How to cite this paper:

Hassan Mansour Hussien, Zaiton Muda, & Sharifah Md Yasin. (2017). Enhance the robustness of secure Rijndael key expansion function based on increment confusion and diffusion bits in Zulikha, J. & N. H. Zakaria (Eds.), Proceedings of the 6th International Conference on Computing & Informatics (pp 722-728). Sintok: School of Computing.

ENHANCE THE ROBUSTNESS OF SECURE RIJNDAEL KEY EXPANSION FUNCTION BASED ON INCREMENT CONFUSION AND DIFFUSION BITS

Hassan Mansour Hussien[1], Zaiton Muda[2], and Sharifah Md Yasin[3]

[1]*Universiti Putra Malaysia, Malaysia, hassanalobady@gmail.com*
[2]*Universiti Putra Malaysia, Malaysia, zaitonm@upm.edu.my*
[3]*Universiti Putra Malaysia, Malaysia, ifah@upm.edu.my*

ABSTRACT. Symmetric block ciphers are the most widely utilized cryptographic primitives. Since block ciphers provide privacy; block ciphers are hence used as core components for the construction of hash functions such as one-way compression functions and pseudorandom number generators, all as part of several cryptographic protocols, etc. These days the most common block cipher is the AES Rijndael, which is used as a standard of symmetric encryption in many countries. Several studies have shown a theoretical attack exploiting the AES key expansion algorithm which allows significant reduction in the complexity time to break the cipher, compared to the brute force attack. The arrack in the related-key model and the long biclique with a meet in the middle attacks in the secret-key model are applied on the AES because of the weak key expansion function. Authors of AES accepted that the key expansion function of Rijndael is comparatively weak. Confusion and diffusion are two properties of the operation a secure cipher. Therefore, although the two properties within the substitution-permutation construct are only applied to state the transformation round function of the Rijndael algorithm, but there is no other strong security for the key expansion function. This article, hence presents a method to improve the Key Schedule of the Rijndael cipher in order to maintain the requirement of bits confusion and diffusion properties besides making the cipher more resistance to differential cryptanalysis.

Keywords: AES, key expansion function, differential cryptanalysis, related-key attack, mixed integer linear programming (MILP), frequency test, SAC test. Active S-boxes

INTRODUCTION

The Advanced Encryption Standard (AES) Daemen, J., Rijmen, V, is a block cipher adopted by NIST. Fifteen years after the adoption, AES “Rijndael" has been widely utilized for commercial and governmental purposes which are implemented in both software and hardware. Moreover, it is an elegant design with a very efficient performance cipher. AES is a block cipher that has a 128-bits state and comes in three various key sizes; 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. It is based on the SP-network, whereby all the bits are altered in each round, where the first round will use XOR in its current state with the round keys. It then passes through a substitution layer, where blocks of data are supplanted with other blocks. After that, it is passes through a permutation layer

where bits are permuted and shuffled around. This operation take place repeatedly until the last round will XOR with a final round key. The output of this process is the end product. However, the well-designed SP network has several rounds of substitution- and permutation – the boxes indicated are part of the Investigation Shannon principles which are confusion and diffusion. In AES "Rijndael," the first N-1 rounds (N is the numbers of round), which are 4x4 matrix of bytes, consist of four several transformation functions which are SubBytes, ShiftRows, MixColumns and AddRoundKey.

The selection of the transformation round function statement of implementing a round for AES as a mixture of simple table lookups and XORs, leads to significant performance benefits. Intel has also established a new AES instruction set, which is labeled by Gueron, S. (2012), as AES-IN. It has also been introduced in the new processors. The new instruction significantly increases the efficiency of the round function of AES. Yet, no special instructions will be available to perform the key schedule routine. However, the key expansion for Rijndael has a special instruction computation lightweight and is efficient in terms of memory and performance. The operation of the product subkeys consist three transformation functions which are RotWord, SubByte, and Rcon.

