On the diffusion matrix employed in the Whirlpool hashing function

Taizo Shirai, Kyoji Shibutani

Ubiquitous Technology Laboratories, Sony Corporation
7-35 Kitashinagawa 6-chome, Shinagawa-ku, Tokyo, 141-0001 Japan
{Taizo.Shirai, Kyoji.Shibutani}@jp.sony.com

Abstract. It has been claimed that the matrix employed in diffusion layer, i.e. the diffusion matrix, of Whirlpool hashing function was designed to hold branch number $\mathcal{B} = 9$. However, we have found that $\mathcal{B} = 8$ by analyzing certain sub-matrix and dependency of columns of the diffusion matrix. Also we show that there are 224 candidates for the diffusion matrix which actually satisfy the conditions posed by the designers of Whirlpool.

1 Introduction

Whirlpool[1] is a hashing function selected for the NESSIE portfolio of cryptographic primitives[1]. Also Whirlpool is proposed to be included in the next revision of the ISO/IEC 10118 standard.

Whirlpool is based on an underlying dedicated block cipher W, with the block length of 512-bit. The block cipher W employs a SPN type round function. It is claimed that the diffusion layer of W uses an 8×8 matrix with the branch number $\mathcal{B} = 9$. Due to the Square pattern propagation theorem, it is guaranteed that the number of S-boxes with a different input value in four consecutive rounds is at least $\mathcal{B}^2 = 81$[1]. By combining S-boxes with the maximum differential probability equal to 2^{-5}, it was shown that no differential characteristic over four rounds of W has probability larger than $(2^{-5})^{81} = 2^{-405}$. Accordingly, it is estimated that the previous is enough to prevent differential attack on the full hash function.

However, we found that if certain type of vector is input to the matrix, the sum of hamming weight of input and output vectors is 8, implying that $\mathcal{B} < 9$. On the other hand, we have found that actually $\mathcal{B} = 8$. Accordingly, the number of S-boxes with a different input value in four consecutive rounds is estimated to be at least $\mathcal{B}^2 = 64$, which is lower than the estimation[1]. This implies a gap between potential security strength and previously estimated security strength of Whirlpool.

Also, we have explained why the branch number of the diffusion matrix appears to be 8, and we showed the candidates for the matrix which actually satisfy the conditions posed by the designers of Whirlpool.

[1] Previous version of this primitive, called Whirlpool-0, is obsolete. In this paper, we consider the final version of this primitive Whirlpool.

2 Definition

In this paper, we use the same definitions as in [1].

Definition 1. *Binary representation of $GF(2^8)$.*
An element $u = u_7x^7 + u_6x^6 + u_5x^5 + u_4x^4 + u_3x^3 + u_2x^2 + u_1x^1 + u_0$ of $GF(2^8)$ where $u_i \in GF(2)$ for all $i = 0, \ldots, 7$ will be denoted by the numerical value $u_7 \cdot 2^7 + u_6 \cdot 2^6 + u_5 \cdot 2^5 + u_4 \cdot 2^4 + u_3 \cdot 2^3 + u_2 \cdot 2^2 + u_1 \cdot 2 + u_0$. For instance, the polynomial $u = x^4 + x + 1$ will be represented by the hexadecimal byte value '13'.

Definition 2. *Hamming weight of vector in $GF(2^p)^k$.*
Let $v = (v_0, v_1, \ldots, v_{k-1}) \in GF(2^p)^k$. Hamming weight of the vector v is defined as follow:

$$w_h(v) = \sharp\{v_i \neq 0 | 0 \leq i \leq k-1\}.$$

Definition 3. *Branch Number.*
The branch number $\mathcal{B}$ of a linear mapping $\theta : GF(2^p)^k \rightarrow GF(2^p)^m$ is defined as:

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

Given a $[k+m, k, d]$ linear code over $GF(2^p)$ with generator matrix $G = [I_{k\times k} M_{k\times m}]$, the linear mapping $\theta : GF(2^p)^k \rightarrow GF(2^p)^m$ defined by $\theta(a) = a \cdot M$ has branch number $\mathcal{B}(\theta) = d$; if the code is MDS, such a mapping is called an optical diffusion mapping.

