 2, 4, 6)
(3, 5, 6, 7)	(0, 3, 5, 6)
(3, 5, 6, 7)	(1, 2, 4, 7)

(3, 5, 6, 7)	(1, 3, 5, 7)
(3, 5, 6, 7)	(2, 3, 6, 7)
(3, 5, 6, 7)	(4, 5, 6, 7)
(4, 5, 6, 7)	(0, 1, 2, 4)
(4, 5, 6, 7)	(0, 1, 2, 7)
(4, 5, 6, 7)	(0, 1, 3, 5)
(4, 5, 6, 7)	(0, 1, 3, 6)
(4, 5, 6, 7)	(0, 1, 4, 7)
(4, 5, 6, 7)	(0, 1, 5, 6)
(4, 5, 6, 7)	(0, 2, 3, 5)
(4, 5, 6, 7)	(0, 2, 3, 6)
(4, 5, 6, 7)	(0, 2, 4, 7)
(4, 5, 6, 7)	(0, 2, 5, 6)
(4, 5, 6, 7)	(0, 3, 4, 5)
(4, 5, 6, 7)	(0, 3, 4, 6)
(4, 5, 6, 7)	(0, 3, 5, 6)
(4, 5, 6, 7)	(0, 3, 5, 7)
(4, 5, 6, 7)	(0, 3, 6, 7)
(4, 5, 6, 7)	(0, 4, 5, 6)
(4, 5, 6, 7)	(0, 5, 6, 7)
(4, 5, 6, 7)	(1, 2, 3, 4)
(4, 5, 6, 7)	(1, 2, 3, 7)
(4, 5, 6, 7)	(1, 2, 4, 5)
(4, 5, 6, 7)	(1, 2, 4, 6)
(4, 5, 6, 7)	(1, 2, 4, 7)
(4, 5, 6, 7)	(1, 2, 5, 7)
(4, 5, 6, 7)	(1, 2, 6, 7)
(4, 5, 6, 7)	(1, 3, 4, 7)
(4, 5, 6, 7)	(1, 3, 5, 6)
(4, 5, 6, 7)	(1, 4, 5, 7)
(4, 5, 6, 7)	(1, 4, 6, 7)
(4, 5, 6, 7)	(2, 3, 4, 7)
(4, 5, 6, 7)	(2, 3, 5, 6)
(4, 5, 6, 7)	(2, 4, 5, 7)
(4, 5, 6, 7)	(2, 4, 6, 7)
(4, 5, 6, 7)	(3, 4, 5, 6)
(4, 5, 6, 7)	(3, 5, 6, 7)
(0, 1, 2, 3, 4)	(0, 1, 2, 4, 7)
(0, 1, 2, 3, 4)	(0, 1, 3, 5, 6)
(0, 1, 2, 3, 4)	(0, 2, 3, 5, 6)
(0, 1, 2, 3, 4)	(0, 3, 4, 5, 6)
(0, 1, 2, 3, 4)	(0, 3, 5, 6, 7)
(0, 1, 2, 3, 4)	(1, 2, 3, 4, 7)
(0, 1, 2, 3, 4)	(1, 2, 4, 5, 7)
(0, 1, 2, 3, 4)	(1, 2, 4, 6, 7)
(0, 1, 2, 3, 5)	(0, 1, 2, 4, 7)
(0, 1, 2, 3, 5)	(0, 1, 3, 5, 6)
(0, 1, 2, 3, 5)	(0, 2, 3, 5, 6)
(0, 1, 2, 3, 5)	(0, 3, 4, 5, 6)
(0, 1, 2, 3, 5)	(0, 3, 5, 6, 7)
(0, 1, 2, 3, 5)	(1, 2, 3, 4, 7)
(0, 1, 2, 3, 5)	(1, 2, 4, 5, 7)
(0, 1, 2, 3, 5)	(1, 2, 4, 6, 7)
(0, 1, 2, 3, 6)	(0, 1, 2, 4, 7)

(0, 1, 2, 3, 6)	(0, 1, 3, 5, 6)
(0, 1, 2, 3, 6)	(0, 2, 3, 5, 6)
(0, 1, 2, 3, 6)	(0, 3, 4, 5, 6)
(0, 1, 2, 3, 6)	(0, 3, 5, 6, 7)
(0, 1, 2, 3, 6)	(1, 2, 3, 4, 7)
(0, 1, 2, 3, 6)	(1, 2, 4, 5, 7)
(0, 1, 2, 3, 6)	(1, 2, 4, 6, 7)
(0, 1, 2, 3, 7)	(0, 1, 2, 4, 7)
(0, 1, 2, 3, 7)	(0, 1, 3, 5, 6)
(0, 1, 2, 3, 7)	(0, 2, 3, 5, 6)
(0, 1, 2, 3, 7)	(0, 3, 4, 5, 6)
(0, 1, 2, 3, 7)	(0, 3, 5, 6, 7)
(0, 1, 2, 3, 7)	(1, 2, 3, 4, 7)
(0, 1, 2, 3, 7)	(1, 2, 4, 5, 7)
(0, 1, 2, 3, 7)	(1, 2, 4, 6, 7)
(0, 1, 2, 4, 5)	(0, 1, 2, 5, 7)
(0, 1, 2, 4, 5)	(1, 3, 4, 5, 6)
(0, 1, 2, 4, 6)	(0, 1, 2, 5, 7)
(0, 1, 2, 4, 6)	(0, 3, 4, 6, 7)
(0, 1, 2, 4, 6)	(1, 3, 4, 5, 6)
(0, 1, 2, 4, 6)	(2, 3, 4, 5, 7)
(0, 1, 2, 4, 7)	(0, 1, 2, 3, 4)
(0, 1, 2, 4, 7)	(0, 1, 2, 3, 5)
(0, 1, 2, 4, 7)	(0, 1, 2, 3, 6)
(0, 1, 2, 4, 7)	(0, 1, 2, 3, 7)
(0, 1, 2, 4, 7)	(0, 4, 5, 6, 7)
(0, 1, 2, 4, 7)	(1, 4, 5, 6, 7)
(0, 1, 2, 4, 7)	(2, 4, 5, 6, 7)
(0, 1, 2, 4, 7)	(3, 4, 5, 6, 7)
(0, 1, 2, 5, 6)	(0, 1, 2, 5, 7)
(0, 1, 2, 5, 6)	(0, 2, 4, 6, 7)
(0, 1, 2, 5, 6)	(1, 3, 4, 5, 6)
(0, 1, 2, 5, 7)	(0, 1, 2, 4, 5)
(0, 1, 2, 5, 7)	(0, 1, 2, 4, 6)
(0, 1, 2, 5, 7)	(0, 1, 2, 5, 6)
(0, 1, 2, 5, 7)	(0, 1, 4, 5, 6)
(0, 1, 2, 5, 7)	(0, 2, 4, 5, 6)
(0, 1, 2, 5, 7)	(1, 2, 4, 5, 6)
(0, 1, 2, 6, 7)	(1, 3, 4, 5, 7)
(0, 1, 3, 4, 5)	(0, 1, 3, 4, 6)
(0, 1, 3, 4, 5)	(0, 2, 4, 5, 7)
(0, 1, 3, 4, 6)	(0, 1, 3, 4, 5)
(0, 1, 3, 4, 6)	(0, 1, 3, 4, 7)
(0, 1, 3, 4, 6)	(0, 1, 3, 5, 7)
(0, 1, 3, 4, 6)	(0, 1, 4, 5, 7)
(0, 1, 3, 4, 6)	(0, 3, 4, 5, 7)
(0, 1, 3, 4, 6)	(1, 3, 4, 5, 7)
(0, 1, 3, 4, 7)	(0, 1, 3, 4, 6)
(0, 1, 3, 4, 7)	(0, 2, 4, 5, 7)
(0, 1, 3, 4, 7)	(1, 3, 5, 6, 7)
(0, 1, 3, 5, 6)	(0, 1, 2, 3, 4)
(0, 1, 3, 5, 6)	(0, 1, 2, 3, 5)
(0, 1, 3, 5, 6)	(0, 1, 2, 3, 6)
(0, 1, 3, 5, 6)	(0, 1, 2, 3, 7)

(0, 1, 3, 5, 6)	(0, 4, 5, 6, 7)
(0, 1, 3, 5, 6)	(1, 4, 5, 6, 7)
(0, 1, 3, 5, 6)	(2, 4, 5, 6, 7)
(0, 1, 3, 5, 6)	(3, 4, 5, 6, 7)
(0, 1, 3, 5, 7)	(0, 1, 3, 4, 6)
(0, 1, 3, 5, 7)	(0, 2, 4, 5, 7)
(0, 1, 3, 5, 7)	(1, 2, 5, 6, 7)
(0, 1, 3, 5, 7)	(2, 3, 4, 5, 6)
(0, 1, 3, 6, 7)	(0, 2, 4, 5, 6)
(0, 1, 4, 5, 6)	(0, 1, 2, 5, 7)
(0, 1, 4, 5, 6)	(1, 3, 4, 5, 6)
(0, 1, 4, 5, 7)	(0, 1, 3, 4, 6)
(0, 1, 4, 5, 7)	(0, 2, 4, 5, 7)
(0, 1, 4, 6, 7)	(1, 2, 3, 5, 7)
(0, 1, 5, 6, 7)	(0, 2, 3, 4, 6)
(0, 2, 3, 4, 5)	(1, 3, 5, 6, 7)
(0, 2, 3, 4, 6)	(0, 1, 5, 6, 7)
(0, 2, 3, 4, 6)	(0, 2, 3, 5, 7)
(0, 2, 3, 4, 6)	(1, 2, 4, 5, 6)
(0, 2, 3, 4, 6)	(1, 3, 4, 6, 7)
(0, 2, 3, 4, 7)	(0, 2, 3, 5, 7)
(0, 2, 3, 4, 7)	(0, 2, 4, 5, 6)
(0, 2, 3, 4, 7)	(1, 3, 4, 6, 7)
(0, 2, 3, 5, 6)	(0, 1, 2, 3, 4)
(0, 2, 3, 5, 6)	(0, 1, 2, 3, 5)
(0, 2, 3, 5, 6)	(0, 1, 2, 3, 6)
(0, 2, 3, 5, 6)	(0, 1, 2, 3, 7)
(0, 2, 3, 5, 6)	(0, 4, 5, 6, 7)
(0, 2, 3, 5, 6)	(1, 4, 5, 6, 7)
(0, 2, 3, 5, 6)	(2, 4, 5, 6, 7)
(0, 2, 3, 5, 6)	(3, 4, 5, 6, 7)
(0, 2, 3, 5, 7)	(0, 2, 3, 4, 6)
(0, 2, 3, 5, 7)	(0, 2, 3, 4, 7)
(0, 2, 3, 5, 7)	(0, 2, 3, 6, 7)
(0, 2, 3, 5, 7)	(0, 2, 4, 6, 7)
(0, 2, 3, 5, 7)	(0, 3, 4, 6, 7)
(0, 2, 3, 5, 7)	(2, 3, 4, 6, 7)
(0, 2, 3, 6, 7)	(0, 2, 3, 5, 7)
(0, 2, 3, 6, 7)	(1, 3, 4, 6, 7)
(0, 2, 4, 5, 6)	(0, 1, 2, 5, 7)
(0, 2, 4, 5, 6)	(0, 1, 3, 6, 7)
(0, 2, 4, 5, 6)	(0, 2, 3, 4, 7)
(0, 2, 4, 5, 6)	(1, 3, 4, 5, 6)
(0, 2, 4, 5, 7)	(0, 1, 3, 4, 5)
(0, 2, 4, 5, 7)	(0, 1, 3, 4, 7)
(0, 2, 4, 5, 7)	(0, 1, 3, 5, 7)
(0, 2, 4, 5, 7)	(0, 1, 4, 5, 7)
(0, 2, 4, 5, 7)	(0, 3, 4, 5, 7)
(0, 2, 4, 5, 7)	(1, 3, 4, 5, 7)
(0, 2, 4, 6, 7)	(0, 1, 2, 5, 6)
(0, 2, 4, 6, 7)	(0, 2, 3, 5, 7)
(0, 2, 4, 6, 7)	(1, 2, 3, 4, 5)
(0, 2, 4, 6, 7)	(1, 3, 4, 6, 7)
(0, 2, 5, 6, 7)	(1, 2, 3, 5, 6)