The advanced encryption standard (AES) has been the target of many cryptographic papers. The designers of Rijndael have adapted by securing it through the use of the MixColumns transformation properties, which relies on the maximum extent separable code. The submitters of Rijndael proved that the differential characteristics exist only for a reduced number of rounds when facing secret-key model attacks.However, further analysis on the security of AES was at most focused on either secret-key attacks or related- (or multiples) key attacks. In the fixed key model attacks were based on the vulnerabilities of the state round function of Rijndael and did not exploit any properties of the Rijndael key schedule Nikolić, I. (2010), (Andrey Bogdanov, at , al ,2015), which was due to the omission of the MixColumns from the last rounds. Accordingly, some cryptanalysis were obtained from the security weakness of AES; such as related key attacks, related subkeys attack, related-key rectangle, and boomerang attack cryptanalysis (Biry-ukov, A., Khovratovich, D. (2010). This is mainly due to the lack of nonlinearity in the key schedule of the AES , which is too linearity has no enough active bytes into each of Subkeys, and biclique attack with a meet in the middle attacks (Andrey Bogdanov, at , al ,2015) due to slow diffusion into the key expansion function . Nevertheless, all these attacks are going to lessen the security of algorithm all in all that are conducted on AES in light of the weakness key expansion function. The reality of these attacks are only theoretical and need a computational power beyond our reach.

The research paper is organized as follows: Similar works are discussed in Section 2, while the proposed approach is described in Section 3. In Section 4, the methodology presented, followed by the conclusion in section 5.

RELATED WORK

After the publicizing of Rijndael as an advanced encryption standard (AES), several studies were carried out on the performance of the Rijndael cipher for the investigation of cryptanalysis and its improvement. There were some studies that showed the key expansion of Rijndael, hence revealing its weakness. The weakness presented in the mentioned studies showed that it had leaking bits in the subkeys, had a slow diffusion, and was too linear.

May et al. (2002) presented three desired properties for a key expansion function; with the first, having a collision-resistant one-way function (irreversible function). The second, having a minimal mutual information between all subkey bits and master key bits and the third one being an efficient implementation. Therefore, the author measured property one with Shannon's concepts of bit confusion and bit diffusion. Property two between the subkeys can be avoided by the achievement of property one; hence the author expected that such a designer would not use master key bits straight in subkeys. However, it was also found that

each of the expanded subkey was not in content with Shannon's concepts, after running two statistical tests where a frequency test is performed to judge the bit confusion property. The other was the Strict Avalanche Criterion (SAC) test to judge the bit diffusion property. As a result, a new design of the key schedule which has high non-linearity into the key schedule was proposed. However, the Standard of related-key attacks model does not work, due to high non-linearity. Choy, Jiali, et al. (2011) proved this proposal resistance to related-key differentials and a boomerang attack.

An additional (but small) numbers of S-Boxes or any other simple operation adds into the structure of Rijndael key expansion function, Nikolić, I. (2010) introduced a newer version of the Rijndael resistance to related-key differential attacks. The security analysis of proving the new version for Rijndael against related-key differential attacks also used the same technique provided by Alex Biryukov, et al. (2010), where automatic algorithm search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers, depends on the key schedule of the analyzed cipher. Huang, et al. (2012), contrarily, presented another new Rijndael key expansion function, without adding either the extra operational S-boxes or rotation, but by only add exchanging the matrix subscripts of rows and columns.

The linear transformation function adds into the Rijndael key expansion function to increase the diffusion property of the key part. Muda, et al. (2010) presented a new 128-bits key version of Rijndael by adding ShiftRow transformation cyclical shifts, where there is no change in the first row , but the state matrix is changed with three bytes to the right in the second row . The third row is changed by two bytes to the right while the fourth row is changed by one byte to the right. The ShiftRow transformation was tested with two statistical tests for security measurement, as suggested by May, et al. (2002) ; confusion and diffusion tests. This new transformation had passed the security requirement with better results compared to the original Rijndael key expansion function. Sulaiman, S, et al. (2015) proposed a new 128-bits Rijndael key expansion function by adding the linear transformation ShiftColumn into the structure of key expansion, which involved slight shifting of the XORing bit, and replaced the column with different offsets. Conversely, the new transformation was also suggested by Mahmod, et al. (2009). The results from the Performance Measurement test, Frequency test (to measure confusion property) and SAC test (to measure diffusion property) showed that this new proposed approach succeeded in attaining both properties compared to the original Rijndael key schedule. Muda, Z., (2010,) investigated the property diffusion in the Key. He added non-Linear transformation into the key expansion function to increase the property diffusion for whole the block cipher. Yan, J., & Chen, F. (2016) presented a method to improve the security of the AES key expansion function by adding a double –S-boxes. The experimental results generated by the three random groups of data, indicated that the improved algorithm has a more stable diffusivity.

METHOD TO IMPROVE RIJNDAEL KEY EXPANSION FUNCTION

This section presents the new proposal of the AES, which is only a tweak cipher in the key expansion function. However, the security of the new version is the main concern of this paper. Hence, we would like to achieve an efficient primitive as well.