Definition 4. *Circulant matrix.*
$cir(a_0, a_1, \ldots, a_{m-1})$ stands for the $m \times m$ circulant matrix whose first row consists of elements $a_0, a_1, \ldots, a_{m-1}$, i.e.

$$cir(a_0, a_1, \ldots, a_{m-1}) \equiv \begin{pmatrix} a_0 & a_1 & \ldots & a_{m-1} \\ a_{m-1} & a_0 & \ldots & a_{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{pmatrix}.$$

3 The matrix in linear diffusion layer of Whirlpool

Whirlpool employs an 8×8 circulant matrix over $GF(2^8)$ in its diffusion layers. The field $GF(2^8)$ is represented as $GF(2)[x]/p(x)$, where $p(x) = x^8 + x^4 + x^3 + x^2 + 1$ is the primitive polynomial of degree 8.

The matrix C used in the diffusion layer of Whirlpool is defined as follows:

$$C = cir('01', '01', '03', '01', '05', '08', '09', '05')$$

$$= \begin{pmatrix} ‘01' & ‘01' & ‘03' & ‘01' & ‘05' & ‘08' & ‘09' & ‘05' \\ ‘05' & ‘01' & ‘01' & ‘03' & ‘01' & ‘05' & ‘08' & ‘09' \\ ‘09' & ‘05' & ‘01' & ‘01' & ‘03' & ‘01' & ‘05' & ‘08' \\ ‘08' & ‘09' & ‘05' & ‘01' & ‘01' & ‘03' & ‘01' & ‘05' \\ ‘05' & ‘08' & ‘09' & ‘05' & ‘01' & ‘01' & ‘03' & ‘01' \\ ‘01' & ‘05' & ‘08' & ‘09' & ‘05' & ‘01' & ‘01' & ‘03' \\ ‘03' & ‘01' & ‘05' & ‘08' & ‘09' & ‘05' & ‘01' & ‘01' \\ ‘01' & ‘03' & ‘01' & ‘05' & ‘08' & ‘09' & ‘05' & ‘01' \end{pmatrix}$$

Note that the designers claimed the following statement.

- **Statement 1**,[1]:Matrix C has been chosen to be an optical diffusion mapping obtained from $[16, 8, 9]$ linear code (MDS), and therefore the branch number $\mathcal{B} = 9$.

On the other hand, according to the square pattern propagation theorem, the number of S-boxes with a different input value in four consecutive rounds is at least $\mathcal{B}^2 = 81$[1].

4 Counterexample

On the contrary, we found a fact that the matrix C does not yield $\mathcal{B} = 9$.

For example, let $\alpha \in GF(2)[x]/p(x)$ and the vector $\mathbf{x} = (‘00', \alpha, ‘00', ‘00', ‘00', ‘00', \alpha, ‘00')$ is given as an input to the matrix, the output vector $\mathbf{y}$ will be:

$$\begin{aligned} \mathbf{y} &= \mathbf{x} \cdot C \\ &= (‘00', \alpha, ‘00', ‘00', ‘00', ‘00', \alpha, ‘00') \begin{pmatrix} ‘01' & ‘01' & ‘03' & ‘01' & ‘05' & ‘08' & ‘09' & ‘05' \\ ‘05' & \underline{‘01'} & ‘01' & ‘03' & ‘01' & \underline{‘05'} & ‘08' & ‘09' \\ ‘09' & ‘05' & ‘01' & ‘01' & ‘03' & ‘01' & ‘05' & ‘08' \\ ‘08' & ‘09' & ‘05' & ‘01' & ‘01' & ‘03' & ‘01' & ‘05' \\ ‘05' & ‘08' & ‘09' & ‘05' & ‘01' & ‘01' & ‘03' & ‘01' \\ ‘01' & ‘05' & ‘08' & ‘09' & ‘05' & ‘01' & ‘01' & ‘03' \\ ‘03' & \underline{‘01'} & ‘05' & ‘08' & ‘09' & \underline{‘05'} & ‘01' & ‘01' \\ ‘01' & ‘03' & ‘01' & ‘05' & ‘08' & ‘09' & ‘05' & ‘01' \end{pmatrix} \\ &= (‘06' \cdot \alpha, \underline{‘00'}, ‘04' \cdot \alpha, ‘0B' \cdot \alpha, ‘08' \cdot \alpha, \underline{‘00'}, ‘09' \cdot \alpha, ‘08' \cdot \alpha) \end{aligned}$$

In this case, $w_h(\mathbf{x}) + w_h(\mathbf{y}) = 2 + 6 = 8$. This property is contradiction with the above statement 1.

5 Discussion

The reason why this conflict happened is that the determinant of the sub-matrix which is constructed from underlined elements, $C_{1,1}, C_{1,5}, C_{6,1}, C_{6,5}$, is 0 (where

$C_{i,j}, (0 \leq i, j \leq 7)$, denotes an element in $(i+1)$-th row and $(j+1)$-th column of the matrix C).

$$det \begin{pmatrix} C_{1,1} & C_{1,5} \\ C_{6,1} & C_{6,5} \end{pmatrix} = det \begin{pmatrix} `01' & `05' \\ `01' & `05' \end{pmatrix} = 0$$

In total, there are 104 sub-matrices of C with determinants equal to 0 (see Appendix A). By further analysis, we have confirmed that there is no combination of $\mathbf{x}$ and $\mathbf{y}$ which hold $w_h(\mathbf{x}) + w_h(\mathbf{y}) \leq 7$ (see Appendix B). Thus the Whirlpool's matrix C holds the branch number $\mathcal{B} = 8$.

6 Matrices satisfying Whirlpool's condition

In this section, we show the search result for the matrices which actually satisfy the conditions posed by the designers of Whirlpool.

Recall that the designers of Whirlpool described the design criteria for choice of the diffusion layer as the followings:

1. the branch number is 9;
2. matrix C has as many 1-elements as possible (namely, 3);
3. the Hamming weight of any element is at most 2.

We have added the following condition to limit the search space implied by the condition 3.

– $C_{i,j} \in \{`01', `02', `03', `04', `05', `06', `08', `09'\}$.

Accordingly, we have found 224 matrices fulfilling the above conditions. These matrices are divided into 14 group of matrices, each group contains 16 matrices. The following 14 matrices are the representative matrix in the corresponding group.

$$\begin{aligned}
C_0 &= cir(`01', `01', `02', `01', `05', `08', `09', `04') \\
C_1 &= cir(`01', `01', `02', `01', `06', `09', `08', `03') \\
C_2 &= cir(`01', `01', `02', `01', `08', `09', `04', `05') \\
C_3 &= cir(`01', `01', `02', `01', `09', `06', `04', `03') \\
C_4 &= cir(`01', `01', `02', `06', `05', `09', `01', `08') \\
C_5 &= cir(`01', `01', `03', `01', `04', `09', `05', `06') \\
C_6 &= cir(`01', `01', `03', `01', `08', `04', `09', `06') \\
C_7 &= cir(`01', `01', `04', `01', `08', `05', `02', `09') \\
C_8 &= cir(`01', `01', `04', `01', `09', `03', `02', `06') \\
C_9 &= cir(`01', `01', `04', `03', `06', `08', `01', `09') \\
C_{10} &= cir(`01', `01', `05', `01', `04', `06', `03', `09') \\
C_{11} &= cir(`01', `01', `05', `08', `02', `09', `01', `06') \\
C_{12} &= cir(`01', `01', `08', `01', `06', `03', `02', `09') \\
C_{13} &= cir(`01', `01', `08', `02', `04', `05', `01', `09')
\end{aligned}$$