(0, 2, 5, 6, 7)	(1, 2, 3, 5, 7)
(0, 2, 5, 6, 7)	(1, 2, 3, 6, 7)
(0, 2, 5, 6, 7)	(1, 2, 5, 6, 7)
(0, 2, 5, 6, 7)	(1, 3, 5, 6, 7)
(0, 2, 5, 6, 7)	(2, 3, 5, 6, 7)
(0, 3, 4, 5, 6)	(0, 1, 2, 3, 4)
(0, 3, 4, 5, 6)	(0, 1, 2, 3, 5)
(0, 3, 4, 5, 6)	(0, 1, 2, 3, 6)
(0, 3, 4, 5, 6)	(0, 1, 2, 3, 7)
(0, 3, 4, 5, 6)	(0, 4, 5, 6, 7)
(0, 3, 4, 5, 6)	(1, 4, 5, 6, 7)
(0, 3, 4, 5, 6)	(2, 4, 5, 6, 7)
(0, 3, 4, 5, 6)	(3, 4, 5, 6, 7)
(0, 3, 4, 5, 7)	(0, 1, 3, 4, 6)
(0, 3, 4, 5, 7)	(0, 2, 4, 5, 7)
(0, 3, 4, 5, 7)	(1, 2, 3, 5, 7)
(0, 3, 4, 6, 7)	(0, 1, 2, 4, 6)
(0, 3, 4, 6, 7)	(0, 2, 3, 5, 7)
(0, 3, 4, 6, 7)	(1, 3, 4, 6, 7)
(0, 3, 5, 6, 7)	(0, 1, 2, 3, 4)
(0, 3, 5, 6, 7)	(0, 1, 2, 3, 5)
(0, 3, 5, 6, 7)	(0, 1, 2, 3, 6)
(0, 3, 5, 6, 7)	(0, 1, 2, 3, 7)
(0, 3, 5, 6, 7)	(0, 4, 5, 6, 7)
(0, 3, 5, 6, 7)	(1, 4, 5, 6, 7)
(0, 3, 5, 6, 7)	(2, 4, 5, 6, 7)
(0, 3, 5, 6, 7)	(3, 4, 5, 6, 7)
(0, 4, 5, 6, 7)	(0, 1, 2, 4, 7)
(0, 4, 5, 6, 7)	(0, 1, 3, 5, 6)
(0, 4, 5, 6, 7)	(0, 2, 3, 5, 6)
(0, 4, 5, 6, 7)	(0, 3, 4, 5, 6)
(0, 4, 5, 6, 7)	(0, 3, 5, 6, 7)
(0, 4, 5, 6, 7)	(1, 2, 3, 4, 7)
(0, 4, 5, 6, 7)	(1, 2, 4, 5, 7)
(0, 4, 5, 6, 7)	(1, 2, 4, 6, 7)
(1, 2, 3, 4, 5)	(0, 2, 4, 6, 7)
(1, 2, 3, 4, 6)	(1, 2, 3, 5, 6)
(1, 2, 3, 4, 6)	(1, 2, 3, 5, 7)
(1, 2, 3, 4, 6)	(1, 2, 3, 6, 7)
(1, 2, 3, 4, 6)	(1, 2, 5, 6, 7)
(1, 2, 3, 4, 6)	(1, 3, 5, 6, 7)
(1, 2, 3, 4, 6)	(2, 3, 5, 6, 7)
(1, 2, 3, 4, 7)	(0, 1, 2, 3, 4)
(1, 2, 3, 4, 7)	(0, 1, 2, 3, 5)
(1, 2, 3, 4, 7)	(0, 1, 2, 3, 6)
(1, 2, 3, 4, 7)	(0, 1, 2, 3, 7)
(1, 2, 3, 4, 7)	(0, 4, 5, 6, 7)
(1, 2, 3, 4, 7)	(1, 4, 5, 6, 7)
(1, 2, 3, 4, 7)	(2, 4, 5, 6, 7)
(1, 2, 3, 4, 7)	(3, 4, 5, 6, 7)
(1, 2, 3, 5, 6)	(0, 2, 5, 6, 7)
(1, 2, 3, 5, 6)	(1, 2, 3, 4, 6)
(1, 2, 3, 5, 6)	(1, 3, 4, 5, 7)
(1, 2, 3, 5, 7)	(0, 1, 4, 6, 7)

(1, 2, 3, 5, 7)	(0, 2, 5, 6, 7)
(1, 2, 3, 5, 7)	(0, 3, 4, 5, 7)
(1, 2, 3, 5, 7)	(1, 2, 3, 4, 6)
(1, 2, 3, 6, 7)	(0, 2, 5, 6, 7)
(1, 2, 3, 6, 7)	(1, 2, 3, 4, 6)
(1, 2, 4, 5, 6)	(0, 1, 2, 5, 7)
(1, 2, 4, 5, 6)	(0, 2, 3, 4, 6)
(1, 2, 4, 5, 6)	(1, 3, 4, 5, 6)
(1, 2, 4, 5, 7)	(0, 1, 2, 3, 4)
(1, 2, 4, 5, 7)	(0, 1, 2, 3, 5)
(1, 2, 4, 5, 7)	(0, 1, 2, 3, 6)
(1, 2, 4, 5, 7)	(0, 1, 2, 3, 7)
(1, 2, 4, 5, 7)	(0, 4, 5, 6, 7)
(1, 2, 4, 5, 7)	(1, 4, 5, 6, 7)
(1, 2, 4, 5, 7)	(2, 4, 5, 6, 7)
(1, 2, 4, 5, 7)	(3, 4, 5, 6, 7)
(1, 2, 4, 6, 7)	(0, 1, 2, 3, 4)
(1, 2, 4, 6, 7)	(0, 1, 2, 3, 5)
(1, 2, 4, 6, 7)	(0, 1, 2, 3, 6)
(1, 2, 4, 6, 7)	(0, 1, 2, 3, 7)
(1, 2, 4, 6, 7)	(0, 4, 5, 6, 7)
(1, 2, 4, 6, 7)	(1, 4, 5, 6, 7)
(1, 2, 4, 6, 7)	(2, 4, 5, 6, 7)
(1, 2, 4, 6, 7)	(3, 4, 5, 6, 7)
(1, 2, 5, 6, 7)	(0, 1, 3, 5, 7)
(1, 2, 5, 6, 7)	(0, 2, 5, 6, 7)
(1, 2, 5, 6, 7)	(1, 2, 3, 4, 6)
(1, 3, 4, 5, 6)	(0, 1, 2, 4, 5)
(1, 3, 4, 5, 6)	(0, 1, 2, 4, 6)
(1, 3, 4, 5, 6)	(0, 1, 2, 5, 6)
(1, 3, 4, 5, 6)	(0, 1, 4, 5, 6)
(1, 3, 4, 5, 6)	(0, 2, 4, 5, 6)
(1, 3, 4, 5, 6)	(1, 2, 4, 5, 6)
(1, 3, 4, 5, 7)	(0, 1, 2, 6, 7)
(1, 3, 4, 5, 7)	(0, 1, 3, 4, 6)
(1, 3, 4, 5, 7)	(0, 2, 4, 5, 7)
(1, 3, 4, 5, 7)	(1, 2, 3, 5, 6)
(1, 3, 4, 6, 7)	(0, 2, 3, 4, 6)
(1, 3, 4, 6, 7)	(0, 2, 3, 4, 7)
(1, 3, 4, 6, 7)	(0, 2, 3, 6, 7)
(1, 3, 4, 6, 7)	(0, 2, 4, 6, 7)
(1, 3, 4, 6, 7)	(0, 3, 4, 6, 7)
(1, 3, 4, 6, 7)	(2, 3, 4, 6, 7)
(1, 3, 5, 6, 7)	(0, 1, 3, 4, 7)
(1, 3, 5, 6, 7)	(0, 2, 3, 4, 5)
(1, 3, 5, 6, 7)	(0, 2, 5, 6, 7)
(1, 3, 5, 6, 7)	(1, 2, 3, 4, 6)
(1, 4, 5, 6, 7)	(0, 1, 2, 4, 7)
(1, 4, 5, 6, 7)	(0, 1, 3, 5, 6)
(1, 4, 5, 6, 7)	(0, 2, 3, 5, 6)
(1, 4, 5, 6, 7)	(0, 3, 4, 5, 6)
(1, 4, 5, 6, 7)	(0, 3, 5, 6, 7)
(1, 4, 5, 6, 7)	(1, 2, 3, 4, 7)
(1, 4, 5, 6, 7)	(1, 2, 4, 5, 7)

