EVALUATING THE NUMBER OF ACTIVE S-BOXES IN DYNAMIC AES BLOCK CIPHERS USING MDS MATRICES OF SIZE 4×4 AND 8×8

Truong Minh Phuong*, Tran Thi Luong
Academy of Cryptography Techniques

ARTICLE INFO

Received: 25/10/2023
Revised: 27/12/2023
Published: 27/12/2023

KEYWORDS

Active S-boxes
AES block cipher
Dynamic MDS matrices
Linear branch number
The number of differential branches

ABSTRACT

AES (Advanced Encryption Standard) was designed by two Belgian cryptographers: Joan Daemen and Vincent Rijmen. AES was recognized as a federal encryption standard by the US National Institute of Standards and Technology on November 26, 2001 and is specified in Federal Information Processing Standard 197 (FIPS 197). However, there have been a number of threats to the security of AES by strong cryptanalysis attacks such as linear, differential cryptanalysis attacks and their variations. Therefore, cryptographic researchers are proposing diverse methods to implement this block cipher dynamically in order to enhance its security. Evaluating the security level of dynamic AES block ciphers is also a significant concern. In this paper, we demonstrate the minimum number of active S-boxes across each four rounds in dynamic AES block ciphers with corresponding 4×4 and 8×8 MDS matrices as 25 and 27, respectively. Subsequently, we assess the number of active S-boxes across the rounds of dynamic AES block ciphers using 4×4 and 8×8 MDS matrices as a basis to demonstrate the security of the dynamic AES block ciphers against linear and differential cryptanalysis across the rounds.

ĐÁNH GIÁ SỐ HỘP S HOẠT ĐỘNG CỦA MÃ KHỐI AES CẢI BIÊN ĐỘNG VỚI CÁC MA TRẬN MDS CỠ 4×4 VÀ 8×8

Trương Minh Phương*, Trần Thị Lượng
Học viện Kỹ thuật mật mã

THÔNG TIN BÀI BÁO

Ngày nhận bài: 25/10/2023
Ngày hoàn thiện: 27/12/2023
Ngày đăng: 27/12/2023

TỪ KHÓA

Hộp S hoạt động
Mã khối AES
Ma trận MDS động
Số nhánh tuyến tính
Số lượng nhánh lượng sai

TÓM TẮT

AES (Advanced Encryption Standard - Tiêu chuẩn mã hóa tiên tiến) được thiết kế bởi hai nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen. AES được Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ công nhận là tiêu chuẩn mã hóa liên bang vào ngày 26/11/2001 và được đặc tả trong Tiêu chuẩn Xử lý thông tin Liên bang 197 (Federal Information Processing Standard - FIPS 197). Tuy nhiên, đã có một số các nguy cơ gây ra mất an toàn cho AES bởi các tấn công thám mã mạnh như tấn công thám mã tuyến tính, lượng sai và các biến thể của chúng. Do đó, các nhà nghiên cứu mật mã đang đề xuất nhiều phương pháp khác nhau để làm động mã khối này nhằm nâng cao độ an toàn của nó. Việc đánh giá độ an toàn của các mã khối AES động cũng là một vấn đề quan trọng được quan tâm. Trong bài báo này, chúng tôi chứng minh số tối thiểu các hộp S hoạt động qua mỗi bốn vòng của các mã khối AES cải biên động với các ma trận MDS cỡ 4×4 và 8×8 tương ứng bằng 25 và 27. Sau đó, chúng tôi đánh giá số hộp S hoạt động qua các vòng của mã khối AES động với các ma trận MDS cỡ 4×4 và 8×8 làm cơ sở chứng minh độ an toàn của mã khối AES động chống lại thám tuyến và thám lượng sai qua các vòng.

DOI: https://doi.org/10.34238/tnu-jst.9053

* Corresponding author. *Email: minhphuongh19@gmail.com*

1. Introduction

The block cipher is an important component of symmetric key cryptography. In addition to being used directly to build security programs, block ciphers also serve as an important component in many different security applications. Currently, there are many different types of block cipher structures, but the SPN structure is one of the most popular structures used to design block cipher algorithms. The SPN structure consists of three layers in a loop: substitution, permutation, and key addition. The substitution layer is nonlinear in a block cipher that creates confusion through the use of substitution boxes called S-boxes. The permutation layer is responsible for diffusing the cryptographic characteristics of the substitution layer through linear transformations. The key addition layer is responsible for adding the states of the block cipher with the round subkeys to create the input in the next round of the substitution layer.

