How to cite this paper:

Hussien, H. M., Muda, Z., & S., Yasin, S. M. (2018). New key expansion function of Rijndael 128-bit resistance to the related-key attacks. *Journal of Information and Communication Technology, 19* (3), 409-434.

NEW KEY EXPANSION FUNCTION OF RIJNDAEL 128-BIT RESISTANCE TO THE RELATED-KEY ATTACKS

Hassan Mansur Hussien, Zaiton Muda & Sharifah Md Yasin
Faculty of Computer Science and Information Technology,
Universiti Putra Malaysia, Malaysia

hassanalobady@gmail.com; zaitonm@upm.edu.my: ifah@upm.edu.my

ABSTRACT

A master key of special length is manipulated based on the key schedule to create round sub-keys in most block ciphers. A strong key schedule is described as a cipher that will be more resistant to various forms of attacks, especially in related-key model attacks. Rijndael is the most common block cipher, and it was adopted by the National Institute of Standards and Technology, USA in 2001 as an Advance Encryption Standard. However, a few studies on cryptanalysis revealed that a security weakness of Rijndael refers to its vulnerability to related-key differential attack as well as the related-key boomerang attack, which is mainly caused by the lack of nonlinearity in the key schedule of Rijndael. In relation to this, constructing a key schedule that is both efficient and provably secure has been an ongoing open problem. Hence, this paper presents a method to improve the key schedule of Rijndael 128-bit for the purpose of making it more resistance to the related-key differential and boomerang attacks. In this study, two statistical tests, namely the Frequency test and the Strict Avalanche Criterion test were employed to respectively evaluate the properties of bit confusion and bit diffusion. The results showed that the proposed key expansion function has excellent statistical properties and agrees with the concept of Shannon's diffusion and confusion bits. Meanwhile, the Mixed

Received: 19 November 2017 **Accepted**: 10 April 2018 **Published:** 12 June 2018

Integer Linear Programming based approach was adopted to evaluate the resistance of the proposed approach towards the related-key differential and boomerang attacks. The proposed approach was also found to be resistant against the two attacks discovered in the original Rijndael. Overall, these results proved that the proposed approach is able to perform better compared to the original Rijndael key expansion function and that of the previous research.

Keywords: Jey expansion function, related-key attacks, Rijndael Cipher, Mixed Integer Linear Programming, active s-boxes.

INTRODUCTION

A secret key block cipher is crucial in primitive cryptography. Generally, one fundamental motivation behind the use of a block cipher is to protect the information that are transmitted in insecure communication environments. On top of that, block ciphers are applied as a component in different security domains, which probably requires the construction of other secret key cryptographic primitives such as cryptographic pseudorandom number generators, message authentication codes, and hash functions. Nowadays, Rijndael has become the most common block cipher that is used as a standard for symmetric encryption in many countries (Lu, 2015). Moreover, it has also been extensively applied as a significant symmetric block cipher algorithm in the computer security field.

The Rijndael algorithm encryption was adopted as an Advanced Encryption Standard (AES) in 2001 by the National Institute of Standards and Technology (NIST) (Daemen & Rijmen, 2013). As a result, it promotes the vast adoption of Rijndael for commercial and governmental purposes by focusing on both hardware and software implementation. Furthermore, it is an agile design with an extremely effective and efficient performance cipher. In regard to this, a recent cryptanalysis study managed to unearth certain security weaknesses in the Rijndael (Biryukov & Khovratovich, 2009; Biryukov et al., 2010; Biryukov & Nikolić, 2010; Jean, 2013; Cui et al., 2015). The findings of the study revealed that three variants of the Rijndael which are 128, 192, and 256 bits of keys are not equipped with the ideal resistance or level of security against the related-key model attack considering that the adversary can encrypt plaintexts or decrypt ciphertext under a set of keys connected via a known relationship. More importantly, it should be noted that these attacks are only theoretical and require computational power that is beyond our reach. Nevertheless, the problem of producing Rijndael algorithm with an ideal resistance in the face

of the cryptographic standards has remained unsolved for quite some time. On a more important note, it has been widely acknowledged that the key expansion function of Rijndael is the weakest point of its design, whereas the round function has been very strongly and securely designed. Therefore, the current research aims to emphasize only on the key expansion function of Rijndael with the unchanged state transformation round function

DESCRIPTION THE SECURITY OF RIJNDAEL

Rijndael is a block cipher that contains both variable block length and variable key length. The block length and key length can be independently specified as any multiple of 32 bits, whereby 128 bits is considered as the minimum and 256 bits as the maximum. This setup is based on the Substitution Permutation Network (SPN) where all bit alterations in each round and the first round of SPN requires the XOR-ing to be performed on the current state with the round keys. Next, it needs to pass through a substitution layer that consists of blocks of data which are supplanted with other blocks. On top of that, it is required to undergo a permutation layer where bits are permuted and shuffled around. Hence, this operation will be repeated again and again until the last round performs an XOR with a final round key to produce the output. In relation to this, it should be noted that a well-designed SPN with several rounds of substitution and permutation boxes adopted the Shannon's principles of confusion and diffusion. Meanwhile, the main part of the transformation in Rijndael is the first N-1 rounds (N is the number of rounds) that involves 4×4, 4×6, and 4×8 matrix of bytes for Rijndael 128-bit, 192-bit, and 256-bit, respectively. Apart from that, it also consists of four several transformation functions, namely SubBytes, ShiftRows, MixColums, and AddRoundKey.

Algorithm 1. The Key expansion function of Rijndael 128-bits

```
"For i = 0 , …. . Nk – 1 do
    W[i] = k[i] ;
 End for
For i = Nk , … … … . , 4(Nr + 1) − 1 Do
    Temp → W{i – 1};
    if i mod Nk == 0 then
Temp → SubByte(RotWord(temp)) ⊕ Rcon N[i/Nk] ;
  W[i] → W[i − Nk] ⊕ temp
End"
```

The key schedule routine is equal to the number of rounds, whereby it takes independent input data that respectively converts a single key of 16, 24, and

32 bytes as well as outputs expanded keys of 16×11, 16×13, and 16×15 bytes for Rijndael 128-bit, 192-bit, and 256-bit. In this case, it should be noted that the processes of producing sub-keys include three elements of the operations function g (), namely RotWord, SubByte, and Rcon. These are applied on the first sub column on the right side of 4×4, 4×6, and 4×8 matrix expanded bytes of sub-keys. Hence, the key expansion function is represented through the source code in Algorithm 1 in order to produce the expanded sub-keys of Rijndael 128-bits.