AES was designed for efficient implementation of software and hardware. Hence, the AES round function is well-designed with excellent security properties which consists of two operation lookups and xors, and it allows fast implementation through a low number of this operation. The Rijndael designer presented a new method which resulted in fast software implementation. The concept of the idea was to merge all round functions (except the rather trivial key addition) into one table lookups whereby the so-called T-box can compute 16 table lookups in one round. Hence, Intel presented a new Instructions processor; AES-NI "Gueron, Shay". The purpose of the instruction set was to improve the speed of applications performing encryption and decryption in AES. Therefore, to perform the essential level of security for a

new proposal, focus will be on improving the current key expansion function of Rijndael while keeping the state transformation round function unchanged.

First and foremost, the main objectives for this study are as follows; firstly, a new key expansion function for Rijndael resistance is created against differential characteristic attacks, so that no related-key differential characteristics exists on the full-round of 128 bits for key size 128 bits. Secondly, the tweaked Rijndael cipher should be efficiently (speed) comparable to the speed of the original Rijndael. Basically, in order to test the speed of key agility in two different ways, one needs to measure the efficiency of a block cipher in the encryption method where the master key is fixed and the subkeys are computed once and used in all of the iterations. Second, where master key is changed on every iteration, and sequentially, the subkeys have to be recomputed in the hash method, while the block cipher is used as an underlying primitive for other cryptographic constructions, e.g. hash functions.

Description of New Proposed Approach

This section describes the new approach for the Rijndael key expansion of 128-bits used in this study. However, there is a slight change in the basic function to the Rotword for Key Rijndael operation, whereby an S () function, which that S () is 4-byte input and output is added. Hence, the S () function applies non-linear transformation of S-Box to all the four input bytes.

The Rijndael key expansion function is word-oriented, where one word = 32 bits and consists three operational functions which are RotWord, SubByte, and Rcon. These operations are called g () function. The RotWord one byte rotation occurs in every round of the generation subkeys .The newly proposed Rotword has a different rotation in every round generation subkeys. Hence, SubByte and Rcon are deliberated to be the same as in AES original. Therefore, the S ( ) function applies on the bytes of the second column in the key expansion. The diagram below gives a formal definition of the new key expansion function for the key size of 128-bits, and is defined as follows:

When k[4][4] is the master key, then the subkeys array w[4][44] is defined as:

$$w[x][y] = \begin{cases} K[x][y] & \text{if } y < 4 \\ SubByte(W[x-1 \bmod 4][y-1]) X \oplus RotWord(w[x][y-4]) \oplus Rcon[x][y/4]; & \text{if } y \bmod 4 == 0 \\ SubByte(W[x-1 \bmod 4][y-1) \oplus W[x][y-4]; & \text{if } y \bmod 4 == 2 \\ W[i-1 \bmod 4][y-1] \oplus W[x][y-4]; & \text{otherwise} \end{cases} \quad (1)$$

To fully understand the idea of the new modification, (as shown in Figure 1), gave a pictorial representation of the S () function when applied to the key expansion function change. Besides that, a new Rotword which has a different rotation in every round of generation subkeys is defined. Basically, rounds 3, 4, 5,6,7,8 of every first word 32-bits have two rotation bytes instead of one byte, and the rest have one rotation bytes.

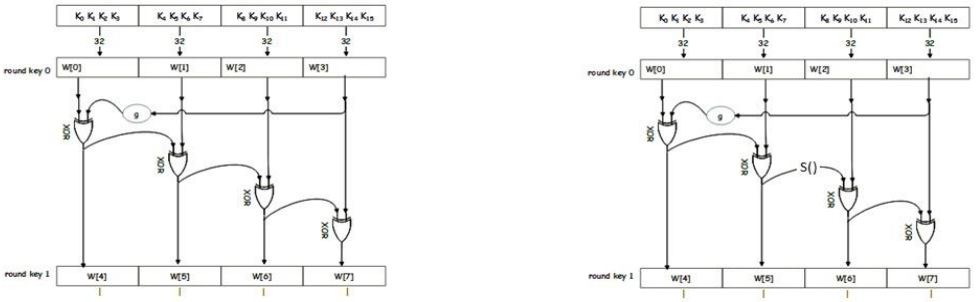

Figure 1. One Subkey for AES 128-Bits (on the Left), New Subkey AES 128-Bits (on the Right), Each W[I] is Subkey Column – 4bytes, G () is the Function Consists of Three Operation (Rotword, Subbyte, Rcon) And The S () is the New Function Adds on the Key AES 128-Bits.