There are many types of SPN block cipher that are used in practical applications as AES (Rijndael) [1], Kalyna [2], PRESENT [3], SAFER [4], SHARK [5], Square [6], and so on. However, AES is the most widely used block cipher in the field of information security. AES (Advanced Encryption Standard) is a US government standard block cipher algorithm that is specified in Federal Information Processing Standard 197 (FIPS 197) and is released on November 26, 2001 by the National Institute of Standards and Technology (NIST).

To enhance the strength of AES block ciphers, researchers often hide one or more components in AES by making this information dynamic. There are many studies aimed at the dynamic method of the diffusion layer, such as in [7] - [12]... One of the other research directions receiving a lot of attention is the dynamic substitution layer. With the dynamic AES S-box direction, there is a variety of research works in this direction as in [13] - [19]. These works generate dynamic S-boxes depending on a secret key based on the initial S-box, this initial S-box is usually the original AES S-box. Additionally, in [20], [21] the authors generate key-dependent dynamic XOR tables, instead of using the conventional binary XOR table used in AES.

In terms of evaluating the safety of current dynamic block cipher algorithms, evaluating their actual safety is a common way used by scientists. One of the first studies on actual safety was published by Knudsen et al. [22]. They defined practical security against linear and differential cryptanalysis of the DES block cipher by showing the non-existence of a feature (correspondingly differential and linear) with sufficiently high probability to successful attack. That is, they showed that a cipher is practically secure when the lower bound on the complexity of the features can be sufficiently small. Another approach was proposed by Daemen, J. and Rijmen, V. in [1], which is to count the minimum number of active S-boxes (differential and linear) across rounds of the block cipher, this is used in the Wide Trail Strategy of AES. In this study, the authors also demonstrated that every 4 rounds of AES has a minimum of 25 active S-boxes.

In general, these proposed dynamic block ciphers are often evaluated for security based on the evaluation of statistical criteria that are not enough to express the security of dynamic block ciphers. In [13], [14], the authors proposed and implemented dynamic algorithms and applied dynamic modification to AES with MDS matrices of sizes $4, 8, 16$. However, the author has only shown the branch number of these matrices, and the number of active S-boxes through rounds of dynamic AES. The security of the dynamic AES block ciphers against differential and linear attacks is based on this number of active S-boxes. Up to now, there has been no research that specifically indicates the number of S-boxes operating through rounds of the dynamic AES block cipher.

In this paper, we demonstrate the minimum number of active S-boxes for the case of dynamic AES using dynamic MixColumn transformations with 4×4 and 8×8 dynamic MDS matrices. Then, we assess the number of active S-boxes across the rounds of the dynamic AES block cipher using 4×4 and 8×8 MDS matrices. From these results, we can indicate the security level of dynamic AES block cipher against linear and differential cryptanalysis through the rounds.

The remaining part of the paper is structured as follows. Section 2 presents the preliminaries and related works. Section 3 evaluates the number of active S-boxes across the rounds of dynamic AES block ciphers using 4×4 and 8×8 MDS matrices. Section 4 assesses the security of the dynamic AES block cipher against linear and differential cryptanalysis through the rounds. The final section is the conclusion.

2. Materials and Methods

2.1. Branch number of a linear transformation

Definition 1 [23], [24]. *The linear branch number of a linear transformation* $F: (GF(2^m))^n \rightarrow (GF(2^m))^n$ *is defined by:*

$$\beta_l = min_{a \neq 0}(W(a) + W(F(a))),$$

where $W(a)$ *is the number of non-zero components (or positions) of the vector* $a \in (GF(2^m))^n$.

For each component of a is the input to the diffusion layer (output of the substitution layer) and $F(a)$ is the output of this diffusion layer (input to the next substitution layer), so the branch number is also the minimum number of active S-boxes in two consecutive rounds of an SPN block cipher. According to [23], [24], β is a measure of the diffusion of F in the sense that the larger β is, the better the diffusion is.