By applying reverse ordering of elements :

$$(a_0, a_1, \cdots, a_7) \rightarrow (a_7, a_6, \cdots, a_0),$$

and rotating elements :

$$(a_0, a_1, \cdots, a_7) \rightarrow (a_{(0+r) \mod 8}, a_{(1+r) \mod 8}, \cdots a_{(7+r) \mod 8}),$$

each circulant matrix generates additional 15 MDS matrices which follow the above conditions.

We note that the total Hamming weight of C_0, C_2, C_7, C_{13} is minimum (namely 10 in each row), and also note that the matrix C_0 is similar to the Whirlpool's matrix $C = cir(`01', `01', `03', `01', `05', `08', `09', `05')$, because C_0 can be obtained from C by replacing $`03' \rightarrow `02'$, the second $`05' \rightarrow `04'$, respectively.

7 Conclusion

We have proved that the branch number of the diffusion matrix employed in Whirlpool is equal to 8. And we have presented some matrices which satisfy the conditions posed by the designers of Whirlpool. Accordingly, this paper points out a fact about the matrix employed in W, but it is out of scope of this paper to discuss the impact of the branch number reduction to security level of Whirlpool. We only note that if the diffusion matrix are used continuously, more detailed analysis on immunity against the differential attack should be required.

Acknowledgment

We would like to thank Miodrag Mihaljevic for carefully reading of this paper.

References

1. P.S.L.M. Barreto and V. Rijmen, "The Whirlpool hashing function," Primitive submitted to NESSIE, https://www.cosic.esat.kuleuven.ac.be/nessie/tweaks.html, Sept. 2000.
2. R. Lidl and H. Niederreiter, "Finite Fields," Encyclopedia of mathematics and its applications 20, Cambridge Univ. Press, 1997.

Appendix A

The following table shows all the sub-matrices with determinant equal to 0. There are totally 104 matrices. A matrix is represented by a 2-tuple of vectors. The first vector indicates the choice of the row index of the diffusion matrix C, and the second one indicates the choice of the column index of C. For the chosen indexes, elements on the intersections are retrieved and formed into sub-matrix.