In most established studies of cryptographic, the main objective has been observed to revolve around the security analysis of Rijndael. Hence, the designers of Rijndael adapted its security resistance to differential cryptanalysis by looking at the property of the "MixColumns" transformation. More importantly, this method relies on the upper extent separable code, whereby the submitters of Rijndael managed to prove its security in regard to the secret-key model attacks. More specifically, the max probability differential of Rijndael is $\frac{4}{256}$ that is found to be approximately equals to 2^{-6} , while the present active S-box Rijndael 128-bit is performed for four rounds with a probability higher than 2^{-300} which is far lower than the desired threshold of 2^{-128} for a 128-bit block cipher. Additionally, Mouha et al. (2012) developed a technique that determines the maximum number of active S-boxes for up to 14 rounds to prove the security bounds of Rijndael or any other block cipher against differential cryptanalysis that rely on the Mixed Integer Linear Programming (MILP) approach. Furthermore, it is important to note that the security analysis of Rijndael is mostly concentrated on either the secret-key model attacks or the related-key model attacks. The secret-key model attacks are established on the exposure of the state transformation round of Rijndael instead of the vulnerabilities of the Rijndael key expansion function. Accordingly, the reduced number of rounds for Rijndael is believed to be caused by the omission of MixColumns from the last rounds, which includes the Partial Sums Technique Attacks on six rounds (Tunstall, 2012), Boomerang Technique Attacks on six rounds (Biryukov, 2005), and Impossible Differential Technique Attacks on seven rounds of Rijndael 128-bit (Mala et al., 2010). On another note, Li and Jin (2016) introduced the Meet-in-the-middle Technique Attack on ten rounds of Rijndael 256-bit. In addition, the improvement for seven-, eight-, and twelve-round attacks on the 128-bit, 192-bit, and 256-bit key variants respectively was carried out on Rijndael based on the omission of MixColumns from the last round using the Biclique cryptanalysis in the Meet-in-the-middle Technique Attack (Bogdanov et al., 2011; Tao & Wu, 2015)

Recently, several weaknesses that include related-key differential attacks and related-key boomerang attacks in the Rijndael key expansion function managed

to found by the cryptanalysts (Biryukov & Khovratovich, 2009; Biryukov et al., 2010; Biryukov & Nikolić, 2010; Jean, 2013; Cui et al., 2015). This situation is mainly caused by the lack of nonlinearity in the key schedule of the Rijndael that leads to a limited number of active bytes in each sub-key and slow diffusion into the key expansion function. In this case, the main reason that causes the slow diffusion into the key expansion function is resulted by the existence of extremely linear function in the structural constraints of the original algorithm. Meanwhile, the related-key model scenario attacks arise as a result of the leaks that occur in the key expansion function. Hence, the related-key differential attack on all 10 rounds of AES 128-bits the adversary was able to recover the keys and managed to work with all the sub-keys. In regard to this, the adversary works only at the weakness of the key based on a few of the characteristic of the differential into the sub-keys bytes. On the other hand, the related-key boomerang attacks have led to key-recovery and managed to work with the whole keys. Table 1 shows the best cryptanalytic effects performed on Rijndael variants in the related-key model attacks.

Table 1

Best cryptanalysis Results on Reduced Rijndael Variants in The Related-Key Model Attacks.

Version	Round	Data	Time	Memory	Technique	Reference
128	5	2^{39}	2^{39}	2^{32}	Boomerang	(Biryukov, 2005)
	6	2^{71}	2^{71}	2^{32}	Boomerang	(Biryukov, 2005)
	7	2^{97}	2^{97}	2^{32}	Boomerang	(Biryukov et al., 2010)
	5	2^{97}	2^{97}	2^{32}	Differential	(Biryukov et al., 2010)
	7	2^{97}	2^{97}	2^{32}	Differential	(Jean, 2013)
	7	2^{24}	2^{130}	2^{32}	square	(Cui et al., 2015)
	9	2^{67}	2^{143}	2^{64}	Boomerang	(Gorski & Lucks, 2008)
192	10	2^{125}	2^{182}	2^{64}	Rectangle	(Kim et al., 2007)
	12	2^{123}	2^{176}	2^{48}	Boomerang	(Biryukov et al., 2010)
	12	2^{116}	2^{169}	2^{32}	Boomerang	(Biryukov et al., 2010)
	9	2^{99}	2^{120}	2^{64}	Rectangle	(Biham et al., 2005; Kim et al., 2007)
	10	2^{114}	2^{173}	2^{64}	Rectangle	(Biham et al., 2005; Kim et al., 2007)
256	14	2^{131}	2^{131}	2^{64}	Differential	(Biryukov et al., 2010)
	14	$2^{99.5}$	$2^{99.5}$	2^{56}	Boomerang	(Biryukov & Khovratovich, 2009)

RELATED WORK

A considerable amount of studies had been carried out to determine the ability of cryptanalysis in enhancing the performance of Rijndael cipher following the establishment of Rijndael as an advanced encryption standard (AES). In relation to this, there have also been several studies that showed the weakness of the key expansion of Rijndael. This weakness showed in their studies as a leaking bit in the subkeys, slow diffusion, and too linear property.

May et al. (2002) presented three desired properties for a key expansion function that are described as follows: (1) resistance against the collision-one-way function (irreversible function), (2) lower respective information between each of the sub-key bits and main key bits, and (3) effective speed in target software implementation. Therefore, property one is quantified with Shannon's concepts of diffusion and confusion bits. Meanwhile, property two between the sub-keys may be avoided altogether with the fulfillment of property one; hence, giving weight to the author's perspective that the designer of such a cryptosystem is not suggested to use the main key bits straight in the sub-keys. However, it was also found that each of the expanded sub-keys was not in line with Shannon's concepts after performing two statistical tests, namely the Frequency test to achieve the bit confusion property and the Strict Avalanche Criterion (SAC) test for the purpose of determining the bit diffusion property. As a result, a new key schedule with high nonlinearity is proposed. However, the standard for a related-key attack model is not suitable due to its high nonlinearity. Nevertheless, the properties developed by May et al. (2002) was proposed before the recent release of attacks of the related-key, whereby it managed to successfully figure out a method that can theoretically break the full AES-192 and AES-256 as well as the 128-bit variation of AES. Meanwhile, Choy et al. (2011) proposed the resisted related-key differentials and the boomerang attack. However, May et al. (2002) emphasizes that key expansion function is able to meet the security objective as it exhibits a strong efficiency drawback when testing for key agility. This situation is driven by the high amount of S-box transformation that is used in the expansion function of the key which significantly decrease the performance speed, especially involving a Re-key for each block message in the hash mode (Jean et al., 2014).

An extra (but small) number of SubByte operations or any other straightforward operation seems to boost the structure of the Rijndael key expansion function. In relation to this, Nikolić (2011) introduced a newer version of the Rijndael resistance to related-key scenario attacks which requires the running of security analysis for the purpose of proving the new version of Rijndael

resistance against differential related-key attacks. In addition, the same technique was developed by Biryukov and Nikolić (2010) which involves an automatic algorithm search for the best differential probability characteristics of an S-box in the SP-network of ciphers that should be carried out based on the expansion function of a key for the purpose of evaluating the block encryption. Furthermore, no extra characteristics in the differential probability are observed in the XAES 128-bit variant of the 128-bit key because the valid differential for 128-bit is 2^{-128}. Apart from that, Biryukov and Nikolić (2010) similarly argued that the bound of active bytes in the block cipher regarding the differential attack would not have $\frac{128}{6} = 22$ active S-boxes. However, Gérault et al. (2017) improved the upper related-key differential for the whole Rijndael 128-bit cipher and showed that the optimal solution for 6 rounds of Rijndael-128 only contains 12 active S-boxes instead of 13, in which is in agreement with the previous works of Biryukov and Nikolić (2010) and Fouque & Peyrin (2013) .Hence, the problem of locating the exact minimum number of active S-boxes for 6-round Rijndael-128 in the related-key model is still unsolved, which has led to 19 active S-boxes due to the lower bound of the bottom for active bytes on the entire original Rijndael 128-bit for all characteristics. Nevertheless, a higher value than the desired threshold of 2^{-128} for a 128-bit block cipher is reflected due to the level of security of 2^{-114} in terms of the valid differential characteristics. Contrastingly, Huang and Lai (2016) presented another Rijndael key expansion function by only adding an exchange of the matrix subscripts in the rows and columns without the extra operational S-boxes or the rotation. However, the resistance of the key schedule of Huang and Lai (2016) has not been formally proven against the related-key differential and boomerang attacks or any others attacks established on the vulnerabilities of the Rijndael key expansion function for the purpose of managing theoretically attack on original Rijndael block cipher in the related-key model.