Definition 2 [23], [24].

In the SPN block cipher, the number of differential branch number β_d *of the linear transformation* θ*:* $(GF(2^m))^n \rightarrow (GF(2^m))^n$ *of the diffusion layer is defined as follows.*

$$\beta_d = min_{\Delta X \neq 0}(W(\Delta X) + W(\theta(\Delta X)))$$

where ΔX *is the input difference of the diffusion layer and* $\theta(\Delta X)$ *is the output difference of this layer.*

It is also shown in [25] that the MDS matrix has a maximum of linear and differential branch number and the two branch numbers are the same. MDS matrices of size 4×4 have the branch number 5, it's 9 for size 8×8, and it's 17 for size 16×16.

2.2. The number of active S-boxes in AES

In [1], the authors of AES indicated the number of active S-boxes of AES as follows:

Theorem 3 [1]. *Any differential/linear characteristic over 4 rounds of AES has at least 25 active S-boxes.*

3. Results and Discussion

In this section, we prove that the number of active S-boxes per four rounds of dynamically modified AES block ciphers with MDS matrices of size 4×4 and 8×8 are 25 and 27, respectively. Next, we evaluate the number of active S-boxes over rounds of a dynamic AES block cipher with MDS matrices of size 4×4 and 8×8. We then show how secure the dynamic AES block cipher is against differential and linear attack across rounds.

3.1. Evaluating the number of active S-boxes across the rounds of the dynamic AES block cipher using 4×4 MDS matrices

The notations for the dynamic AES transformations are as follows.

SubByte = Sub, ShiftRow = Shift, MixColumn = Mix_{4x4}. In this context, Mix_{4x4} denotes the MixColumn transformation using a dynamic key-dependent 4×4 MDS matrix.

Notations:

B_i represents the number of active S-boxes in round i.

The input state array for round 1 is A of size 4×4 with one active byte.

The matrices A_i are the results of the transformations SubByte, ShiftRow, Mix_{4x4} across the rounds.

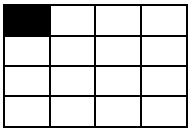
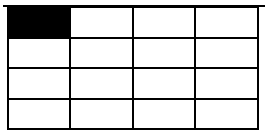
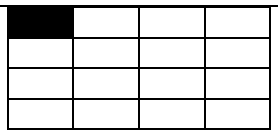
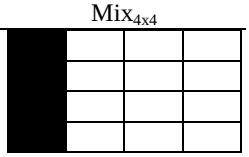
To find the minimum number of active S-boxes across the rounds of the dynamic AES, we will consider the "worst-case" scenarios to minimize the number of active S-boxes as much as possible.

Proposition 1. *The minimum number of active S-boxes across every* 4 *rounds of the dynamic AES block cipher using a* 4×4 *MDS matrix in the MixColumn transformation is* 25.

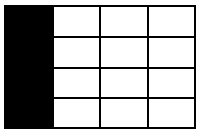
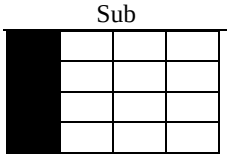
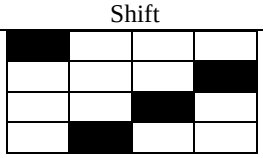
Proof.

We prove this proposition based on the tabular form through rounds.

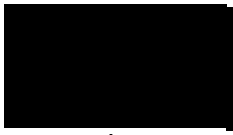
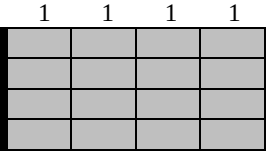
Round 1:

Input	Round 1			Number of active S-boxes
	Sub	Shift	Mix_{4x4}	
				$B_1 = 1$
A	A_1	A_2	A_3	
	Without loss of generality, we consider the non-zero byte located in the leftmost corner of the state.		Since the 4×4 MDS matrix has branch number equal to 5, at least 4 bytes in column 1 of A_3 are nonzero.	