(1, 4, 5, 6, 7)	(1, 2, 4, 6, 7)
(2, 3, 4, 5, 6)	(0, 1, 3, 5, 7)
(2, 3, 4, 5, 7)	(0, 1, 2, 4, 6)
(2, 3, 4, 6, 7)	(0, 2, 3, 5, 7)
(2, 3, 4, 6, 7)	(1, 3, 4, 6, 7)
(2, 3, 5, 6, 7)	(0, 2, 5, 6, 7)
(2, 3, 5, 6, 7)	(1, 2, 3, 4, 6)
(2, 4, 5, 6, 7)	(0, 1, 2, 4, 7)
(2, 4, 5, 6, 7)	(0, 1, 3, 5, 6)
(2, 4, 5, 6, 7)	(0, 2, 3, 5, 6)
(2, 4, 5, 6, 7)	(0, 3, 4, 5, 6)
(2, 4, 5, 6, 7)	(0, 3, 5, 6, 7)
(2, 4, 5, 6, 7)	(1, 2, 3, 4, 7)
(2, 4, 5, 6, 7)	(1, 2, 4, 5, 7)
(2, 4, 5, 6, 7)	(1, 2, 4, 6, 7)
(3, 4, 5, 6, 7)	(0, 1, 2, 4, 7)
(3, 4, 5, 6, 7)	(0, 1, 3, 5, 6)
(3, 4, 5, 6, 7)	(0, 2, 3, 5, 6)
(3, 4, 5, 6, 7)	(0, 3, 4, 5, 6)
(3, 4, 5, 6, 7)	(0, 3, 5, 6, 7)
(3, 4, 5, 6, 7)	(1, 2, 3, 4, 7)
(3, 4, 5, 6, 7)	(1, 2, 4, 5, 7)
(3, 4, 5, 6, 7)	(1, 2, 4, 6, 7)
(0, 1, 2, 3, 4, 6)	(0, 1, 3, 4, 5, 7)
(0, 1, 2, 3, 4, 6)	(1, 2, 3, 5, 6, 7)
(0, 1, 2, 3, 5, 7)	(0, 1, 2, 4, 5, 6)
(0, 1, 2, 3, 5, 7)	(0, 2, 3, 4, 6, 7)
(0, 1, 2, 4, 5, 6)	(0, 1, 2, 3, 5, 7)
(0, 1, 2, 4, 5, 6)	(0, 1, 2, 4, 5, 7)
(0, 1, 2, 4, 5, 6)	(0, 1, 2, 5, 6, 7)
(0, 1, 2, 4, 5, 6)	(0, 1, 3, 4, 5, 6)
(0, 1, 2, 4, 5, 6)	(1, 2, 3, 4, 5, 6)
(0, 1, 2, 4, 5, 6)	(1, 3, 4, 5, 6, 7)
(0, 1, 2, 4, 5, 7)	(0, 1, 2, 4, 5, 6)
(0, 1, 2, 4, 5, 7)	(0, 1, 3, 4, 5, 7)
(0, 1, 2, 5, 6, 7)	(0, 1, 2, 4, 5, 6)
(0, 1, 2, 5, 6, 7)	(1, 2, 3, 5, 6, 7)
(0, 1, 3, 4, 5, 6)	(0, 1, 2, 4, 5, 6)
(0, 1, 3, 4, 5, 6)	(0, 1, 3, 4, 5, 7)
(0, 1, 3, 4, 5, 7)	(0, 1, 2, 3, 4, 6)
(0, 1, 3, 4, 5, 7)	(0, 1, 2, 4, 5, 7)
(0, 1, 3, 4, 5, 7)	(0, 1, 3, 4, 5, 6)
(0, 1, 3, 4, 5, 7)	(0, 1, 3, 4, 6, 7)
(0, 1, 3, 4, 5, 7)	(0, 2, 3, 4, 5, 7)
(0, 1, 3, 4, 5, 7)	(0, 2, 4, 5, 6, 7)
(0, 1, 3, 4, 6, 7)	(0, 1, 3, 4, 5, 7)
(0, 1, 3, 4, 6, 7)	(0, 2, 3, 4, 6, 7)
(0, 2, 3, 4, 5, 7)	(0, 1, 3, 4, 5, 7)
(0, 2, 3, 4, 5, 7)	(0, 2, 3, 4, 6, 7)
(0, 2, 3, 4, 6, 7)	(0, 1, 2, 3, 5, 7)
(0, 2, 3, 4, 6, 7)	(0, 1, 3, 4, 6, 7)
(0, 2, 3, 4, 6, 7)	(0, 2, 3, 4, 5, 7)
(0, 2, 3, 4, 6, 7)	(0, 2, 3, 5, 6, 7)
(0, 2, 3, 4, 6, 7)	(1, 2, 3, 4, 6, 7)

(0, 2, 3, 4, 6, 7)	(1, 3, 4, 5, 6, 7)
(0, 2, 3, 5, 6, 7)	(0, 2, 3, 4, 6, 7)
(0, 2, 3, 5, 6, 7)	(1, 2, 3, 5, 6, 7)
(0, 2, 4, 5, 6, 7)	(0, 1, 3, 4, 5, 7)
(0, 2, 4, 5, 6, 7)	(1, 2, 3, 5, 6, 7)
(1, 2, 3, 4, 5, 6)	(0, 1, 2, 4, 5, 6)
(1, 2, 3, 4, 5, 6)	(1, 2, 3, 5, 6, 7)
(1, 2, 3, 4, 6, 7)	(0, 2, 3, 4, 6, 7)
(1, 2, 3, 4, 6, 7)	(1, 2, 3, 5, 6, 7)
(1, 2, 3, 5, 6, 7)	(0, 1, 2, 3, 4, 6)
(1, 2, 3, 5, 6, 7)	(0, 1, 2, 5, 6, 7)
(1, 2, 3, 5, 6, 7)	(0, 2, 3, 5, 6, 7)
(1, 2, 3, 5, 6, 7)	(0, 2, 4, 5, 6, 7)
(1, 2, 3, 5, 6, 7)	(1, 2, 3, 4, 5, 6)
(1, 2, 3, 5, 6, 7)	(1, 2, 3, 4, 6, 7)
(1, 3, 4, 5, 6, 7)	(0, 1, 2, 4, 5, 6)
(1, 3, 4, 5, 6, 7)	(0, 2, 3, 4, 6, 7)

Table 1.4: Whirlwind m_1 (1.69) singular submatrices

The fact that we have found singular submatrices for Whirlwind's m_0 and m_1 matrices shows they are not MDS in $GF(2^4)$. However, it is relevant to note that, in [2], the authors mention the usage of the $GF(2^{16})$ field with *decompositions* to $GF(2^4)$, as well as the usage of a *normal basis* representation for the finite fields. It is possible that, despite not MDS in $GF(2^4)$ with $p(x) = x^4+x+1$ as the irreducible polynomial and a polynomial basis $\{1, x, x^2, x^3, x^4\}$, matrices (1.67) and (1.69) be MDS for the normal basis representation. We are still studying and evaluating this in our research. This report will be updated with our future findings. For this reason, we place Whirlwind's matrices in Table 1.5, while we are still investigating.

Year	**Ord**	**Type**	**Inv**	**Use**	**Bib**	$GF(2)[x]/(p(x))$	**#xor**	**#xtime**	**Matrices**
2010	8	dyadic	no	Whirlwind	[2]	$x^4 + x + 1$	104 128	136 136	(1.67) (1.68)
2010	8	dyadic	no	Whirlwind	[2]	$x^4 + x + 1$	128 128	128 128	(1.69) (1.70)

Table 1.5: Non-MDS matrices under further investigation: parameters, usage and cost

$$\begin{bmatrix} 5_x & 4_x & a_x & 6_x & 2_x & d_x & 8_x & 3_x \\ 4_x & 5_x & 6_x & a_x & d_x & 2_x & 3_x & 8_x \\ a_x & 6_x & 5_x & 4_x & 8_x & 3_x & 2_x & d_x \\ 6_x & a_x & 4_x & 5_x & 3_x & 8_x & d_x & 2_x \\ 2_x & d_x & 8_x & 3_x & 5_x & 4_x & a_x & 6_x \\ d_x & 2_x & 3_x & 8_x & 4_x & 5_x & 6_x & a_x \\ 8_x & 3_x & 2_x & d_x & a_x & 6_x & 5_x & 4_x \\ 3_x & 8_x & d_x & 2_x & 6_x & a_x & 4_x & 5_x \end{bmatrix} \quad (1.67)$$

$$\begin{bmatrix} 7_x & 3_x & e_x & b_x & 8_x & 1_x & 6_x & c_x \\ 3_x & 7_x & b_x & e_x & 1_x & 8_x & c_x & 6_x \\ e_x & b_x & 7_x & 3_x & 6_x & c_x & 8_x & 1_x \\ b_x & e_x & 3_x & 7_x & c_x & 6_x & 1_x & 8_x \\ 8_x & 1_x & 6_x & c_x & 7_x & 3_x & e_x & b_x \\ 1_x & 8_x & c_x & 6_x & 3_x & 7_x & b_x & e_x \\ 6_x & c_x & 8_x & 1_x & e_x & b_x & 7_x & 3_x \\ c_x & 6_x & 1_x & 8_x & b_x & e_x & 3_x & 7_x \end{bmatrix} \tag{1.68}$$

$$\begin{bmatrix} 5_x & e_x & 4_x & 7_x & 1_x & 3_x & f_x & 8_x \\ e_x & 5_x & 7_x & 4_x & 3_x & 1_x & 8_x & f_x \\ 4_x & 7_x & 5_x & e_x & f_x & 8_x & 1_x & 3_x \\ 7_x & 4_x & e_x & 5_x & 8_x & f_x & 3_x & 1_x \\ 1_x & 3_x & f_x & 8_x & 5_x & e_x & 4_x & 7_x \\ 3_x & 1_x & 8_x & f_x & e_x & 5_x & 7_x & 4_x \\ f_x & 8_x & 1_x & 3_x & 4_x & 7_x & 5_x & e_x \\ 8_x & f_x & 3_x & 1_x & 7_x & 4_x & e_x & 5_x \end{bmatrix} \tag{1.69}$$

$$\begin{bmatrix} f_x & 1_x & c_x & 9_x & 3_x & 5_x & 2_x & b_x \\ 1_x & f_x & 9_x & c_x & 5_x & 3_x & b_x & 2_x \\ c_x & 9_x & f_x & 1_x & 2_x & b_x & 3_x & 5_x \\ 9_x & c_x & 1_x & f_x & b_x & 2_x & 5_x & 3_x \\ 3_x & 5_x & 2_x & b_x & f_x & 1_x & c_x & 9_x \\ 5_x & 3_x & b_x & 2_x & 1_x & f_x & 9_x & c_x \\ 2_x & b_x & 3_x & 5_x & c_x & 9_x & f_x & 1_x \\ b_x & 2_x & 5_x & 3_x & 9_x & c_x & 1_x & f_x \end{bmatrix} \tag{1.70}$$

1.8 Non-MDS matrix catalogue

Table 1.6 presents matrices which were reported in the literature for usage in symmetric block ciphers (or hash functions) but are not MDS. It shows their **xor** and **xtime** costs, as well as the respective branch numbers. Column **Ord** refers to the matrix dimensions, **Bib** contains the bibliographic reference, **#xor** and **#xtime** refer to the required amount of **xor** and **xtime** operations, i.e the costs, and $\mathcal{B}(\theta)$ presents the branch number.