The linear transformation function boosts the Rijndael key expansion function by increasing the diffusion property of the key part. On another note, Muda et al. (2010) presented a new 128-bit key version of Rijndael block cipher by adding ShiftRow transformation cyclical shifts without doing any changes to the first row of the expanded sub-key. However, the state matrix is changed by shifting three bytes to the right in the second row. Meanwhile, the third row is changed with a shift of two bytes to the right, while the fourth row is changed with a shift of one byte to the right. As recommended by May et al. (2002), the ShiftRow transformation was tested with two statistical tests for security measurement, namely the confusion and diffusion tests. This new transformation managed to fulfil the security requirement with better results

compared to the original Rijndael key expansion function. On top of that, Muda et al. (2015) proposed a new 128-bit Rijndael key expansion function by adding the ShiftColumn linear transformation into the key expansion structure which include the slight shifting of the XOR-ing bit as well as the replacement of the column with different offsets. Conversely, the new ShiftColumn transformation was also developed by Mahmod et al. (2009). In relation to this, the results from the measurement Performance Tests, the Frequency test (to measure confusion property), and SAC test (to measure diffusion property) showed that this new proposed approach were successful in attaining both properties compared to the original Rijndael key schedule and the approach proposed by Muda et al. (2010) through the investigation performed on the diffusion property in Rijndael block cipher. On another note, Yan and Chen (2016) added a non-linear transformation into the key expansion function for the purpose of increasing the diffusion property for the block cipher as a whole. Moreover, a method was presented to improve the security of the AES key expansion function by adding double S-boxes. More importantly, the experimental results generated by the three random groups of data indicate that the improved algorithm has a more stable diffusivity. However, according to the studies of Muda et al. (2010;2015) and Yan and Chen (2016), the resistance of the key schedules has not been officially proven against related-key differential and related-key boomerang attacks or any other attacks established on the vulnerabilities of the Rijndael key expansion function. Hence, it is still not able to manage theoretical attacks on the cipher in the related-key model. Therefore, only the key schedule was shown to have excellent statistical properties that adhere to the concepts of Shannon's confusion and diffusion, but without conducting a test on the key agility.

DESCRIPTION OF THE PROPOSED APPROACH

This section elaborates on the new design for the key scheduling that was employed in the Rijndael 128-bit block cipher. The proposed approach for the new Rijndael key schedule can be presented in two perspectives. First, the interior design of the core function for the Rotword operation is adjusted. Moreover, it should be noted that the new xRotword has a different rotation in the round, whereby every first word of the 32 bits has two-rotation bytes instead of one byte in order to generate the sub-keys. Currently, the rotate operations (Rotword) are performed according to the bit permutations that produce a diffusion layer in the key expansion function. More importantly, any changes made on every round of key schedule function will increase the diffusion layer. According to Bogdanov et al. (2011), the symmetric key block

cipher will not be vulnerable to the related-key attacks provided that the shift pattern in the key scheduling are executed.

Second, an extra function is added to the constraint structure of the key expansion function which is known as the S ( ) function. The S ( ) function is described as four bytes of input and output. Hence, the S ( ) function works by requesting the nonlinear transformation of SubBytes to all the four input bytes. On top of that, a byte-wise S-box substitution function is used in every second column and XORing with the previous column which acts as the basic structure of the key schedule. On a more important note, a byte-wise S-box substitution consists of the confusion layer and symmetry elimination in Rijndael and provides nonlinearity with the purpose of prohibiting the full determination of differences in the expanded key. Hence, this approach is believed to increase the security of the key expansion function while also mixing the key bits of the initial key for the sub-keys. Nevertheless, it is important to note that diffusion and confusion are considered as the best solutions in enhancing the security of the Rijndael key expansion against attacks. Moreover, the addition of nonlinear transformation into the key expansion function will lead to a more differential characteristic (active S-boxes), thus ensuring that the cipher will most likely be secured against differential attacks in related-key models based on the differential characteristics. Apart from that, the change in the key expansion function has led to the achievement of the following two objectives: (1) the improvement of security algorithm of the key expansion function, and (2) the positive maintenance of the algorithm performance.

The Rijndael key expansion function is word-oriented that represents one word = 32 bits and consists of three operational functions, namely RotWord, SubByte, and Rcon. These operations are called the g ( ) function which is described as a nonlinear transformation that applies a four-byte input and output on each of the first sub-column for the expanded keys. Meanwhile, the remaining three words of the sub-keys are recursively computed. On top of that, the RotWord one-byte rotation occurs in every round of the generation of sub-keys. In regard to this, it should be noted that the newly proposed xRotword consists of two rotations in every round that generate sub-keys. Hence, SubByte and Rcon are deliberated to be similar to the original Rijndael 128-bit. Therefore, the bytes of the second column are applied by the new S ( ) function in the key expansion.

The design of the proposed algorithm approach for the key expansion function is represented via the source code in Algorithm 2, while a pictorial representation of the outlines of the internal structure of the key expansion function is depicted in Figure 1.

Algorithm 2. A new Key schedule of AES 128-bits

"For i = 0 , …. . Nk – 1 do
W[i] = k[i] ;
End for
For i = Nk , … … … . , 4(Nr + 1) − 1 Do
Temp → W[i – 1];
if i mod Nk == 0 then
Temp → SubByte (xRotword(temp)) Rcon N[i/Nk] ;
End if
If Nk = 4 and i mod 4 == 2 then
Temp S () [temp] ; which the S () function request non − linear transformation of SubBytes
End if
W[i] → W[i − Nk] ⊕ temp
End"

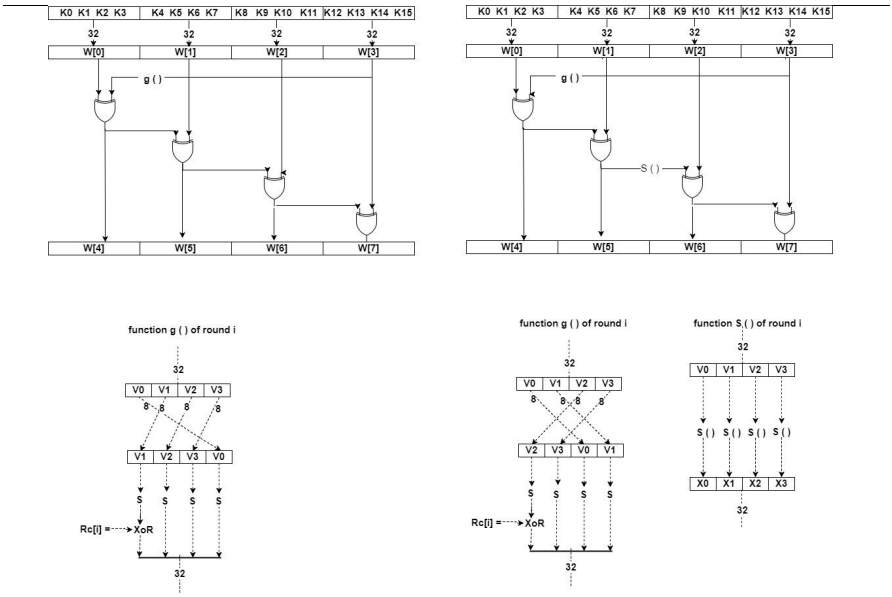

Figure 1. The Internal Structure of the key expansion function.