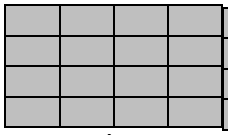
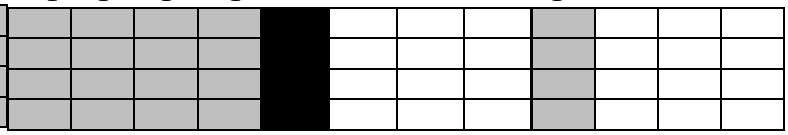
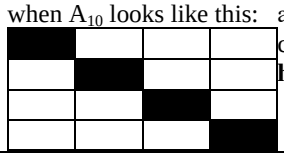
Round 2:

Input	Round 2			Number of active S-boxes
	Sub	Shift	Mix_{4x4}	
				$B_2 = 4$
A_3	A_4	A_5	A_6	
		The ShiftRow transformation shifts the active bytes of A_4, resulting in A_5	Because the 4×4 MDS matrix has branch number equal to 5, each column of A_6 must have 4 non-zero bytes. Therefore, A_6 has 16 non-zero bytes.	

Round 3:

Input	Round 3			Number of active S-boxes
	Sub	Shift	Mix_{4x4}	
			1 1 1 1	
				$B_3 = 16$
A_6	A_7	A_8	A_9	
		The ShiftRow transformation shifts the active bytes of A_7, resulting in A_8	Since the 4×4 MDS matrix has branch number equal to 5, each column of A_9 has at least one non-zero byte. In the "worst" case, **each column of A_9 has 1 nonzero byte.**	

Round 4:

Input	Round 4			Number of active S-boxes
	Sub	Shift	Mix_{4x4}	
1 1 1 1	1 1 1 1		1	
				$B_4 = 4$
A_9	A_{10}	A_{11}	A_{12}	
		Consider the "worst" case: through the ShiftRow transformation, the 4 active bytes of A_{10} are pushed to the same column. For example, when A_{10} looks like this: 	Since the 4×4 MDS matrix has branch number equal to 5, column 1 of A_{12} has at least one non-zero byte. The remaining columns are all 0. In the "worst" case, **column 1 of A_{12} has 1 byte other than 0.**	

The result of round 4 will be array A_{12} containing only one non-zero byte in column 1, and A_{12} will be the input of round 5. Thus, the operation of round 5 will be similar to round 1. Then 4 next rounds (rounds 5, 6, 7, 8) will work similarly to rounds 1, 2, 3, 4. The rounds after that (after round 8) will work similarly according to the same rules.

Thus, for every 4 rounds of dynamic AES using a 4×4 MDS matrix in the Mixcolumn transformation, there will be at least 25 active S-boxes.

Through the above evaluation, we can sum up the number of S-boxes operating through each round, and the total number of active S-boxes through rounds of dynamic AES using a 4×4 MDS matrix as shown in Table 1 below.

Table 1. *Number of active S-boxes through rounds of dynamic AES using a 4×4 MDS matrix*

Round	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Number of active S-boxes of each round	1	4	16	4	1	4	16	4	1	4	16	4	1	4
Total number of active S-boxes across rounds	1	5	21	**25**	26	30	46	**50**	51	55	71	**75**	72	76

3.2. Evaluating the number of active S-boxes across the rounds of the dynamic AES block cipher using 8×8 MDS matrices

The notations for the dynamic AES transformations are as follows.

SubByte = Sub, ShiftRow = Shift, MixColumn = Mix_{8x8}. In this context, Mix_{8x8} denotes the MixColumn transformation using a dynamic key-dependent 8×8 MDS matrix.

Notations:

C_{8x2} is the transformation of a 4×4 array into an 8×2 array, and C_{4x4} is the transformation of an 8×2 array into a 4×4 array,

B_i represents the number of active S-boxes in round i.

The input state array for round 1 is A of size 4×4 with one active byte.

The matrices A_i are the results of the transformations SubByte, ShiftRow, Mix_{4x4} across the rounds.

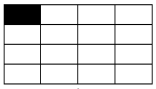
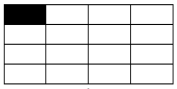
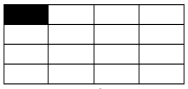
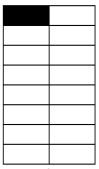
To find the minimum number of active S-boxes across the rounds of the dynamic AES, we will consider the "worst-case" scenarios to minimize the number of active S-boxes as much as possible.