Fiquei em dúvida quando fui calcular o branch number das matrizes binárias do Hierocrypt, podemos revisar isso na próxima reunião? Obrigada!

Year	**Ord**	**Bib**	**Type**	**Use**	$\mathcal{B}(\theta)$	**#xor**	**#xtime**	**Matrix**
2000	16	[10]	binary	Hierocrypt-3	branch	160	0	(1.31)
2000	8	[11]	binary	Hierocrypt-L1	branch	37	0	(1.32)
2003	8	[26]	right circulant	Whirlpool-0	8	89 247	87 366	(1.33) (1.34)

Table 1.6: Non-MDS matrices: parameters, usage and costs.

1.9 About the irreducible polynomials

to be written It is worth noting that, when changing the irreducible polynomial, the finite field changes, and that may cause the inverse matrices to change, resulting in inverse matrices with different computational costs. In this work, we briefly explore this. Table **??** shows, for each matrix studied in this work (column A) and each possible irreducible polynomial (column $p(x)$), the determinant (column $|A|$), the multiplicative inverse of the determinant ($\frac{1}{|A|}$), the **xor** cost (xr), the **xtime** cost (xt), whether A is involutory (column Iv), whether the MDS property holds (column MDS) on the finite field, the determinant of the inverse matrix, A^{-1}, on the finite field (column $|A|_i$), **xor** and **xtime** costs (xr_i and xt_i, respectively), involutory property for A^{-1} (Iv_i) and, finally, MDS property for A^{-1} (MDS_i).

It is worth noting that, for some matrices and fields, the MDS property does not hold. It is the case of SHARK, where the MDS property only holds for the $p(x)$ chosen by the cipher's authors. However, for others, such as Rijndael, KHAZAD and Anubis, the MDS and involutory properties always hold, no matter the field, and the **xor** and **xtime** costs of the inverse matrix do not change. This suggests that it is possible to choose the best irreducible polynomial when designing a diffusion layer — the polynomial which keeps MDS property and yields inverse matrices with the lowest cost.

A	$p(x)$	$\lvert A\rvert$	$\frac{1}{\lvert A\rvert}$	xr	xt	Iv	MDS	$\lvert A\rvert_i$	xr_i	xt_i	Iv_i	MDS_i
SHARK (1.3)	$x^8+x^4+x^3+x+1$	A1	7C	235	369	no	no	7C	261	399	no	no
SHARK (1.3)	$x^8+x^4+x^3+x^2+1$	FE	7E	235	369	no	no	7E	233	372	no	no
SHARK (1.3)	$x^8+x^5+x^3+x+1$	23	E8	235	369	no	no	E8	237	380	no	no
SHARK (1.3)	$x^8+x^5+x^3+x^2+1$	55	89	235	369	no	no	89	235	370	no	no
SHARK (1.3)	$x^8+x^5+x^4+x^3+1$	87	9B	235	369	no	no	9B	255	380	no	no
SHARK (1.3)	$x^8+x^5+x^4+x^3+x^2+x+1$	60	E3	235	369	no	no	E3	258	389	no	no
SHARK (1.3)	$x^8+x^6+x^3+x^2+1$	4F	E3	235	369	no	no	E3	257	398	no	no
SHARK (1.3)	$x^8+x^6+x^4+x^3+x^2+x+1$	C2	EA	235	369	no	no	EA	260	390	no	no
SHARK (1.3)	$x^8+x^6+x^5+x+1$	FD	CB	235	369	no	no	CB	232	384	no	no
SHARK (1.3)	$x^8+x^6+x^5+x^2+1$	4E	B8	235	369	no	no	B8	242	396	no	no
SHARK (1.3)	$x^8+x^6+x^5+x^3+1$	3C	E	235	369	no	no	E	257	375	no	no
SHARK (1.3)	$x^8+x^6+x^5+x^4+1$	5B	95	235	369	no	no	95	225	372	no	no
SHARK (1.3)	$x^8+x^6+x^5+x^4+x^2+x+1$	94	67	235	369	no	no	67	249	396	no	no
SHARK (1.3)	$x^8+x^6+x^5+x^4+x^3+x+1$	91	B3	235	369	no	no	B3	257	392	no	no
SHARK (1.3)	$x^8+x^7+x^2+x+1$	9A	EA	235	369	no	no	EA	240	387	no	no
SHARK (1.3)	$x^8+x^7+x^3+x+1$	1D	F6	235	369	no	no	F6	256	400	no	no
SHARK (1.3)	$x^8+x^7+x^3+x^2+1$	63	4	235	369	no	no	4	247	373	no	no
SHARK (1.3)	$x^8+x^7+x^4+x^3+x^2+x+1$	29	32	235	369	no	no	32	233	377	no	no
SHARK (1.3)	$x^8+x^7+x^5+x+1$	EF	95	235	369	no	no	95	241	380	no	no
SHARK (1.3)	$x^8+x^7+x^5+x^3+1$	76	54	235	369	no	no	54	246	381	no	no
SHARK (1.3)	$x^8+x^7+x^5+x^4+1$	8	36	235	369	no	no	36	230	390	no	no
SHARK (1.3)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	A	AD	235	369	no	no	AD	245	382	no	no

SHARK (1.3)	$x^8+x^7+x^6+x+1$	34	64	235	369	no	no	64	243	394	no	no
SHARK (1.3)	$x^8+x^7+x^6+x^3+x^2+x+1$	F9	78	235	369	no	no	78	274	403	no	no
SHARK (1.3)	$x^8+x^7+x^6+x^4+x^2+x+1$	A3	24	235	369	no	no	24	230	383	no	no
SHARK (1.3)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	86	CE	235	369	no	no	CE	241	379	no	no
SHARK (1.3)	$x^8+x^7+x^6+x^5+x^2+x+1$	37	52	235	369	no	no	52	254	375	no	no
SHARK (1.3)	$x^8+x^7+x^6+x^5+x^4+x+1$	29	40	235	369	no	no	40	254	395	no	no
SHARK (1.3)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	FC	EC	235	369	no	yes	EC	223	393	no	yes
SHARK (1.3)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	BF	1B	235	369	no	no	1B	257	385	no	no
SQUARE (1.5)	$x^8+x^4+x^3+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^4+x^3+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^5+x^3+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^5+x^3+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^5+x^4+x^3+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^5+x^4+x^3+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^6+x^3+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^6+x^4+x^3+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^6+x^5+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^6+x^5+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^6+x^5+x^3+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^6+x^5+x^4+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^6+x^5+x^4+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^6+x^5+x^4+x^3+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^3+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^3+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^4+x^3+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^5+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^5+x^3+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^5+x^4+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^6+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^6+x^3+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^6+x^4+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^6+x^5+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^6+x^5+x^4+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
SQUARE (1.5)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	1	1	16	8	no	yes	1	40	48	no	yes
BKSQ (1.14)	$x^8+x^4+x^3+x+1$	3	F6	9	9	no	yes	F6	57	63	no	yes
BKSQ (1.14)	$x^8+x^4+x^3+x^2+1$	3	F4	9	9	no	yes	F4	48	63	no	yes
BKSQ (1.14)	$x^8+x^5+x^3+x+1$	3	E6	9	9	no	yes	E6	48	63	no	yes

BKSQ (1.14)	$x^8+x^5+x^3+x^2+1$	3	E4	9	9	no	yes	E4	39	63	no	yes
BKSQ (1.14)	$x^8+x^5+x^4+x^3+1$	3	E8	9	9	no	yes	E8	39	63	no	yes
BKSQ (1.14)	$x^8+x^5+x^4+x^3+x^2+x+1$	3	EA	9	9	no	yes	EA	48	63	no	yes
BKSQ (1.14)	$x^8+x^6+x^3+x^2+1$	3	C4	9	9	no	yes	C4	30	63	no	yes
BKSQ (1.14)	$x^8+x^6+x^4+x^3+x^2+x+1$	3	CA	9	9	no	yes	CA	39	63	no	yes
BKSQ (1.14)	$x^8+x^6+x^5+x+1$	3	DE	9	9	no	yes	DE	57	63	no	yes
BKSQ (1.14)	$x^8+x^6+x^5+x^2+1$	3	DC	9	9	no	yes	DC	48	63	no	yes
BKSQ (1.14)	$x^8+x^6+x^5+x^3+1$	3	D8	9	9	no	yes	D8	39	63	no	yes
BKSQ (1.14)	$x^8+x^6+x^5+x^4+1$	3	D0	9	9	no	yes	D0	30	63	no	yes
BKSQ (1.14)	$x^8+x^6+x^5+x^4+x^2+x+1$	3	D2	9	9	no	yes	D2	39	63	no	yes
BKSQ (1.14)	$x^8+x^6+x^5+x^4+x^3+x+1$	3	D6	9	9	no	yes	D6	48	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^2+x+1$	3	82	9	9	no	yes	82	21	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^3+x+1$	3	86	9	9	no	yes	86	30	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^3+x^2+1$	3	84	9	9	no	yes	84	21	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^4+x^3+x^2+x+1$	3	8A	9	9	no	yes	8A	30	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^5+x+1$	3	9E	9	9	no	yes	9E	48	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^5+x^3+1$	3	98	9	9	no	yes	98	30	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^5+x^4+1$	3	90	9	9	no	yes	90	21	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	3	94	9	9	no	yes	94	30	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^6+x+1$	3	BE	9	9	no	yes	BE	57	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^6+x^3+x^2+x+1$	3	BA	9	9	no	yes	BA	48	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^6+x^4+x^2+x+1$	3	B2	9	9	no	yes	B2	39	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	3	B4	9	9	no	yes	B4	39	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^6+x^5+x^2+x+1$	3	A2	9	9	no	yes	A2	30	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^6+x^5+x^4+x+1$	3	AE	9	9	no	yes	AE	48	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	3	AC	9	9	no	yes	AC	39	63	no	yes
BKSQ (1.14)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	3	A8	9	9	no	yes	A8	30	63	no	yes
Tavares (1.7)	$x^8+x^4+x^3+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^4+x^3+x^2+1$	1	1	240	344	yes	yes	1	240	344	yes	yes
Tavares (1.7)	$x^8+x^5+x^3+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^5+x^3+x^2+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^5+x^4+x^3+1$	1	1	240	344	yes	yes	1	240	344	yes	yes
Tavares (1.7)	$x^8+x^5+x^4+x^3+x^2+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^6+x^3+x^2+1$	1	1	240	344	yes	yes	1	240	344	yes	yes
Tavares (1.7)	$x^8+x^6+x^4+x^3+x^2+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^6+x^5+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^6+x^5+x^2+1$	1	1	240	344	yes	yes	1	240	344	yes	yes
Tavares (1.7)	$x^8+x^6+x^5+x^3+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^6+x^5+x^4+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^6+x^5+x^4+x^2+x+1$	1	1	240	344	yes	yes	1	240	344	yes	yes
Tavares (1.7)	$x^8+x^6+x^5+x^4+x^3+x+1$	1	1	240	344	yes	no	1	240	344	yes	no