THE MEASUREMENT OF SECURITY

The main objective of the current research is to enhance and strengthen the security of the Rijndael key expansion function. In this case, the diffusion and confusion bits of the key expansion function for the proposed approach (SAES) is measured against the key expansion function of the original Rjndael (AES) as well as the previous approach (TAES) that were respectively taken from the studies of Daemen and Rijmen (2013) and Muda et al. (2015).

On top of that, two statistical tests which are known as the Frequency test and the Strict Avalanche Criterion (SAC) test were utilized for the purpose pf measuring Shannon's concepts of diffusion and confusion bits as suggested by May et al. (2002). On another note, it is assumed that no differential characteristics for related-key attacks and boomerang attacks will occur on the whole round of 128 bits for the key size of 128 bits in the evaluation of the resistance of the proposed approach in terms of differential cryptanalysis. More importantly, the MILP-Based approach was employed to count the minimum bound of active S-boxes as well as to determine the differential characteristic for the cipher for a given number of rounds in the related-key model.

Frequency Test

The purpose of Frequency test is to test the randomness of a sequence of of zeros and ones. Moreover, the p (probability) value that is used to measure the confusion bits in the Frequency is readily available in the NIST package. The decision rule for this test is that the p-value should be more than or equivalent to 0.01. On the other hand, too many zeros will exist in the sequence of data input and the test fails if the p-value is less than 0.01.

Strict Avalanche Criterion Test

The SAC test is able to produce an excellent absolute difference between the empirical distribution (sample observed) and theoretical distribution (hypothesis). The purpose of this test is to check whether each input bit that affects each output bit on average will change to half the bits in the output of the key. The SAC test is generated using the Statistical Product and Service Solutions (SPSS) software through a one-sample Kolmogorov-Smirnov test (1-sample K-S test). Meanwhile, SPSS computes the expected parameter (mean) for the poisson distribution from the data. The decision rule for this test is that the D-value should be less than 1.628 to ensure that the null hypothesis will be accepted. Otherwise, the null hypothesis will be rejected, thus causing the alternative hypothesis to be accepted. Overall, the null hypothesis indicates that the bit diffusion is satisfied at the 0.01% critical level.

MILP-based Approach

The mixed-integer linear programming (MILP) optimized approach is seen from a high-level point of view as a method that can minimize or maximize the linear objective function of many variables subjected to specific linear constraints on the variables. The model technique used in this research

is the MILP-based approach considering its ability to relieve the whole integer constraint on the standard linear programming variables. Hence, this particular set up as is referred as the 0-1 MILP variables. Mouha et al. (2012) recommended the use of either a 0 or 1 variable for the purpose of describing the differential propagation out of the rounds presented in word-oriented block encryption. Hence, it should be noted that the generated variables are subjected to constraints imposed by the particular structures as well as the operations of the definition cipher. Moreover, this technique provides the analysis of any block cipher based on XORs, three-forked branches, and MDS code operations. In this case, it is best to suppose that the Rijndael block cipher algorithm contains Equations (1), (2), and (3) presented below:

$$1.\ \mathrm{S-box}, \mathrm{S} = f_2^w \rightarrow f_2^w \tag{1}$$

$$2.\ \mathrm{XOR}, \oplus = f_2^w \times f_2^w \rightarrow f_2^w \tag{2}$$

$$3.\ \text{Linear transformation } \mathrm{L} = f_{2^w}^m \rightarrow f_{2^w}^m \tag{3}$$

On a more important note, the aim is to find the differential characteristics from the all zero-difference input state to the same all-zero output state after a variable number of steps. As has been mentioned, the measure of security for the proposed approach relies on the number of active S-boxes, whereby a lower bound on the success probability of a related-key differential attacks may lead to state collisions. Next, the finding differential characteristics were transformed into MILP-Based Approach with the objective functions of counting and minimizing the number of active S-boxes in the AES cipher.

Variables Involved In MILP-Based Approach

The MILP-based approach is a method that automatically evaluates the security of SPN structures and can be applied in single-key or related-key scenarios. On top of that, it can also be used to obtain security bounds for the purpose of minimizing or maximizing the number of active S-boxes. In addition, the original Rijndael 128-bit (AES) and the previous approach (TAES) are used as benchmarks in calculating the minimized bounds of active bytes in the scenario of related-key attacks of the proposed approach (SAES).

Constraints generation for S-box and objective function

Figure 2 depicts every input difference $\Delta_i \in \mathrm{F}_2^{\mathrm{w}}$ of the entire S – box, S issued in the diagram of the operation Rijndael algorithm cipher. The present study presents a new 0-1 variable A_i in order to perform corresponding S-boxes,

be it in active or inactive state. For instance, let $A_i = 1$ or $A_i = 0$ for $\Delta_i \# 0$ or $\Delta_i = 0$. Additionally, the full number of active S-boxes $\Sigma_i A_i$ bytes are selected in minimizing the objective function that is subjected to the constraints of the operation of the Rijndael algorithm cipher, including the round function and key schedule algorithm. However, an S-box will be considered active provided that it has a difference of $A_i = 1$.

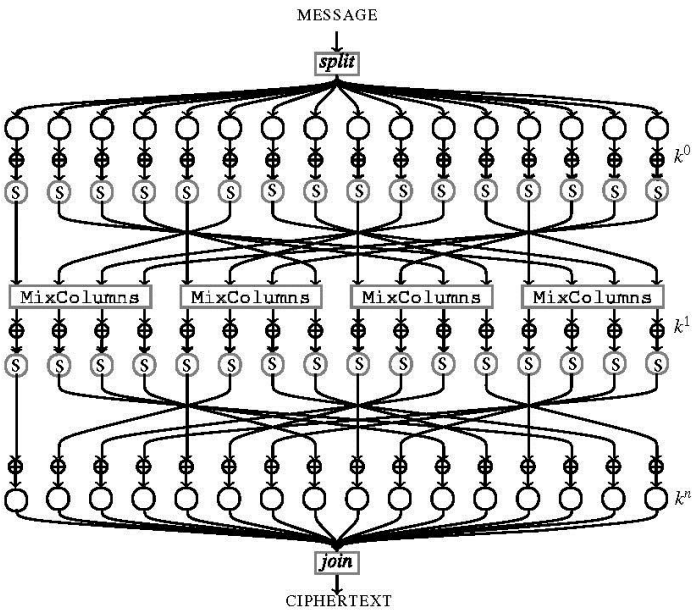

Figure 2: Illustration of the Two Encryption Rounds of the Rijndael 128-bit (Lars & Matthew, 2011).