Proposition 2. *The minimum number of active S-boxes across every 4 rounds of the dynamic AES block cipher using a* 8×8 *MDS matrix in the MixColumn transformation is 27.*

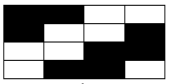
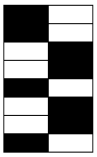
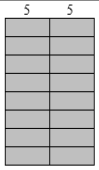
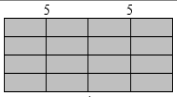
Proof.

We prove this proposition based on the tabular form through rounds.

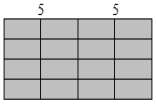
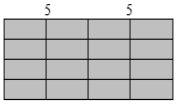
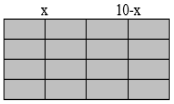
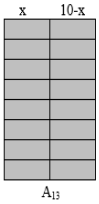
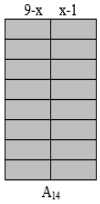
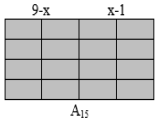
Round 1:

Input	Round 1					Number of active S-boxes
	Sub	Shift	C_{8x2}	Mix_{8x8}	C_{4x4}	
 A	 A_1	 A_2	 A_3	 A_4	 A_5	$B_1 = 1$
	Without loss of generality, we consider the non-zero byte located in the leftmost corner of the state.			Since the 8×8 MDS matrix has branch number equal to 9, at least 8 bytes in column 1 of A_4 are nonzero.		

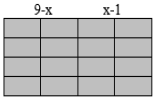
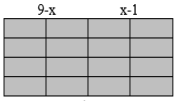
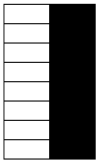
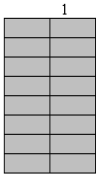
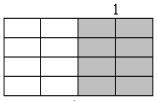
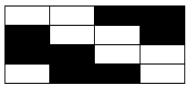
Round 2:

Input	Round 2					Number of active S-boxes
	Sub	Shift	C_{8x2}	Mix_{8x8}	C_{4x4}	
 A_5	 A_6	 A_7	 A_8	5 5  A_9	5 5  A_{10}	$B_2 = 8$
				Because the 8×8 MDS matrix has branch number equal to 9, at least 5 bytes in column 1 and 5 bytes in column 2 of A_9 are non-zero. Consider the "worst" case: Both columns of A_9 have 5 non-zero bytes.	The two left half columns and the two right half columns of A10 all have 5 non-zero bytes	

Round 3:

Input	Round 3					Number of active S-boxes
	Sub	Shift	C_{8x2}	Mix_{8x8}	C_{4x4}	
5 5  A_{10}	5 5  A_{11}	x 10-x  A_{12}	x 10-x  A_{13}	9-x x-1  A_{14}	9-x x-1  A_{15}	$B_3 = 10$
		Because A_{11} has 10 non-zero bytes, through the ShiftRow transformation, there are definitely at least 2 non-zero bytes in the two left half columns or in the two right half columns of A_{12}. We denote the two left half columns as having x $(2 \leq x \leq 8)$ non-zero bytes, then the two right half columns as having $(10 - x)$ non-zero bytes.	Column 1 of A_{13} has x $(2 \leq x \leq 8)$ non-zero bytes, column 2 of A_{13} has (10-x) non-zero bytes.	Because the 8×8 MDS matrix has 9 branches, at least $(9 - x)$ bytes in column 1 and $(x - 1)$ bytes in column 2 of A_{14} are non-zero. Consider the "worst" case: Column 1 of A_{14} has $(9 - x)$ non-zero bytes, column 2 has $(x - 1)$ non-zero bytes The total number of non-zero bytes of A_{14} is equal to 8.	The two left half columns of A_{15} have $(9 - x)$ non-zero bytes, the two right half columns have $(x - 1)$. The total number of non-zero bytes in A_{15} is 8.	