Tavares (1.7)	$x^8+x^7+x^2+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^3+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^3+x^2+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^4+x^3+x^2+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^5+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^5+x^3+1$	1	1	240	344	yes	yes	1	240	344	yes	yes
Tavares (1.7)	$x^8+x^7+x^5+x^4+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^6+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^6+x^3+x^2+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^6+x^4+x^2+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^6+x^5+x^2+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^6+x^5+x^4+x+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	1	1	240	344	yes	no	1	240	344	yes	no
Tavares (1.7)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	1	1	240	344	yes	no	1	240	344	yes	no
KHAZAD (1.8)	$x^8+x^4+x^3+x+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^4+x^3+x^2+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^5+x^3+x+1$	1	1	112	120	yes	no	1	112	120	yes	no
KHAZAD (1.8)	$x^8+x^5+x^3+x^2+1$	1	1	112	120	yes	no	1	112	120	yes	no
KHAZAD (1.8)	$x^8+x^5+x^4+x^3+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^5+x^4+x^3+x^2+x+1$	1	1	112	120	yes	no	1	112	120	yes	no
KHAZAD (1.8)	$x^8+x^6+x^3+x^2+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^6+x^4+x^3+x^2+x+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^6+x^5+x+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^6+x^5+x^2+1$	1	1	112	120	yes	no	1	112	120	yes	no
KHAZAD (1.8)	$x^8+x^6+x^5+x^3+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^6+x^5+x^4+1$	1	1	112	120	yes	no	1	112	120	yes	no
KHAZAD (1.8)	$x^8+x^6+x^5+x^4+x^2+x+1$	1	1	112	120	yes	no	1	112	120	yes	no
KHAZAD (1.8)	$x^8+x^6+x^5+x^4+x^3+x+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^7+x^2+x+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^7+x^3+x+1$	1	1	112	120	yes	no	1	112	120	yes	no
KHAZAD (1.8)	$x^8+x^7+x^3+x^2+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^7+x^4+x^3+x^2+x+1$	1	1	112	120	yes	no	1	112	120	yes	no
KHAZAD (1.8)	$x^8+x^7+x^5+x+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^7+x^5+x^3+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^7+x^5+x^4+1$	1	1	112	120	yes	no	1	112	120	yes	no
KHAZAD (1.8)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^7+x^6+x+1$	1	1	112	120	yes	no	1	112	120	yes	no
KHAZAD (1.8)	$x^8+x^7+x^6+x^3+x^2+x+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^7+x^6+x^4+x^2+x+1$	1	1	112	120	yes	no	1	112	120	yes	no
KHAZAD (1.8)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	1	1	112	120	yes	no	1	112	120	yes	no
KHAZAD (1.8)	$x^8+x^7+x^6+x^5+x^2+x+1$	1	1	112	120	yes	no	1	112	120	yes	no

KHAZAD (1.8)	$x^8+x^7+x^6+x^5+x^4+x+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
KHAZAD (1.8)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	1	1	112	120	yes	yes	1	112	120	yes	yes
Anubis (1.9)	$x^8+x^4+x^3+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^4+x^3+x^2+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^5+x^3+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^5+x^3+x^2+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^5+x^4+x^3+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^5+x^4+x^3+x^2+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^6+x^3+x^2+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^6+x^4+x^3+x^2+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^6+x^5+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^6+x^5+x^2+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^6+x^5+x^3+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^6+x^5+x^4+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^6+x^5+x^4+x^2+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^6+x^5+x^4+x^3+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^2+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^3+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^3+x^2+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^4+x^3+x^2+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^5+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^5+x^3+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^5+x^4+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^6+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^6+x^3+x^2+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^6+x^4+x^2+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^6+x^5+x^2+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^6+x^5+x^4+x+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (1.9)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	1	1	16	20	yes	yes	1	16	20	yes	yes
Anubis (KE) (1.10)	$x^8+x^4+x^3+x+1$	63	D3	20	32	no	yes	D3	65	96	no	yes
Anubis (KE) (1.10)	$x^8+x^4+x^3+x^2+1$	A5	C2	20	32	no	yes	C2	69	101	no	yes
Anubis (KE) (1.10)	$x^8+x^5+x^3+x+1$	A9	EF	20	32	no	yes	EF	71	100	no	yes
Anubis (KE) (1.10)	$x^8+x^5+x^3+x^2+1$	7B	B1	20	32	no	yes	B1	55	93	no	yes
Anubis (KE) (1.10)	$x^8+x^5+x^4+x^3+1$	E5	3C	20	32	no	yes	3C	59	97	no	yes
Anubis (KE) (1.10)	$x^8+x^5+x^4+x^3+x^2+x+1$	3B	29	20	32	no	yes	29	61	101	no	yes

Anubis (KE) (1.10)	$x^8+x^6+x^3+x^2+1$	9D	F4	20	32	no	yes	F4	47	81	no	yes
Anubis (KE) (1.10)	$x^8+x^6+x^4+x^3+x^2+x+1$	E1	18	20	32	no	yes	18	55	104	no	yes
Anubis (KE) (1.10)	$x^8+x^6+x^5+x+1$	EC	D0	20	32	no	yes	D0	57	97	no	yes
Anubis (KE) (1.10)	$x^8+x^6+x^5+x^2+1$	4	59	20	32	no	yes	59	57	93	no	yes
Anubis (KE) (1.10)	$x^8+x^6+x^5+x^3+1$	BD	D4	20	32	no	yes	D4	49	81	no	yes
Anubis (KE) (1.10)	$x^8+x^6+x^5+x^4+1$	96	4D	20	32	no	yes	4D	63	101	no	yes
Anubis (KE) (1.10)	$x^8+x^6+x^5+x^4+x^2+x+1$	72	56	20	32	no	yes	56	63	100	no	yes
Anubis (KE) (1.10)	$x^8+x^6+x^5+x^4+x^3+x+1$	C1	F3	20	32	no	yes	F3	67	92	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^2+x+1$	AC	B	20	32	no	yes	B	61	98	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^3+x+1$	37	A5	20	32	no	yes	A5	57	93	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^3+x^2+1$	B9	EC	20	32	no	yes	EC	63	100	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^4+x^3+x^2+x+1$	2D	42	20	32	no	yes	42	57	94	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^5+x+1$	F3	B	20	32	no	yes	B	63	93	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^5+x^3+1$	E0	42	20	32	no	yes	42	59	96	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^5+x^4+1$	73	88	20	32	no	yes	88	53	101	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	FA	41	20	32	no	yes	41	61	100	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^6+x+1$	87	5A	20	32	no	yes	5A	67	97	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^6+x^3+x^2+x+1$	34	C5	20	32	no	yes	C5	59	100	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^6+x^4+x^2+x+1$	AD	AA	20	32	no	yes	AA	61	93	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	A6	F5	20	32	no	yes	F5	61	101	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^6+x^5+x^2+x+1$	88	3B	20	32	no	yes	3B	53	102	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^6+x^5+x^4+x+1$	AE	3	20	32	no	yes	3	59	98	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	2	FA	20	32	no	yes	FA	57	95	no	yes
Anubis (KE) (1.10)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	A3	36	20	32	no	yes	36	57	93	no	yes
Whirlwind m_0 (1.67)	x^4+x+1	B	5	104	136	no	no	5	128	136	no	no
Whirlwind m_0 (1.67)	x^4+x^3+1	4	6	104	136	no	no	6	112	160	no	no