Constraints generation for XOR

Suppose that $A, B\ are\ \in f_2^w$ and consists of different input of XOR operations within Rijndael (key expansion function algorithm, AddRoundKey). Also, $C \in f_2^w$ if it contains output difference.

$$\begin{cases} A + B + C \geq 2d_{\oplus} \\ d_{\oplus} \geq a \\ d_{\oplus} \geq b \\ d_{\oplus} \geq c \end{cases} \quad (4)$$

Where the $\boldsymbol{d}_{\oplus}$ variable is dummy data that takes the value of 0-1.

The above-mentioned Equation (2) is introduced for each sub-key XOR operation in the Rijndael cipher, especially for each XOR operation that may have a positive or negative value in input difference in contrast to the related-key model. However, it might not have any difference or receive at most one non-zero input difference. However, the XOR operations may be ignored if there is no effect on the output difference. Meanwhile, all the XORs depicted in Figure 2 are taken into consideration in the related-key model.

Constraints generation for linear transformation

0-1 is the dependent variable that indicates the level-word for a linear transformation; hence, the above-mentioned Equation (3) is introduced for input and output difference of a diffusion linear-transformation into the Rijndael cipher. Suppose that $\{i_0, ..., i_{n-1}\}$ and $\{j_0, ..., j_{n-1}\}$ are the permutation layer of $\{0, ..., n-1\}$ Then, let $X_{i\,k}$ and $y_{i\,k}$, $k \in \{0, ..., n-1\}$, whereby the variables have been previously subjected to the following constraints:

$$\begin{cases} \sum_{k=0}^{n-1} (X_{i\,k} + y_{j\,k}) \geq B \\ d_L \geq X_i \\ \dots\dots \\ d_L \geq X_{i\,n-1} \\ d_L \geq y_{j0} \\ \dots. \\ d_L \geq y_{j\,n-1} \end{cases} \tag{5}$$

Where the d_L variable refers to a dummy data request either 0 or 1 in value, or the value of B_L d_L is described as the number of branches in the linear transformation $L = f_{2^w}^m \rightarrow f_{2^w}^m$.

The representation of the variables in the construction of the MILP-based approach that corresponds to a characteristic can be changed by minimizing the bounds of active bytes for the block cipher in the scenario of related-key attacks. Hence, an S-box is determined to be active if and only if it has a difference which acts as a method that determines the new linear diffusion transformation prior to the utilization of the MILP-based approach in TAES. The ShiftColumn that consists of three basic operations (left shift, XOR, Right shift) alongside

with Rotword, SubBytes, and Rcon operations should be developed and applied on the first sub-column for the key schedule algorithm. The new component is applied to the key schedule algorithm of TAES in order to contribute to the diffusion property with the purpose of enhancing the security of the whole cipher. Hence, a component is assumed to have input and output if and only if it has a difference. Next, a new 0-1 variable of linear transformation relying on Equation (3) is introduced by finding the difference using the XOR in Equation (2). Nevertheless, it is not difficult to check the diffusion effect of the linear transformation because the ShiftColumn function is assumed to be applied on the variable $f_2^w \rightarrow f_2^w$ with branch number $B_r < w + 1$.

Overall, the outcome of the four primary transformations of the AES, TAES, and SAES round function is assessed by calculating the round keys. Consequently, a function to keep track of the indices for the active or non-active objective function is presented through the operations of AES that requires at least one S-box to be active considering that the SubByte transformation preserves this property. Hence, it is safe to say that the SubByte transformation did not introduce any linear constraints to the MILP-based approach. In addition, the same holds true for the ShiftRows transformation because the only permutation of the bytes involve the internal state of AES. However, the MixColumns transformation implemented a linear code with maximal distance (MDS) and introduced a linear constraint to the MILP-based approach. In addition, the AddRoundKey transformation XORs for the Rijndael-128-bit sub-key into the state similarly introduced linear inequalities into the MILP-based approach considering that the XOR $y = x_1 \oplus x_2$ of two variables, $x_i, x_2 \in \{0, 1\}$, x_1 is performed with sub-keys, while x_2 is described as the round function state. Similarly, the key expansion function (calculation of round keys) also introduced linear constraints into the MILP-based approach based on the fact that each XOR operation for every word byte of the expanded sub-keys has one X_i variable per key byte $\in \{0, 1\}$, $X_i = 1$ that will be performed only if it has a difference and $X_i = 0$ without any difference. In the event of $(x_1, x_2) = (0, 0)$, it should be noted that y certainly becomes 0, and y becomes 1 if $(x_1, x_2) \in \{(0, 1), (1, 0)\}$. However, the behavior is undetermined where the $(x_1, x_2) = (1, 1)$, as y can either be 0 or 1 based on the actual values of the corresponding differences.

On a more important note, a practical approach to evaluate the security of a block cipher against related-key differential attacks is by determining the lower bound of the number of active S-boxes of all rounds throughout the cipher and key. Hence, this is believed to prove the resistance of the proposed approach against related-key differential attacks. Apart from that, it will also allow the development of differential characteristics on all rounds provided that the characteristics are equipped with the following formal properties:

1) No two differential characteristics will occur with a probability of 2^{-p1} and 2^{-p2} on round one and round two, respectively considering that Round1 + Round2 ≥ rounds − 2 and $2^{p1} + 2^{p2} \leq k$, whereby k refers to 128 bits. Moreover, the purpose of this determination is to stop the boomerang attacks on the full rounds of Rijndael 128-bit. However, it can be assumed that two rounds can be gained for free via several techniques, but the remaining Round1 + Round2 will remain to be part of the boomerang.

2) No differential characteristics will occur on the full rounds with a probability higher than 2^{-128}, where k refers to 128 bits. Hence, this is certainly presented to stop the related-key differential attacks on the full round of Rijndael 128-bit.

EXPERIMENTAL RESULTS

This section will further discuss the analysis of the results in regard to the experiments conducted for the purpose of comparing the proposed approach (SAES) with the original Rijndael (AES) as well as the previous approach (TAES).

The Frequency Test and Strict Avalanche Criterion Test Results

The Frequency and Strict Avalanche Criterion SAC tests are considered as the suitable methods to determine the weakness in each sub-key due to their ability to identify security weakness in the key expansion function.

The Frequency Test

Figure 3 shows the plotted graph for the Frequency test that measures the confusion property by only observing the key expansion function. In this case, all 20 sub-keys that successfully meet the decision rule for the P-value test are generated from the key of the proposed approach as shown in Figure 3. On the other hand, the sub-keys in the previous approach (TAES) failed to meet this rule because the TAES presented a linear diffusion transformation (ShiftColumn) which was applied on the first sub-column for the key schedule algorithm. However, the confusion test showed that not all the sub-keys managed to adhere to this property. Similarly, the key expansion for the original Rijndael (AES) is revealed to be lacking in this property. Meanwhile, the concept of Shannon's confusion can only be achieved after seven rounds of sub-keys. On top of that, the new transformation presented into the key expansion function known as the S ( ) function requires the a SubBytes operation to be applied on

the second column of each sub-key with the purpose of maintaining the concept of Shannon's confusion. In this case, it is believed that the S ( ) function introduces non-linearity to the key expansion function. Therefore, it is clear that the SubBytes operation acts as the common element in achieving confusion.