Round 4:

Input	Round 4					Number of active S-boxes
	Sub	Shift	C_{8x2}	Mix_{8x8}	C_{4x4}	
9-x x-1  A_{15}	9-x x-1  A_{16}	 A_{17}	 A_{18}	1  A_{19}	1  A_{20}	$B_4 = 8$
	The two left half columns of A_{16} have $(9-x)$ non-zero bytes, the two right half columns have $(x-1)$. The total number of non-zero bytes of A16 is equal to 8.	Because A_{16} has 8 non-zero bytes, through the ShiftRow transformation, in the worst" case occurs when all 8 non-zero bytes are pushed to the two left half columns or two right half columns of A_{17}. For example, when A_{16} has the following form: 		Since the 8 × 8 MDS matrix has branch number equal to 9 , there is at least 1 non-zero byte in column 2 of A_{19}. Column 1 has all bytes 0. Consider the "worst" case: Column 1 of A_{19} has all bytes 0, and column 2 has one non-zero byte.	The two left half columns of A20 are all 0 bytes, the two right half columns have 1 non-zero byte.	

The result of round 4 will be the array A_{20} containing only one non-zero byte in the two right half columns, and A_{20} will be the input of round 5. Thus, the operation of round 5 will be the same as round 1. Therefore, 4 next rounds (round 5, 6, 7, 8) will work the same way as round 1, 2, 3, 4. The rounds after that (after round 8) will work similarly according to the same rules. Thus, for every 4 rounds of the dynamic AES, there will be 27 active S-boxes.

Through the above evaluation, we can sum up the number of S-boxes operating through each round, and the total number of active S-boxes through rounds of dynamic AES with an 8×8 MDS matrix in the Mixcolumn transformation as shown in Table 2.

Table 2. *Number of active S-boxes through rounds of dynamic AES using a* 8×8 *mds matrix*

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Number of active S-boxes of each round	1	8	10	8	1	8	10	8	1	8	10	8	1	8
Total number of active S-boxes across rounds	1	9	19	**27**	28	36	46	**54**	55	63	73	**81**	82	90

3.3. Evaluate the security of dynamic AES block ciphers against linear and differential cryptanalysis across rounds

In this section, we evaluate the practical security of dynamic AES block ciphers following the approach of Knudsen [22]. Therefore, we evaluate the number of active S-boxes over rounds of a dynamic AES block cipher with MDS matrices of size 4×4 and 8×8 with a secret key of length 128 bits.

Note here that, because the AES block cipher is dynamic, some components of the AES will be “hidden”, such as the S-box or the MDS matrix in the Mixcolumn transformation. They will be dynamic and key-dependent components. Therefore, in addition to evaluating the safety based on the number of active S-boxes, the security of dynamic AES will be multiplied by the number of dynamic S-boxes or the number of dynamic MDS matrices. We assume that the total number of possible dynamic parameters is c. Then, the security against linear and differential cryptanalysis of dynamic AES with dynamic MDS matrices of size 4×4 and 8×8 are presented in Tables 3 and 4. In addition, dynamic S-boxes, if used for dynamic AES, are also guaranteed to preserve the good cryptographic properties of AES S-box, so dynamic S-boxes also have the following parameters.

The deviation in linear cryptanalysis $\delta_{max} = 2^{-3}$.
The maximum differential probability $DP_{max} = 2^{-6}$.

Table 3. *Safety of dynamic AES with* 4×4 *MDS matrix*

Round	Differential cryptanalysis		Linear cryptanalysis	
	Upper bound of the differential probability	Data Complexity	Upper bound of the deviation	Data Complexity
1	2^{-6}	2^{6+c}	2^{-3}	$2^{3+\mathbf{c}}$
2	2^{-30}	2^{30+c}	2^{-15}	$2^{15+\mathbf{c}}$
3	2^{-126}	$2^{126+\mathbf{c}}$	2^{-63}	$2^{63+\mathbf{c}}$
4	2^{-150}	$2^{150+\mathbf{c}}$	2^{-75}	$2^{75+\mathbf{c}}$
5	2^{-156}	$2^{156+\mathbf{c}}$	2^{-78}	$2^{78+\mathbf{c}}$
6	2^{-180}	$2^{180+\mathbf{c}}$	2^{-90}	$2^{90+\mathbf{c}}$
7	2^{-276}	$2^{276+\mathbf{c}}$	2^{-138}	$2^{138+\mathbf{c}}$
8	2^{-300}	$2^{300+\mathbf{c}}$	2^{-150}	$2^{150+\mathbf{c}}$
9	2^{-306}	$2^{306+\mathbf{c}}$	2^{-153}	$2^{153+\mathbf{c}}$
10	2^{-330}	$2^{330+\mathbf{c}}$	2^{-165}	$2^{165+\mathbf{c}}$