Whirlwind m_0 (1.67)	$x^4+x^3+x^2+x+1$	E	B	104	136	no	no	B	128	128	no	no
Whirlwind m_1 (1.69)	x^4+x+1	9	2	128	128	no	no	2	128	128	no	no
Whirlwind m_1 (1.69)	x^4+x^3+1	6	4	128	128	no	no	4	120	144	no	no
Whirlwind m_1 (1.69)	$x^4+x^3+x^2+x+1$	C	D	128	128	no	no	D	120	160	no	no
Grøstl (1.29)	$x^8+x^4+x^3+x+1$	1A	FD	104	96	no	yes	FD	232	376	no	yes
Grøstl (1.29)	$x^8+x^4+x^3+x^2+1$	1C	A0	104	96	no	no	A0	240	384	no	no
Grøstl (1.29)	$x^8+x^5+x^3+x+1$	2A	B9	104	96	no	no	B9	288	376	no	no
Grøstl (1.29)	$x^8+x^5+x^3+x^2+1$	2C	74	104	96	no	no	74	216	352	no	no
Grøstl (1.29)	$x^8+x^5+x^4+x^3+1$	38	C7	104	96	no	no	C7	248	408	no	no
Grøstl (1.29)	$x^8+x^5+x^4+x^3+x^2+x+1$	3E	22	104	96	no	no	22	224	408	no	no
Grøstl (1.29)	$x^8+x^6+x^3+x^2+1$	4C	3C	104	96	no	no	3C	240	400	no	no
Grøstl (1.29)	$x^8+x^6+x^4+x^3+x^2+x+1$	5E	91	104	96	no	no	91	248	432	no	no
Grøstl (1.29)	$x^8+x^6+x^5+x+1$	62	2B	104	96	no	no	2B	264	416	no	no
Grøstl (1.29)	$x^8+x^6+x^5+x^2+1$	64	1C	104	96	no	no	1C	240	328	no	no
Grøstl (1.29)	$x^8+x^6+x^5+x^3+1$	68	34	104	96	no	yes	34	248	376	no	yes
Grøstl (1.29)	$x^8+x^6+x^5+x^4+1$	70	7A	104	96	no	no	7A	288	384	no	no
Grøstl (1.29)	$x^8+x^6+x^5+x^4+x^2+x+1$	76	63	104	96	no	no	63	232	400	no	no
Grøstl (1.29)	$x^8+x^6+x^5+x^4+x^3+x+1$	7A	3D	104	96	no	no	3D	208	360	no	no
Grøstl (1.29)	$x^8+x^7+x^2+x+1$	86	B8	104	96	no	no	B8	280	376	no	no
Grøstl (1.29)	$x^8+x^7+x^3+x+1$	8A	F7	104	96	no	no	F7	208	376	no	no
Grøstl (1.29)	$x^8+x^7+x^3+x^2+1$	8C	A9	104	96	no	yes	A9	200	384	no	yes
Grøstl (1.29)	$x^8+x^7+x^4+x^3+x^2+x+1$	9E	B1	104	96	no	yes	B1	176	360	no	yes
Grøstl (1.29)	$x^8+x^7+x^5+x+1$	A2	DF	104	96	no	no	DF	224	376	no	no
Grøstl (1.29)	$x^8+x^7+x^5+x^3+1$	A8	3B	104	96	no	no	3B	272	376	no	no
Grøstl (1.29)	$x^8+x^7+x^5+x^4+1$	B0	7F	104	96	no	no	7F	216	344	no	no
Grøstl (1.29)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	BC	79	104	96	no	no	79	272	376	no	no
Grøstl (1.29)	$x^8+x^7+x^6+x+1$	C2	F8	104	96	no	no	F8	248	352	no	no
Grøstl (1.29)	$x^8+x^7+x^6+x^3+x^2+x+1$	CE	C0	104	96	no	no	C0	240	416	no	no
Grøstl (1.29)	$x^8+x^7+x^6+x^4+x^2+x+1$	D6	29	104	96	no	no	29	232	384	no	no
Grøstl (1.29)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	DC	8D	104	96	no	no	8D	200	344	no	no
Grøstl (1.29)	$x^8+x^7+x^6+x^5+x^2+x+1$	E6	E0	104	96	no	no	E0	256	384	no	no
Grøstl (1.29)	$x^8+x^7+x^6+x^5+x^4+x+1$	F2	1B	104	96	no	no	1B	240	376	no	no
Grøstl (1.29)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	F4	13	104	96	no	no	13	200	312	no	no
Grøstl (1.29)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	F8	70	104	96	no	yes	70	256	408	no	yes
Curupira (1.26)	$x^8+x^4+x^3+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^4+x^3+x^2+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^5+x^3+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^5+x^3+x^2+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^5+x^4+x^3+1$	1	1	12	15	yes	yes	1	12	15	yes	yes

Curupira (1.26)	$x^8+x^5+x^4+x^3+x^2+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^6+x^3+x^2+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^6+x^4+x^3+x^2+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^6+x^5+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^6+x^5+x^2+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^6+x^5+x^3+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^6+x^5+x^4+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^6+x^5+x^4+x^2+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^6+x^5+x^4+x^3+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^2+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^3+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^3+x^2+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^4+x^3+x^2+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^5+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^5+x^3+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^5+x^4+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^6+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^6+x^3+x^2+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^6+x^4+x^2+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^6+x^5+x^2+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^6+x^5+x^4+x+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (1.26)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	1	1	12	15	yes	yes	1	12	15	yes	yes
Curupira (KE) (1.27)	$x^8+x^4+x^3+x+1$	1D	40	27	36	no	yes	40	12	54	no	yes
Curupira (KE) (1.27)	$x^8+x^4+x^3+x^2+1$	1D	83	27	36	no	yes	83	18	63	no	yes
Curupira (KE) (1.27)	$x^8+x^5+x^3+x+1$	1D	33	27	36	no	yes	33	27	45	no	yes
Curupira (KE) (1.27)	$x^8+x^5+x^3+x^2+1$	1D	B0	27	36	no	yes	B0	30	63	no	yes
Curupira (KE) (1.27)	$x^8+x^5+x^4+x^3+1$	1D	18	27	36	no	yes	18	21	36	no	yes
Curupira (KE) (1.27)	$x^8+x^5+x^4+x^3+x^2+x+1$	1D	61	27	36	no	yes	61	18	54	no	yes
Curupira (KE) (1.27)	$x^8+x^6+x^3+x^2+1$	1D	1C	27	36	no	yes	1C	30	36	no	yes
Curupira (KE) (1.27)	$x^8+x^6+x^4+x^3+x^2+x+1$	1D	3B	27	36	no	yes	3B	36	45	no	yes
Curupira (KE) (1.27)	$x^8+x^6+x^5+x+1$	1D	9E	27	36	no	yes	9E	48	63	no	yes

Curupira (KE) (1.27)	$x^8+x^6+x^5+x^2+1$	1D	3F	27	36	no	yes	3F	45	45	no	yes
Curupira (KE) (1.27)	$x^8+x^6+x^5+x^3+1$	1D	BB	27	36	no	yes	BB	45	63	no	yes
Curupira (KE) (1.27)	$x^8+x^6+x^5+x^4+1$	1D	79	27	36	no	yes	79	36	54	no	yes
Curupira (KE) (1.27)	$x^8+x^6+x^5+x^4+x^2+x+1$	1D	1E	27	36	no	yes	1E	39	36	no	yes
Curupira (KE) (1.27)	$x^8+x^6+x^5+x^4+x^3+x+1$	1D	F5	27	36	no	yes	F5	45	63	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^2+x+1$	1D	64	27	36	no	yes	64	30	54	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^3+x+1$	1D	F6	27	36	no	yes	F6	57	63	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^3+x^2+1$	1D	2F	27	36	no	yes	2F	36	45	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^4+x^3+x^2+x+1$	1D	16	27	36	no	yes	16	30	36	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^5+x+1$	1D	51	27	36	no	yes	51	18	54	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^5+x^3+1$	1D	A5	27	36	no	yes	A5	27	63	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^5+x^4+1$	1D	EC	27	36	no	yes	EC	48	63	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	1D	6A	27	36	no	yes	6A	39	54	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^6+x+1$	1D	23	27	36	no	yes	23	18	45	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^6+x^3+x^2+x+1$	1D	EF	27	36	no	yes	EF	54	63	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^6+x^4+x^2+x+1$	1D	41	27	36	no	yes	41	9	54	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	1D	85	27	36	no	yes	85	18	63	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^6+x^5+x^2+x+1$	1D	95	27	36	no	yes	95	27	63	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^6+x^5+x^4+x+1$	1D	78	27	36	no	yes	78	39	54	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	1D	F3	27	36	no	yes	F3	45	63	no	yes
Curupira (KE) (1.27)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	1D	27	27	36	no	yes	27	27	45	no	yes
Rijndael (1.12)	$x^8+x^4+x^3+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^4+x^3+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^5+x^3+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^5+x^3+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^5+x^4+x^3+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^5+x^4+x^3+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes

Rijndael (1.12)	$x^8+x^6+x^3+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^6+x^4+x^3+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^6+x^5+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^6+x^5+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^6+x^5+x^3+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^6+x^5+x^4+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^6+x^5+x^4+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^6+x^5+x^4+x^3+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^3+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^3+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^4+x^3+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^5+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^5+x^3+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^5+x^4+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^6+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^6+x^3+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^6+x^4+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^6+x^5+x^2+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^6+x^5+x^4+x+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	1	1	16	8	no	yes	1	40	48	no	yes
Rijndael (1.12)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	1	1	16	8	no	yes	1	40	48	no	yes
Hierocrypt (low) (1.16)	$x^8+x^4+x^3+x+1$	F1	23	52	108	no	yes	23	64	100	no	yes
Hierocrypt (low) (1.16)	$x^8+x^4+x^3+x^2+1$	33	2E	52	108	no	yes	2E	64	100	no	yes
Hierocrypt (low) (1.16)	$x^8+x^5+x^3+x+1$	C	AC	52	108	no	yes	AC	64	96	no	yes
Hierocrypt (low) (1.16)	$x^8+x^5+x^3+x^2+1$	CA	61	52	108	no	yes	61	56	96	no	yes
Hierocrypt (low) (1.16)	$x^8+x^5+x^4+x^3+1$	69	EF	52	108	no	yes	EF	44	96	no	yes
Hierocrypt (low) (1.16)	$x^8+x^5+x^4+x^3+x^2+x+1$	CD	18	52	108	no	yes	18	64	100	no	yes
Hierocrypt (low) (1.16)	$x^8+x^6+x^3+x^2+1$	AA	66	52	108	no	yes	66	60	92	no	yes
Hierocrypt (low) (1.16)	$x^8+x^6+x^4+x^3+x^2+x+1$	32	E6	52	108	no	yes	E6	80	108	no	yes
Hierocrypt (low) (1.16)	$x^8+x^6+x^5+x+1$	13	85	52	108	no	yes	85	52	104	no	yes
Hierocrypt (low) (1.16)	$x^8+x^6+x^5+x^2+1$	1B	31	52	108	no	yes	31	48	96	no	yes

Hierocrypt (low) (1.16)	$x^8+x^6+x^5+x^3+1$	63	6F	52	108	no	yes	6F	36	76	no	yes
Hierocrypt (low) (1.16)	$x^8+x^6+x^5+x^4+1$	12	EE	52	108	no	yes	EE	40	88	no	yes
Hierocrypt (low) (1.16)	$x^8+x^6+x^5+x^4+x^2+x+1$	C	8F	52	108	no	yes	8F	48	96	no	yes
Hierocrypt (low) (1.16)	$x^8+x^6+x^5+x^4+x^3+x+1$	28	3C	52	108	no	yes	3C	52	96	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^2+x+1$	6	41	52	108	no	yes	41	68	100	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^3+x+1$	5	FB	52	108	no	yes	FB	32	40	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^3+x^2+1$	FA	31	52	108	no	yes	31	36	68	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^4+x^3+x^2+x+1$	CD	79	52	108	no	yes	79	60	104	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^5+x+1$	D9	6E	52	108	no	yes	6E	64	92	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^5+x^3+1$	46	B	52	108	no	yes	B	76	108	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^5+x^4+1$	95	78	52	108	no	yes	78	76	100	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	C5	E2	52	108	no	yes	E2	60	96	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^6+x+1$	A4	86	52	108	no	yes	86	56	108	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^6+x^3+x^2+x+1$	EB	3B	52	108	no	yes	3B	60	100	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^6+x^4+x^2+x+1$	AB	B6	52	108	no	yes	B6	68	108	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	DB	AD	52	108	no	yes	AD	68	100	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^6+x^5+x^2+x+1$	AD	94	52	108	no	no	94	56	108	no	no
Hierocrypt (low) (1.16)	$x^8+x^7+x^6+x^5+x^4+x+1$	DC	7	52	108	no	yes	7	40	84	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	B2	79	52	108	no	yes	79	48	88	no	yes
Hierocrypt (low) (1.16)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	3D	B6	52	108	no	no	B6	76	104	no	no
Hierocrypt-3 (high) (1.18)	x^4+x+1	5	B	32	40	no	yes	B	40	44	no	yes
Hierocrypt-3 (high) (1.18)	x^4+x^3+1	E	7	32	40	no	no	7	28	32	no	no
Hierocrypt-3 (high) (1.18)	$x^4+x^3+x^2+x+1$	8	4	32	40	no	yes	4	16	28	no	yes
Hierocrypt L1 (high) (1.20)	x^4+x+1	2	9	8	10	no	yes	9	7	11	no	yes
Hierocrypt L1 (high) (1.20)	x^4+x^3+1	8	3	8	10	no	yes	3	8	10	no	yes