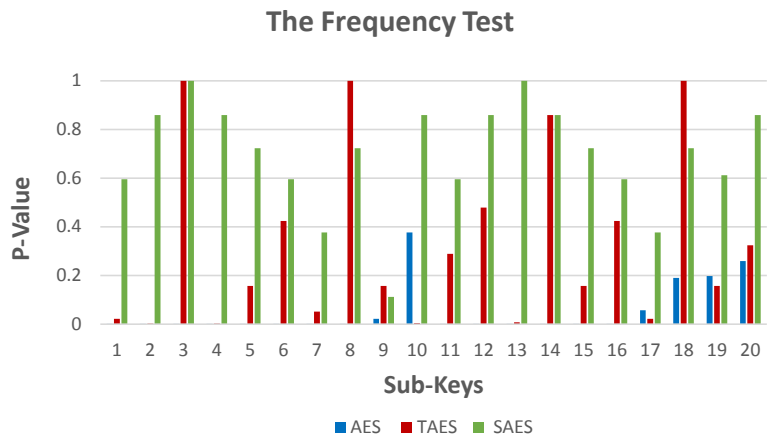

Figure 3. 20 Selected Sub-Keys from the Result of the Frequency Test.

Finally, a total of 180 sub-keys from the key of the proposed approach were tested, and the results showed that the sub-keys managed to obtain the confusion bits. Hence, this is believed that the P-values of the sub-keys that are greater than 0.01 further indicates that bit mixing can be satisfied at the 1% significant level. Therefore, this implies that the sequence is considered random with a confidence level of 99%.

The Strict Avalanche Criterion Test

Figure 4 shows the D-value of the 20 sub-keys generated from the key expansion of the proposed approach (SAES) that manages to successfully meet the decision rule for measuring the diffusion property. However, a slight change in the g ( ) function of the key expansion function can also be observed with the introduction of the xRotWord operation. Nevertheless, it still manages to fulfill the concept of Shannon's diffusion due to the fact that the xRotword has a different rotation in the round of generation sub-keys. Basically, it should be understood that every first 32-bit (sub-column) word has two rotation bytes instead of one byte. As a result of this change, a big difference can be observed in the rest of the sub-columns in the single sub-key based on the concept of each input bit that will affect each output bit.

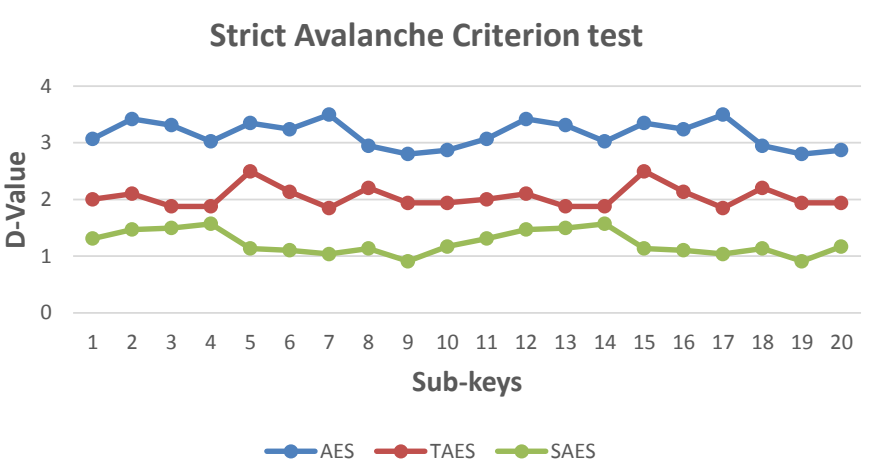

Figure 4. 20 Selected Sub-Keys from the Result of the (SAC) Test.

The original Rijndael (AES) failed the SAC test because the D-value of the sub-key is higher than 1.628. Meanwhile, the key expansion function in AES is lacking the concept of Shannon's diffusion.

On the contrary, the previous approach known as TAES presented a linear diffusion transformation (ShiftColumn) into the first sub-column for the key schedule algorithm. This approach was found to produce excellent statistical properties which agrees with the concept of Shannon's diffusion bits. However, it suffered from a strong efficiency drawback when tested for key agility due to the complex round function transformation in the key expansion function. Hence, the speed performance of the block cipher was significantly decreased, especially when a Re-key was used for each block message in the hash mode.

Resistance Against Related-key Differential Attack

The related-key model involves the expansion of differential attacks, whereas the key expansion function becomes part of the primitive that include the construction of a long differential characteristic. The attacks attempt to build long characteristic differentials on the whole round of the Rijndael 128-bit, whereby the attack specifies a difference in the master key for the Rijndael 128-bit for the purpose of creating related keys. Meanwhile, the best differential

probability of an S-box should be 2^{-6} in order to benefit from related keys. Therefore, the results of the differential should activate fewer nonlinear operations in the state compared to that of the best regular differential. On top of that, the probability of the valid characteristic must be higher than 2^{-128} because the lower bound of active bytes in differential attacks should not exceed $\frac{128}{6} = 22 \text{ active s} - \text{boxes}$.

Table 2 summarizes the number of differential characteristics in the related-key model. The MILP-based approach was constructed in correspond to the characteristic of the AES 128-bit, TAES 128-bit, and SAES 128-bit with lower bounds of active S-boxes bytes. Meanwhile, C++ implementation managed to generate the MILP-based approach that was then solved using the IBM ILOG CPLEX Optimizer 12.7 running on a personal laptop with a CPU Intel(R) Core(TM) i7-3610QM (2.30 GHz) and 8.00 GB RAM (CPLEX, 2011).

As can be observed in Table 2, the lower bounds of the active s-boxes of the bytes in the related-key model of AES 128-bit consist of 20 active S-boxes. Hence, the best related-key differential characteristic in terms of the valid differential characteristics is shown as10-round $(2^{-6})^{20} = 2^{-120}$, which is considered higher than the needed threshold of 2^{-128} for a 128-bit. On the other hand, the result of the differential refers to the activation of fewer nonlinear operations in the key part of the AES 128-bit compared to the state round function. This situation is believed to be the result of the key expansion function part of AES 128-bit that only has a $g()$ function, which is a non-linear function with a four-byte input and output applied on the first of each sub-column for the expanded keys. Meanwhile, the remaining three words of the sub-keys are recursively computed with the XOR operation, thus resulting in an extremely linear key part. According to previous studies (e.g. Gérault et al., 2017; Khoo at al., 2017), the lower bound of active s-boxes of the bytes for the original AES 128-bit in all the characteristics is 19 active s-boxes; hence, the level of security in terms of valid differential characteristics is $(2^{-6})^{19} = 2^{-114}$.