Table 4. *Security of dynamic AES with* 8×8 *MDS matrix*

Round	Differential cryptanalysis		Linear cryptanalysis	
	Upper bound of the differential probability	Data Complexity	Upper bound of the deviation	Data Complexity
1	2^{-6}	2^{6+c}	2^{-3}	$2^{3+\mathbf{c}}$
2	2^{-54}	2^{54+c}	2^{-15}	$2^{15+\mathbf{c}}$
3	2^{-114}	2^{114+c}	2^{-63}	$2^{63+\mathbf{c}}$
4	2^{-162}	2^{162+c}	2^{-75}	$2^{75+\mathbf{c}}$
5	2^{-168}	2^{168+c}	2^{-78}	$2^{78+\mathbf{c}}$
6	2^{-216}	2^{216+c}	2^{-90}	$2^{90+\mathbf{c}}$
7	2^{-276}	2^{276+c}	2^{-138}	$2^{138+\mathbf{c}}$
8	2^{-324}	2^{324+c}	2^{-150}	$2^{150+\mathbf{c}}$
9	2^{-330}	2^{330+c}	2^{-153}	$2^{153+\mathbf{c}}$
10	2^{-378}	2^{378+c}	2^{-165}	$2^{165+\mathbf{c}}$

From this result, we can show how secure the dynamic AES block ciphers against linear and differential cryptanalysis across rounds. Obviously, the security of dynamic AES block ciphers is higher than that of the original AES block cipher. For example, $c = 50$, the actual security of dynamic AES is also greatly increased, which is especially meaningful in practice.

4. Conclusion

In this paper, we have demonstrated the number of active S-boxes across each 4-round and the total number of active S-boxes across rounds for dynamic AES using the dynamic Mixcolumn transformation. In which, the original AES with the 4×4 MDS matrix is replaced by key-dependent $4 \times 4, 8 \times 8$ dynamic MDS matrices. We then evaluate the number of active S-boxes over rounds of the dynamic AES block cipher with MDS matrices of size 4×4 and 8×8. From this result, we can show how secure the dynamic AES block cipher is against linear and differential cryptanalysis across rounds. This is the important mathematical basis to prove the practical security of AES dynamic block cipher against strong attacks such as linear and differential cryptanalysis. This result is very useful as an important basis for us to develop future dynamic AES algorithms to improve the robustness of AES. In the next studies, we will research to show the number of active S-boxes through each four rounds of dynamically modified AES block ciphers with MDS matrices of size $n \times n$ with $n = 2^k$ where k is the non-zero positive integer.

TÀI LIỆU THAM KHẢO/ REFERENCES

[1] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard.* Springer, *2002.*

[2] S. K. Gupta, M. Ghosh, and S. K. Mohanty, "Cryptanalysis of Kalyna Block Cipher Using Impossible Differential Technique," *Proceedings of the Sixth International Conference on Mathematics and Computing. Advances in Intelligent Systems and Computing*, vol. 1262, pp. 162-166, 2020.

[3] G. A. W. S. Wang, "Differential fault analysis on PRESENT key schedule," *International Conference on Computational Intelligence and Security*, 2010, pp. 362-366.

[4] J. Kelsey, B. Schneier, and D. Wagner, "Key-schedule cryptanalysis of idea, g-des, gost, safer, and triple-des," *Annual international cryptology conference*, Springer, 1996, pp. 237-251.

[5] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. D. Win, "The cipher SHARK," *International Workshop on Fast Software Encryption*, 1996, pp. 99-111.

[6] J. Daemen, L. Knudsen, and V. Rijmen, "The block cipher Square," *International Workshop on Fast Software Encryption*, 1997, pp. 149–165.

[7] G. Murtaza, A. A. Khan, and S. W. Alam, *Fortification of aes with dynamic mix-column transformation*, IACR Cryptology ePrint Archive, ISBN-10: 3659363634, 2011, p. 184.