Hierocrypt L1 (high) (1.20)	$x^4+x^3+x^2+x+1$	E	B	8	10	no	yes	B	9	10	no	yes
FOX mu4 (1.22)	$x^8+x^4+x^3+x+1$	C4	DA	30	25	no	yes	DA	70	105	no	yes
FOX mu4 (1.22)	$x^8+x^4+x^3+x^2+1$	62	CA	30	25	no	yes	CA	58	91	no	yes
FOX mu4 (1.22)	$x^8+x^5+x^3+x+1$	75	FD	30	25	no	yes	FD	76	111	no	yes
FOX mu4 (1.22)	$x^8+x^5+x^3+x^2+1$	55	89	30	25	no	yes	89	71	103	no	yes
FOX mu4 (1.22)	$x^8+x^5+x^4+x^3+1$	1F	35	30	25	no	yes	35	43	85	no	yes
FOX mu4 (1.22)	$x^8+x^5+x^4+x^3+x^2+x+1$	1C	E2	30	25	no	yes	E2	46	90	no	yes
FOX mu4 (1.22)	$x^8+x^6+x^3+x^2+1$	79	CE	30	25	no	yes	CE	61	104	no	yes
FOX mu4 (1.22)	$x^8+x^6+x^4+x^3+x^2+x+1$	B6	25	30	25	no	yes	25	58	91	no	yes
FOX mu4 (1.22)	$x^8+x^6+x^5+x+1$	AA	F2	30	25	no	yes	F2	59	87	no	yes
FOX mu4 (1.22)	$x^8+x^6+x^5+x^2+1$	55	6C	30	25	no	yes	6C	59	100	no	yes
FOX mu4 (1.22)	$x^8+x^6+x^5+x^3+1$	60	E8	30	25	no	yes	E8	75	98	no	yes
FOX mu4 (1.22)	$x^8+x^6+x^5+x^4+1$	BC	2B	30	25	no	yes	2B	89	95	no	yes
FOX mu4 (1.22)	$x^8+x^6+x^5+x^4+x^2+x+1$	66	D4	30	25	no	yes	D4	73	112	no	yes
FOX mu4 (1.22)	$x^8+x^6+x^5+x^4+x^3+x+1$	28	3C	30	25	no	yes	3C	76	96	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^2+x+1$	14	DC	30	25	no	yes	DC	66	106	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^3+x+1$	72	18	30	25	no	yes	18	61	95	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^3+x^2+1$	DB	E6	30	25	no	yes	E6	79	91	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^4+x^3+x^2+x+1$	69	7D	30	25	no	yes	7D	65	109	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^5+x+1$	B6	98	30	25	no	yes	98	52	100	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^5+x^3+1$	25	B7	30	25	no	yes	B7	72	97	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^5+x^4+1$	F2	64	30	25	no	yes	64	67	112	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	32	F8	30	25	no	yes	F8	59	100	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^6+x+1$	D3	16	30	25	no	no	16	57	103	no	no
FOX mu4 (1.22)	$x^8+x^7+x^6+x^3+x^2+x+1$	8A	D	30	25	no	yes	D	61	104	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^6+x^4+x^2+x+1$	90	5D	30	25	no	yes	5D	86	108	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	A8	65	30	25	no	yes	65	56	106	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^6+x^5+x^2+x+1$	3	A2	30	25	no	yes	A2	59	84	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^6+x^5+x^4+x+1$	71	70	30	25	no	yes	70	64	88	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	D6	11	30	25	no	yes	11	47	103	no	yes
FOX mu4 (1.22)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	13	26	30	25	no	yes	26	72	106	no	yes
FOX mu8 (1.23)	$x^8+x^4+x^3+x+1$	3	F6	141	169	no	no	F6	283	399	no	no
FOX mu8 (1.23)	$x^8+x^4+x^3+x^2+1$	5A	CB	141	169	no	no	CB	268	371	no	no
FOX mu8 (1.23)	$x^8+x^5+x^3+x+1$	43	44	141	169	no	no	44	268	391	no	no
FOX mu8 (1.23)	$x^8+x^5+x^3+x^2+1$	BD	FA	141	169	no	no	FA	248	392	no	no
FOX mu8 (1.23)	$x^8+x^5+x^4+x^3+1$	A2	11	141	169	no	no	11	229	405	no	no
FOX mu8 (1.23)	$x^8+x^5+x^4+x^3+x^2+x+1$	11	7C	141	169	no	no	7C	194	369	no	no
FOX mu8 (1.23)	$x^8+x^6+x^3+x^2+1$	CD	71	141	169	no	no	71	290	411	no	no
FOX mu8 (1.23)	$x^8+x^6+x^4+x^3+x^2+x+1$	A2	34	141	169	no	no	34	234	350	no	no
FOX mu8 (1.23)	$x^8+x^6+x^5+x+1$	14	A3	141	169	no	no	A3	290	418	no	no
FOX mu8 (1.23)	$x^8+x^6+x^5+x^2+1$	3	DC	141	169	no	no	DC	255	405	no	no
FOX mu8 (1.23)	$x^8+x^6+x^5+x^3+1$	85	DE	141	169	no	no	DE	229	399	no	no
FOX mu8 (1.23)	$x^8+x^6+x^5+x^4+1$	9B	6F	141	169	no	no	6F	246	392	no	no

FOX mu8 (1.23)	$x^8+x^6+x^5+x^4+x^2+x+1$	E5	51	141	169	no	no	51	212	342	no	no
FOX mu8 (1.23)	$x^8+x^6+x^5+x^4+x^3+x+1$	E2	9A	141	169	no	no	9A	251	364	no	no
FOX mu8 (1.23)	$x^8+x^7+x^2+x+1$	31	D7	141	169	no	no	D7	234	397	no	no
FOX mu8 (1.23)	$x^8+x^7+x^3+x+1$	19	CD	141	169	no	no	CD	256	406	no	no
FOX mu8 (1.23)	$x^8+x^7+x^3+x^2+1$	F8	C4	141	169	no	no	C4	257	364	no	no
FOX mu8 (1.23)	$x^8+x^7+x^4+x^3+x^2+x+1$	FA	FB	141	169	no	no	FB	235	371	no	no
FOX mu8 (1.23)	$x^8+x^7+x^5+x+1$	BA	E1	141	169	no	no	E1	255	427	no	no
FOX mu8 (1.23)	$x^8+x^7+x^5+x^3+1$	5	EF	141	169	no	no	EF	246	404	no	no
FOX mu8 (1.23)	$x^8+x^7+x^5+x^4+1$	A1	E1	141	169	no	no	E1	235	392	no	no
FOX mu8 (1.23)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	73	DC	141	169	no	no	DC	172	363	no	no
FOX mu8 (1.23)	$x^8+x^7+x^6+x+1$	CE	C	141	169	no	no	C	263	371	no	no
FOX mu8 (1.23)	$x^8+x^7+x^6+x^3+x^2+x+1$	49	EC	141	169	no	no	EC	256	391	no	no
FOX mu8 (1.23)	$x^8+x^7+x^6+x^4+x^2+x+1$	1D	41	141	169	no	no	41	230	406	no	no
FOX mu8 (1.23)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	51	BB	141	169	no	no	BB	283	426	no	no
FOX mu8 (1.23)	$x^8+x^7+x^6+x^5+x^2+x+1$	71	EB	141	169	no	no	EB	304	378	no	no
FOX mu8 (1.23)	$x^8+x^7+x^6+x^5+x^4+x+1$	20	52	141	169	no	no	52	269	377	no	no
FOX mu8 (1.23)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	82	1B	141	169	no	no	1B	276	383	no	no
FOX mu8 (1.23)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	F0	99	141	169	no	yes	99	284	392	no	yes
Whirlpool-0 (1.33)	$x^8+x^4+x^3+x+1$	1A	FD	88	88	no	no	FD	248	336	no	no
Whirlpool-0 (1.33)	$x^8+x^4+x^3+x^2+1$	1C	A0	88	88	no	no	A0	240	360	no	no
Whirlpool-0 (1.33)	$x^8+x^5+x^3+x+1$	2A	B9	88	88	no	no	B9	256	416	no	no
Whirlpool-0 (1.33)	$x^8+x^5+x^3+x^2+1$	2C	74	88	88	no	no	74	248	392	no	no
Whirlpool-0 (1.33)	$x^8+x^5+x^4+x^3+1$	38	C7	88	88	no	no	C7	264	440	no	no
Whirlpool-0 (1.33)	$x^8+x^5+x^4+x^3+x^2+x+1$	3E	22	88	88	no	no	22	256	408	no	no
Whirlpool-0 (1.33)	$x^8+x^6+x^3+x^2+1$	4C	3C	88	88	no	no	3C	192	360	no	no
Whirlpool-0 (1.33)	$x^8+x^6+x^4+x^3+x^2+x+1$	5E	91	88	88	no	no	91	280	440	no	no
Whirlpool-0 (1.33)	$x^8+x^6+x^5+x+1$	62	2B	88	88	no	no	2B	264	424	no	no
Whirlpool-0 (1.33)	$x^8+x^6+x^5+x^2+1$	64	1C	88	88	no	no	1C	224	384	no	no
Whirlpool-0 (1.33)	$x^8+x^6+x^5+x^3+1$	68	34	88	88	no	no	34	216	328	no	no
Whirlpool-0 (1.33)	$x^8+x^6+x^5+x^4+1$	70	7A	88	88	no	no	7A	272	376	no	no
Whirlpool-0 (1.33)	$x^8+x^6+x^5+x^4+x^2+x+1$	76	63	88	88	no	no	63	248	408	no	no
Whirlpool-0 (1.33)	$x^8+x^6+x^5+x^4+x^3+x+1$	7A	3D	88	88	no	no	3D	272	408	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^2+x+1$	86	B8	88	88	no	no	B8	184	328	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^3+x+1$	8A	F7	88	88	no	no	F7	208	328	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^3+x^2+1$	8C	A9	88	88	no	no	A9	216	392	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^4+x^3+x^2+x+1$	9E	B1	88	88	no	no	B1	256	400	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^5+x+1$	A2	DF	88	88	no	no	DF	256	376	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^5+x^3+1$	A8	3B	88	88	no	no	3B	256	392	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^5+x^4+1$	B0	7F	88	88	no	no	7F	264	400	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^5+x^4+x^3+x^2+1$	BC	79	88	88	no	no	79	240	400	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^6+x+1$	C2	F8	88	88	no	no	F8	264	400	no	no