Table 2

Results of related-key differential analysis

# Rounds	AES 128-bit		TAES 128-bit		SAES 128-bit	
	# active S-boxes	# time in the seconds	# active S-boxes	# time in the seconds	# active S-boxes	# time (in the seconds
1	**0**	1	**0**	1	**0**	1

(continued)

# Rounds	AES 128-bit		TAES 128-bit		SAES 128-bit	
	# active S-boxes	# time in the seconds	# active S-boxes	# time in the seconds	# active S-boxes	# time (in the seconds
2	**1**	1	**1**	1	**2**	1
3	**3**	1	**3**	3	**4**	1
4	**9**	1	**9**	4	**10**	1
5	**11**	5	**11**	5	**14**	6
6	**12**	16	**12**	18	**17**	18
7	**14**	20	**14**	25	**20**	21
8	**17**	24	**17**	28	**23**	25
9	**19**	27	**19**	30	**25**	30
10	**20**	35	**20**	45	**28**	40

In this case, it is important to note that TAES 128–bit shares similar security vulnerabilities as the AES 128-bit key expansion function that are responsible to manage the theoretical attack on the cipher in the related-key model. In relation to this, the analysis for the component of the key expansion function of TAES 128-bit does not produce any extra differential characteristic. On a more important note, an assessment on the new linear diffusion transformation was performed on the ShiftColumn that consists of three basic operations (left shift, XOR, Right shift), which was introduced into the key schedule algorithm. Apart from that, the new component was applied on the first subcolumn for each of the expanded sub-key alongside with the g () function, while the rest of the subcolumns were recursively computed using only the XOR operation. Unfortunately, this only contributes to the shifting of the bits without introducing any extra differential concerning the active s-boxes bytes. Hence, the best related-key differential characteristic in terms of the valid differential characteristics for TAES 128-bit for the 10-round is $(2^{-6})^{20} = (2^{-120})$. Hence, it is considered higher than the required threshold of the level of security for the differential probability 2^{-128} for the 128-bit.

Finally, it can be concluded that no differential characteristics were found in the proposed approach (SAES 128-bit), particularly in the full rounds with a probability higher than 2^{-128}. This situation is believed to be caused by the minimum number of active s-boxes in the related-key model on the full rounds that contains 28 active s-boxes or in other words, $(2^{-6})^{28} = 2^{-168}$ differential probability. Hence, the attacks will not work because the value is much lower compared to the required threshold of 2^{-128} for a 128-bit. The valid extra differential characteristic presented in the SAES 128-bit is due to the extra nonlinear transformation of the key expansion function of SAES. In this case, the S ( ) function is applied on the bytes of the second column in

the key expansion for the purpose of preventing the related-key differential attacks from occurring on the full round of AES 128-bit. Hence, this approach was found to contribute to a higher security for the key expansion function, thus it is considered to be more secured against related-key differential attacks compared to the recently established AES 128-bit.

Resistance Against Related-key Boomerangs Attack

It is important to note that differential characteristic is utilized on a smaller number of rounds in the case of Boomerangs attacks. Hence, the attacker can use either single-key or related-key differential characteristics. Moreover, the adversary builds two short differential characteristics instead of one long characteristic on the block cipher. In AES, the best differential probability of an S-box is 2^{-6}; hence, no two differential characteristics should occur with a probability higher than 2^{-128} for all combinations of two characteristics that have a total of 10 rounds. The purpose of presenting this determination is to stop the boomerang attacks on the full rounds of AES 128-bit.

Meanwhile, this will allow the development of the Boomerang attacks on the whole 10 rounds, particularly in the context of AES 128-bit. Moreover, the reader is reminded that the lower bound of active S-boxes of the bytes on the AES 128-bit for all the characteristics are 20 active s-boxes. Hence, it is possible to build two independent differential characteristics for all combinations of two characteristics that contains 10 rounds in total. On a more important note, this differential characteristic must not exist with a probability higher than 2^{-128} or 22 active S-boxes. According to this concept, the AES 128-bit has 0 active S-boxes for the top characteristics for Round 1, while there is a total of 20 active S-boxes for the bottom characteristics of Round 9. Hence, the adversary was found to have a 2^{-120} probability that is considered higher than the valid probability 2^{-128} for the AES 128-bit. Therefore, the attacker has a remainder of 22-20 = 2 active S-boxes that is deemed adequate for an attack to cover 10 rounds. Therefore, it can be said that the AES 128-bit could be attacked with two characteristics in total to cover all 10 rounds. On the other hand, the total probability for the boomerang attacks is higher than 2^{-128} for the rest of the rounds of AES 128-bit that will enable the attack for key-recovery and all the keys, which is similar to the TAES-128 bit. This situation is believed to be caused by absence of extra differential characteristics based on the analysis of this study conducted on the component of the key expansion function of TAES. Nevertheless, it should be noted that TAES shares similar security margin to boomerangs attacks as that of the AES-128 bit.

On another note, the number of active S-boxes in the differential characteristic is $\frac{128}{6}$equal to 22 for the security analysis of the SAES 128-bit regarding

Boomerang attacks. The characteristic of Round 1 is 0, while the characteristic of Round 9 is 25. Meanwhile, the adversary showed the probability of $(2^{-6})^{25} = 2^{-150}$ which is much lower than the valid probability 2^{-128} for the AES 128-bit; hence, it will prevent the boomerang attacks. Likewise, the number of active S-boxes would be 2+23 = 25 and 17+10 =27 for the two characteristics build on 2, 8 and 6, 4 rounds, respectively. However, this is considered much lower compared to the valid differential probability. Meanwhile, the lower bound of the active S-boxes of the bytes will be 14 +14 = 28 when two characteristics is built on 5 rounds, which is greater than 22. In addition, the characteristics of Rounds 3 and 7 consist of 24 active S-boxes, thus exceeding the 22 active S-boxes. Hence, all the characteristics have proven that the proposed approach (SAES) is secured against Boomerang attacks based on all the combinations of the two characteristics that cover 10 rounds in total with a probability lower than 2^{-128}. Therefore, this managed to proof the security of the proposed approach against the related-key Boomerang attacks.

Resistance Against Other Attacks in the Form of a Secret-key Model

In this case, it should be reminded that the secret-key attacks are established on the exposure of the state transformation round of Rijndael instead of the vulnerabilities of the Rijndael key expansion function. The secret-key model scenario attacks occurred due to the omission of MixColumns from the last round. According to Dunkelman and Keller (2010) and AlMarashda et al. (2011), the omission of MixColumns affects the security of (reduced-round) AES. On top of that, the state round function of AES has been strongly and securely designed in regard to differential cryptanalysis in the secret-key model attack scenario, with the best differential characteristics of probability 2^{-330} on 10 rounds of AES. Meanwhile, the state round function remains unchanged and only the key schedule was adjusted.

CONCLUSION

The current research successfully presented an enhancement to the security of the Rijndael key schedule algorithm. In this case, it is important to note that there are three different variants to the key schedule in the Rijndael cipher which are the 128-bit, 192-bit, and 256-bit for10, 12, and 14 rounds, respectively. However, the present study only focused on the 128-bit key size due to the recent theoretical attacks that occurred as a result of the weakness found in this key schedule. On top of that, the 128-bit key schedule of the Rijndael cipher are not equipped with sufficient differential characteristics (active S-boxes), thus able to prevent the related-key model attacks caused by the extremely linear nature of the constraint in the original algorithm. On another

note, the proposed key expansion function (SAES) showed better statistical properties in terms of the confusion and diffusion bits compared to the original key expansion function (AES) and previous key expansion function (TAES). Moreover, the proposed approach managed to illustrate ideal security against related-key attacks in the form of differential cryptanalysis and boomerang attacks. This situation is believed to be caused by the number of active S-boxes of the bytes which is 28 as well as the security level recorded as 2^{-168}, thus reflecting a much lower value than the valid requirement in managing the attacks theoretically. Finally, it can be concluded that the original approach and previous approach do not have ideal security against these attacks.

ACKNOWLEDGMENT

This work was supported by Putra Research Grant Scheme, project Code GP/2017/9588400. The authors gratefully acknowledge use of service and facilities of the Faculty of Computer Science and Information Technology at Universiti Putra Malaysia.