[8] R. W. Mohamed, M. Abdulrashid, S. M. Moesfa, and M. Ramlan, "A method for linear transformation in substitution permutation network symmetric-key block cipher," *International application published under the patent cooperation treaty*, 2012, pp. 3-14.

[9] A. H. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. Udzir, "A new DNA based approach of generating key dependent Mixcolumns transformation," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 7, no. 2, pp. 33-38, 2015.

[10] T. T. Luong, "Building the dynamic diffusion layer for SPN block ciphers based on direct exponent and scalar multiplication," *Journal of Science and Technology on Information Security*, vol. 1, no CS(15), pp. 38-45, 2022.

[11] T. T. Luong, "Constructing Recursive MDS Matrices Effective for Implementation from Reed-Solomon Codes and Preserving the Recursive Property of MDS Matrix of Scalar Multiplication," *Journal of Informatics & Mathematical Sciences*, vol. 11, no 2, pp. 155-177, 2019.

[12] T. T. Luong, "Proposals and implementations of MDS diffusion layer dynamic algorithms for AES block cipher," *Journal on Information technologies & Communication*, vol. 2023, no. 2, pp. 28-35, 2022.

[13] Abd-ElGhafar, A. Rohiem, A. Diaa, and F. Mohammed , "Generation of aes key dependent s-boxes using rc4 algorithm," *13th International Conference on Aerospace Sciences & Aviation Technology, ASAT- 13*, 2009, pp. ASAT-13-CE-24.

[14] K. Kazlauskas and J. Kazlauskas, "Key-dependent s-box generation in aes block cipher system," *INFORMATICA*, vol. 20, no. 1, pp. 23-34, 2009.

[15] R. Hosseinkhani and H. H. S. Javadi, "Using cipher key to generate dynamic s-box in aes cipher system," *International Journal of Computer Science and Security (IJCSS)*, vol. 6, pp. 32-38, 2012.

[16] E. M. Mahmoud, A. A. E. Hafez, T. A. Elgarf, and A. Zekry, "Dynamic aes-128 with key-dependent s-box," *International Journal of Engineering Research and Applications*, vol. 3, no 1, pp. 1662-1670, 2013.

[17] J. Juremi, R. Mahmod, Z. A. Zukarnain, and S. M. Yasin, "Modified AES s-box Based on Determinant Matrix Algorithm," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7, no 1, pp. 162-168, 2017.

[18] P. Agarwal, A. Singh, and A. Kilicman, "Development of key-dependentdynam ic s-boxes with dynamic irreducible polynomial and affine constant," *Advances in mechanical engineering*, vol. 10, no. 7, pp. 1–18, 2018.

[19] H. T. Assafli, and I. A. Hashim, "Generation and Evaluation of a New Time-Dependent Dynamic s-box Algorithm for AES Block Cipher Cryptosystems," *3rd International Conference on Recent Innovations in Engineering (ICRIE 2020), Materials Science and Engineering*, 2020, pp. 62-68.

[20] A. I. Salih, A. Alabaichi, and A. S. Abbas, "A novel approach for enhancing security of advance encryption standard using private Xor table and 3d chaotic regarding to software quality factor," *ICIC Express Letters Part B: Applications*, vol. 10, no 9, pp. 1574 -1581, 2019.

[21] A. Salih, A. Alabaichi, and A. Y. Tuama, "Enhancing advance encryption standard security based on dual dynamic XOR table and mixcolumns transformation," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 19, no. 3, pp. 1574 -1581, 2020.

[22] L. R. Knudsen, *Practically secure Feistel ciphers, S*pringer Berlin Heidelberg, 1993, pp. 211-221.

[23] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. D. Win, "The cipher shark," in *Fast Software Encryption.* Springer, 1996, pp. 99-111.

[24] R. Elumalai and A. R. Reddy, "Improving diffusion power of aes rijndael with 8x8 mds matrix," *International Journal of Scientific & Engineering Research,* vol. 2, pp. 1-5, 2011.

[25] J. S. Kang, S. Hong, S. Lee, O. Yi, C. Park, and J. Lim, "Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks," *ETRI Journal*, vol. 23, no 4, pp. 49-55, 2001.