Whirlpool-0 (1.33)	$x^8+x^7+x^6+x^3+x^2+x+1$	CE	C0	88	88	no	no	C0	240	432	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^6+x^4+x^2+x+1$	D6	29	88	88	no	no	29	184	384	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^6+x^4+x^3+x^2+1$	DC	8D	88	88	no	no	8D	248	336	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^6+x^5+x^2+x+1$	E6	E0	88	88	no	no	E0	240	432	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^6+x^5+x^4+x+1$	F2	1B	88	88	no	no	1B	272	392	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^6+x^5+x^4+x^2+1$	F4	13	88	88	no	no	13	200	360	no	no
Whirlpool-0 (1.33)	$x^8+x^7+x^6+x^5+x^4+x^3+1$	F8	70	88	88	no	no	70	272	424	no	no

Table 1.7: Studying different irreducible polynomials for each matrix

1.10 Computing xtime and xor of the matrices

One can compute the costs manually, however, the following following C code can also be used for this purpose, considering that polynomials in GF(2^8) are stored in integers (a set bit means coefficient equal to 1, a zero bit means coefficient equal to 0).

For e.g SHARK and SQUARE, the field order is equal to 8, therefore `ORDER` must be set to 8 and `DEGREE_LIMIT_MASK` must be set to x^8.

```
#define DEGREE_LIMIT_MASK 0x100
#define ORDER 8
```

The following function obtains the amount of **xtime** required to multiply by the polynomial.

```
unsigned int poly_xtime_cost(unsigned int poly) {
        unsigned int degree_mask = DEGREE_LIMIT_MASK;
        unsigned int degree = ORDER;
        while ((poly & degree_mask) == 0) {
                degree_mask >>= 1;
                degree--;
        }
        return degree;
}
```

The following function obtains the amount of **xor** required to multiply by the polynomial.

```
unsigned int poly_xor_cost(unsigned int poly) {
        unsigned int mask = 1;
        unsigned int set_bits = 0;
        unsigned int current_bit = 0;
        while (current_bit <= ORDER) {
                set_bits += ((poly & mask) != 0);
                mask <<= 1;
                current_bit++;
```

```
        }
        return set_bits - 1;
}
```

And, to compute the **xtime** and **xor** costs of a matrix, we must sum the costs of each row, which is accomplished by the following functions. Note that for e.g SHARK `DIM` must be set to 8, for SQUARE, to 4, and so forth.

```
#define DIM 8

unsigned int matrix_xtime_cost(unsigned int mat [DIM][DIM]) {
        unsigned int total_cost = 0;
        for (int row = 0; row < DIM; row++) {
                unsigned int row_cost = 0;
                for (int col = 0; col < DIM; col++) {
                        row_cost += poly_xtime_cost(mat[row][col]);
                }
                printf("Row %d costs %d xtime\n", row, row_cost);
                total_cost += row_cost;
        }
        printf("The full matrix costs %d xtime\n", total_cost);
        return total_cost;
}

unsigned int matrix_xor_cost(unsigned int mat[DIM][DIM]) {
        unsigned int total_cost = 0;
        for (int row = 0; row < DIM; row++) {
                unsigned int row_cost = DIM - 1; //sum elements
                for (int col = 0; col < DIM; col++) {
                        row_cost += poly_xor_cost(mat[row][col]);
                }
                printf("Row %d costs %d xor\n", row, row_cost);
                total_cost += row_cost;
        }
        printf("The full matrix costs %d xor\n", total_cost);
        return total_cost;
}
```

1.10.1 SQUARE manual calculation example

The computational cost for matrix (1.3), used in the SQUARE cipher, was explained in Section 1.3.6.

For matrix (1.6), used in SQUARE's decryption process, each row contains elements from $\{0e_x, 09_x, 0d_x, 0b_x\}$.

$$0e_x = 00001110_2 = x^3 + x^2 + x \text{ requires 3 } \textbf{xtime} \text{ and 2 } \textbf{xor}$$

$$09_x = 00001001_2 = x^3 + 1 \text{ requires 3 } \textbf{xtime} \text{ and 1 } \textbf{xor}$$

$$0d_x = 00001101_2 = x^3 + x^2 + 1 \text{ requires 3 } \textbf{xtime} \text{ and 2 } \textbf{xor}$$

$$0b_x = 00001011_2 = x^3 + x + 1 \text{ requires 3 } \textbf{xtime} \text{ and 2 } \textbf{xor}$$

There are 3 **xor** to add the intermediate row multiplication results, totalizing 12 **xtime** and 10 **xor** per row. There are 4 rows, hence 48 **xtime** and 40 **xor**.

1.11 Conclusions

yet to be written

Bibliography

[1] Paulo Barreto. Whirlpool Web Page. `https://web.archive.org/web/20171129084214/http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html`, 2008. [Online; accessed 01-February-2022].

[2] Paulo S. L. M. Barreto, Ventzislav Nikov, Svetla Nikova, Vincent Rijmen, and Elmar Tischhauser. Whirlwind: a new cryptographic hash function. *Des. Codes Cryptogr.*, 56(2-3):141–162, 2010.

[3] Paulo S. L. M. Barreto and Vincent Rijmen. The ANUBIS block cipher. In *First NESSIE Workshop, Heverlee, Belgium*, 2000.

[4] Paulo S. L. M. Barreto and Vincent Rijmen. The KHAZAD Legacy-Level block cipher. In *First NESSIE Workshop, Heverlee, Belgium*, 2000.

[5] PSLM Barreto and M Simplicio. Curupira, a block cipher for constrained platforms. *Anais do 25o Simpsio Brasileiro de Redes de Computadores e Sistemas Distribudos-SBRC*, 1:61–74, 2007.

[6] K.G. Beauchamp. *Walsh Functions and Their Applications*. Nutrition, Basic and Applied Science. Academic Press, 1975.

[7] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Keccak. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 313–314. Springer, 2013.

[8] Eli Biham, Ross J. Anderson, and Lars R. Knudsen. Serpent: A new block cipher proposal. In Serge Vaudenay, editor, *Fast Software Encryption, 5th International Workshop, FSE '98, Paris, France, March 23-25, 1998, Proceedings*, volume 1372 of *Lecture Notes in Computer Science*, pages 222–238. Springer, 1998.

[9] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: an ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, 2007.

[10] Toshiba Corporation. Specification of Hierocrypt-3. In *First NESSIE Workshop, Heverlee, Belgium*, 2000.

[11] Toshiba Corporation. Specification of Hierocrypt-L1. In *First NESSIE Workshop, Heverlee, Belgium*, 2000.

[12] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher SQUARE. In Eli Biham, editor, *Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings*, volume 1267 of *Lecture Notes in Computer Science*, pages 149–165. Springer, 1997.

[13] Joan Daemen and Vincent Rijmen. The block cipher BKSQ. In Jean-Jacques Quisquater and Bruce Schneier, editors, *Smart Card Research and Applications, This International Conference, CARDIS '98, Louvain-la-Neuve, Belgium, September 14-16, 1998, Proceedings*, volume 1820 of *Lecture Notes in Computer Science*, pages 236–245. Springer, 1998.

[14] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[15] Praveen Gauravaram, Lars R. Knudsen, Krystian Matusiewicz, Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen. Grøstl - a SHA-3 candidate. In Helena Handschuh, Stefan Lucks, Bart Preneel, and Phillip Rogaway, editors, *Symmetric Cryptography, 11.01. - 16.01.2009*, volume 09031 of *Dagstuhl Seminar Proceedings*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Germany, 2009.

[16] Kenneth Hoffmann and Ray Kunze. Linear algebra. *Mathematics of Computation*, 15(75):407, 1971.

[17] Pascal Junod and Serge Vaudenay. FOX : A new family of block ciphers. In Helena Handschuh and M. Anwar Hasan, editors, *Selected Areas in Cryptography, 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers*, volume 3357 of *Lecture Notes in Computer Science*, pages 114–129. Springer, 2004.

[18] X Lai and J Massey. The idea block cipher. *NESSIE Block Cipher Submissions*, 2000.

[19] S. Lang. *Linear Algebra*. Springer Undergraduate Texts in Mathematics and Technology. Springer, 1987.

[20] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-holland Publishing Company, 2nd edition, 1978.

[21] A.M. Masuda and D. Panario. *Tópicos de corpos finitos com aplicações em criptografia e teoria de códigos*. Publicações matemáticas. IMPA, 2007.

[22] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., USA, 1st edition, 1996.

[23] G.L. Mullen and D. Panario. *Handbook of Finite Fields*. Discrete Mathematics and Its Applications. CRC Press, 2013.

[24] Vincent Rijmen, Joan Daemen, Bart Preneel, Antoon Bosselaers, and Erik De Win. The cipher SHARK. In Dieter Gollmann, editor, *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 21-23, 1996, Proceedings*, volume 1039 of *Lecture Notes in Computer Science*, pages 99–111. Springer, 1996.

[25] Taizo Shirai and Kyoji Shibutani. On the diffusion matrix employed in the whirlpool hashing function. 01 2003.

[26] Paulo S.L.M and Vincent Rijmen. The whirlpool hashing function. 2003.

[27] A. M. Youssef, S. Mister, and S. E. Tavares. On the design of linear transformations for substitution permutation encryption networks. In C. Adams and M. Just, editors, *Selected Areas in Cryptography, 11th International Workshop, SAC 1997, Ottawa, Canada, August 11 - 12, 1997, Revised Selected Papers*, pages 40–48. Springer, 1997.