REFERENCES

AlMarashda, K., AlSalami, Y., Salah, K., & Martin, T. (2011). On the security of inclusion or omission of MixColumns in AES cipher. In *6th International Conference for Internet Technology and Secured Transactions* (pp. 34–39). IEEE.

Biaoshuai, T., & Wu, H. (2015). Improving the Biclique cryptanalysis of AES. In *Australasian Conference on Information Security and Privacy* (pp. 39–56). Springer, Cham. https://doi.org/10.1007/978-3-319-19962-7_3

Biham, E., Dunkelman, O., & Keller, N. (2005). Related-Key Boomerang and Rectangle Attacks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 507–525). Springer, Berlin, Heidelberg. https://doi.org/10.1007/11426639_30.

Biryukov, A. (2005). The Boomerang Attack on 5 and 6-Round Reduced AES Boomerang Attack. In *International Conference on Advanced Encryption Standard* (pp. 11–15). https://doi.org/10.1007/11506447.

Biryukov, A., & Khovratovich, D. (2009). Related-key cryptanalysis of the full AES-192 and AES-256. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 1–18).

Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-10366-7_1.

Biryukov, A., Khovratovich, D., & Nikolić, I. (2010). Distinguisher and related-key attack on the full AES-256. In *Advances in Cryptology-CRYPTO 2009* (pp. 231–249). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-03356-8_14.

Biryukov, A., & Nikolić, I. (2010). Automatic search for related-key differential characteristics in byte-oriented block ciphers: Application to AES, Camellia, Khazad and others. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 322–344). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_17.

Bogdanov, A., Khovratovich, D., & Rechberger, C. (2011). Biclique cryptanalysis of the full AES. In *Advances in cryptology–ASIACRYPT* (pp. 344–371). https://doi.org/10.1007/978-3-642-25385-0_19

Choy, J., Zhang, A., Khoo, K., Henricksen, M., & Poschmann, A. (2011). AES variants secure against related-key differential and boomerang attacks. In *International Workshop on Information Security Theory and Practices* (pp. 191–207). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21040-2_13.

Cui, J., Zhong, H., Shi, R., & Wang, J. (2015). Related-key cryptanalysis on 7-round AES-128/192. *International Journal of Electronic Security and Digital Forensics*, *7*(2), 166–178. https://doi.org/10.1504/IJESDF.2015.069609.

Daemen, J., & Rijmen, V. (2013). *The Design of Rijndael: AES - The Advanced Encryption Standard*. *Springer Science & Business Media*. https://doi.org/10.1007/978-3-662-04722-4.

Dunkelman, O., & Keller, N. (2010). The effects of the omission of last round's MixColumns on AES. *Information Processing Letters*, *110*(8–9), 304–308. https://doi.org/10.1016/j.ipl.2010.02.007

Fouque, P., Jean, J., & Peyrin, T. (2013). Structural Evaluation ofAES and Chosen-Key Distinguisher of 9-round AES-128. In *Advances in Cryptology–CRYPTO* (pp. 183–203). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40041-4_11

Gérault, D., Lafourcade, P., Minier, M., & Solnon, C. (2017). Revisiting AES Related-Key Differential Attacks with Constraint Programming. *IACR Cryptology EPrint Archive*, 139. Retrieved from ia.cr/2017/139

Gorski, M., & Lucks, S. (2008). New Related-Key Boomerang Attacks on AES. In *International Conference on Cryptology in India* (pp. 266–278). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-89754-5_21

Huang, J., & Lai, X. (2016). Transposition of AES Key Schedule. In *International Conference on Information Security and Cryptology.* (p. 260). Springer, Cham. https://doi.org/10.1007/978-3-319-54705-3_6

Jean, J. (2013). *Cryptanalysis of symmetric-key primitives based on the AES block cipher. Cryptography and Security [cs.CR]*. (Unpublished doctoral dissertation). Ecole Normale Supérieure de Paris-ENS Paris. Retrieved from https://tel.archives-ouvertes.fr/tel-00911049

Jean, J., Nikolic, I., & Peyrin, T. (2014). Tweaks and keys for block ciphers: The TWEAKEY framework. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 274–288). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45608-8_15.

Khoo, K., Lee, E., Peyrin, T., & Sim, S. M. (2017). Human-readable proof of the related-key security of AES-128. *IACR Transactions on Symmetric Cryptology*, *2*, 59–83. https://doi.org/10.13154/tosc.v2017.i2.59-83.

Kim, J., Hong, S., & Preneel, B. (2007). Related-key rectangle attacks on reduced AES-192 and AES-256. In *International Workshop on Fast Software Encryption* (pp. 225–241). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74619-5_155.

Lars, K. R., & Matthew, R. (2011). *The block chipher companion*. Springer. Retrieved from www.springer.com/gp/book/9783642173417.

Li, R., & Jin, C. (2016). Meet-in-the-middle attacks on 10-round AES-256. *Designs, Codes, and Cryptography*, *80*(3), 459–471. https://doi.org/10.1007/s10623-015-0113-3.

Lu, J. (2015). A methodology for differential-linear cryptanalysis and its applications. *Designs, Codes, and Cryptography*, *77*(1), 11–48. https://doi.org/10.1007/s10623-014-9985-x

Mahmod, R., Ali, S. A., Azim, A., & Ghani, A. (2009). A shift column with different offset for better rijndael security. *International Journal of Cryptology Research*, *1*(2), 245–255.

Mala, H., Dakhilalian, M., Rijmen, V., & Modarres-Hashemi, M. (2010). Improved impossible differential cryptanalysis of 7-round AES-128. In *Lecture Notes in Computer Science* (pp. 282–291). https://doi.org/10.1007/978-3-642-17401-8_20.

May, L., Henricksen, M., Millan, W., Carter, G., & Dawson, E. (2002). Strengthening the Key Schedule of the AES. In *Proceedings of the 7th Australian Conference on Information Security and Privacy* (pp. 226–240). https://doi.org/10.1007/3-540-45450-0_19

Mouha, N., Wang, Q., Gu, D., & Preneel, B. (2012). Differential and linear cryptanalysis using mixed-integer linear programming. In *International Conference on Information Security and Cryptology*, 57–76. https://doi.org/10.1007/978-3-642-34704-7_5

Muda, Z., Mahmod, R., & Sulong, M. R. (2010). Key transformation approch for Rijndael secuirty. *Information Technology Journal*, *9*(2), 290–297.

Muda, Z., Sulaiman, S., Yasin, S. M., & Mahmod, R. (2015). Tshiftcolumn: A new transformation in 128-bit Rijndael key expansion to improve security requirements. *Journal of Theoretical and Applied Information Technology*, *73*(1), 130–136.

Nikolić, I. (2011). Tweaking AES. *Lecture Notes in Computer Science*, *6544*, 198–210. https://doi.org/10.1007/978-3-642-19574-7_14.

Tunstall, M. (2012). Improved "Partial Sums"-based square attack on AES. In *International Conference on Security and Cryptography* (pp. 25–34). https://doi.org/10.5220/0003990300250034.

Yan, J., & Chen, F. (2016). An improved AES key expansion algorithm. In *International Conference on Electrical, Mechanical and Industrial Engineering* (pp. 113–116).