n = 2 (24)	((0,2),(2,4)) ((0,3),(3,7)) ((1,3),(3,5)) ((0,4),(0,3)) ((0,4),(4,7)) ((1,4),(0,4)) ((2,4),(4,6)) ((0,5),(0,4)) ((1,5),(1,4)) ((1,5),(0,5)) ((2,5),(1,5)) ((3,5),(5,7)) ((0,6),(0,2)) ((1,6),(1,5)) ((2,6),(2,5)) ((2,6),(1,6)) ((3,6),(2,6)) ((4,6),(0,6)) ((1,7),(1,3)) ((2,7),(2,6)) ((3,7),(3,6)) ((3,7),(2,7)) ((4,7),(3,7)) ((5,7),(1,7))
n = 3 (24)	((0,1,3),(1,2,5)) ((0,2,3),(3,4,6)) ((1,2,4),(2,3,6)) ((0,3,4),(2,4,5)) ((1,3,4),(4,5,7)) ((0,1,5),(1,2,7)) ((2,3,5),(3,4,7)) ((1,4,5),(3,5,6)) ((2,4,5),(0,5,6)) ((0,1,6),(1,2,4)) ((1,2,6),(0,2,3)) ((3,4,6),(0,4,5)) ((0,5,6),(2,6,7)) ((2,5,6),(4,6,7)) ((3,5,6),(1,6,7)) ((0,2,7),(0,1,4)) ((1,2,7),(2,3,5)) ((2,3,7),(1,3,4)) ((0,4,7),(0,1,6)) ((0,5,7),(0,1,3)) ((4,5,7),(1,5,6)) ((1,6,7),(0,3,7)) ((3,6,7),(0,5,7)) ((4,6,7),(0,2,7))
n = 4 (48)	((0,1,2,3),(2,3,5,7)) ((0,1,2,4),(2,4,5,7)) ((0,2,3,4),(2,5,6,7)) ((1,2,3,4),(0,3,4,6)) ((0,1,2,5),(3,4,5,7)) ((0,2,3,5),(3,5,6,7)) ((1,2,3,5),(0,3,5,6)) ((0,2,4,5),(4,5,6,7)) ((0,3,4,5),(0,2,6,7)) ((1,3,4,5),(0,3,6,7)) ((2,3,4,5),(1,4,5,7)) ((0,1,2,6),(0,3,4,5)) ((0,1,3,6),(1,3,4,5)) ((0,2,3,6),(2,3,4,5)) ((1,2,3,6),(0,4,5,6)) ((0,1,4,6),(0,1,2,3)) ((1,3,4,6),(0,4,6,7)) ((2,3,4,6),(1,4,6,7)) ((0,3,5,6),(0,1,2,6)) ((1,3,5,6),(0,5,6,7)) ((0,4,5,6),(0,1,3,6)) ((1,4,5,6),(0,1,3,7)) ((2,4,5,6),(0,1,4,7)) ((3,4,5,6),(0,2,5,6)) ((0,1,2,7),(1,2,4,6)) ((0,1,3,7),(1,3,4,6)) ((1,2,3,7),(1,4,5,6)) ((0,1,4,7),(2,3,4,6)) ((1,2,4,7),(2,4,5,6)) ((1,3,4,7),(3,4,5,6)) ((2,3,4,7),(1,5,6,7)) ((0,1,5,7),(2,3,4,7)) ((0,2,5,7),(0,2,3,4)) ((1,2,5,7),(1,2,3,4)) ((0,3,5,7),(0,1,2,7)) ((2,4,5,7),(0,1,5,7)) ((3,4,5,7),(0,2,5,7)) ((0,1,6,7),(0,1,3,5)) ((0,2,6,7),(0,2,3,5)) ((0,3,6,7),(1,2,3,5)) ((0,4,6,7),(1,2,3,6)) ((1,4,6,7),(1,2,3,7)) ((2,4,6,7),(0,1,6,7)) ((0,5,6,7),(0,2,4,7)) ((1,5,6,7),(1,2,4,7)) ((2,5,6,7),(0,1,2,4)) ((3,5,6,7),(0,1,2,5)) ((4,5,6,7),(1,3,6,7))
n = 5 (8)	((0,1,3,4,5),(1,2,5,6,7)) ((0,1,2,5,6),(2,3,4,6,7)) ((1,2,4,5,6),(0,2,3,6,7)) ((0,2,3,4,7),(0,1,4,5,6)) ((0,1,4,5,7),(1,2,3,5,6)) ((1,2,3,6,7),(0,3,4,5,7)) ((0,3,4,6,7),(0,1,2,4,5)) ((2,3,5,6,7),(0,1,3,4,7))

n: dimension of matrix, ( ):number of matrices

Appendix B

To check the branch number of the diffusion matrix, the following lemma was used.

Lemma 1. *[2] A linear code LC with parity-check matrix H has minimum distance $d_{LC} \geq s + 1$ if and only if any s columns of H are linearly independent.*

Since, the generator matrix G is

$$G = [I_{8\times 8}C],$$

the parity-check matrix H is

$$H = [-C^T I_{8\times 8}] = [C^T I_{8\times 8}].$$

We checked all possible combinations of 7 columns in H, and found that there is no combination of 7 columns which is linearly dependent. Therefore

$$d_{LC} \geq 8.$$

Since an example of code word whose hamming weight is equal to 8 has been presented in section 4, and thus we can conclude that

$$d_{LC} = \mathcal{B} = 8$$