METHODOLOGY

This point discusses the research methodology and the research design of the proposed model and conferes on the evalution of this research. This research aims at enhancing the robustness of securing the Rijndael 128-bits cipher by changing its Key Expansion Function, while maintaining the required bit confusion and diffusion properties , hence leading to the evalution of the resistance of our proposal, in regards to differential cryptanalysis. The implementation used to carry out our methods is in C++.

Security Measurement

The main objective of this study to increase the security of Rijndael key expansion by proving a new proposal to achieve this goal. We would like to use two statistical tests as suggested by May et al. (2002) for measuring Shannon's concepts of bit confusion and bit diffusion. The two statistical tests, with the first being a frequency test, is performed to judge the bit confusion property. The second one, is the Strict Avalanche Criterion (SAC) test meant for measuring the bit diffusion property. The two different sample datasets of random and non-random numbers used in this study are generated from the key expansion function.

The Frequency test is of the fraction amount of zeros and ones which are approximately same. The p (probability) value used in Frequency test (from NIST package) should be greater than or equal to 0.01. If the p-value is less than 0.01, there will be too many zeros in the sequence of the data input.

The SAC test is a product of the largest absolute difference between the empirical distribution (sample observed) and theoretical distribution (hypothesis).This test checks that the a one-bit change produced in the input key, on average, changes to half the bits in the output of key. The SAC test is generated by using the statistical product and service solutions (SPSS) software through a one-sample Kolmogorov-Smirnov test (1-sample K-S test). SPSS will compute the expected parameter (mean) for the Poisson distribution from the data. The decision rule for this research is that D value should be less than 1.628, in order to accept the null hypothesis or else otherwise, the null hypothesis will be rejected and the alternative hypothesis will be accepted. The null hypothesis indicates that the bit diffusion is satisfied at the 0.01% critical level.

Computing Active S-Boxes

In order to evaluate the resistance of our proposed approach regarding differential cryptanalysis, on the notion that no related-key differential characteristics exist on the full-round of 128 bits for key size 128 bits, we relied on counts of numbers of active S-boxes in a given number of rounds for the tweak cipher. Several methods were presented to count the number of Active-bytes (s-boxes.) in which some were of costly computations similar Biryukov, A., & Nikolić, I. (2010) where three variants of Matsui's Algorithm was presented to find a bound on number active s-boxes in the byte-oriented block cipher. The others were extremely complex, thus making it impossible to use without a long explanation from his or her side beforehand, demonstrated before by as Fouque, P. A., et al. (2013), Sajadieh, Mahdi, et al. (2016). There have been much simpler and efficient tools introduced recently, particularly using Mixed Integer Linear Programing (MILP) Mouha, Nicky et al. (2012).

However, in the case to count the number of active-bytes(S-boxes) will construct MILP that corresponds to the characteristic with a minimal number of active S-boxes and then solve the MILP to find the characteristic. The max differential propagation probability of an S-box is 4/256 = 2^{-6}. Thus, any related-key differential characteristic for a state of AES 128-bits with key size of 128-bits (to be able to use it in an attack) may have at most 21 active S-box. This is because 128/6 = 21 active s-boxes. Therefore, to construct a MILP that will focus on state and key expansion functions of AES to find a minimal number of active S-boxes, a program will be written in C to generate the equations for this optimization problem in the

CPLEX LP format. Moreover, this will also solve the problem using the IBM ILOG CPLEX Optimizer (which is free for academic use).

Efficiency Analysis

The other objectives of this study to evaluate the efficiency (speed) of the new approach. In the earlier sections, two ways to test the speed of key agility were given. In general, there are two different existing approaches for the implement of the key schedules, which are the Precomputation and the on-the-fly.

Firstly, in an environment where the master key is fixed and the encrypted message is longer (encryption method), then we assume that the "encryption mode" is AES-CBC. This is the encryption method mentioned in the earlier section, which is the same as the precomputation that one of the approaches of implementations of Key schedule Rijndael. This means, at the beginning all the subkeys have to be computed once (there are 11 subkeys used in the 10 rounds of AES-128), stored, and used to encrypt many messages. The encryption of all these message blocks uses the same set of 11 subkeys. Thus, the manner in which this test tests the efficiency of the key schedule does not matter because the subkeys have to be computed just one and used repeatedly in a lot of message encryptions(block message).However, this test only focuses on the speed ratios of the key-setup time to single block encryption.

The second test is done when the cipher is used as an underlying primitive for other cryptographic constructions, e.g. hash functions. Then, the master key is changed on every iteration, and sequentially, the subkeys have to be recomputed. In this context, the efficiency of the key schedule comes to a forefront, and has a significant impact on the efficiency of the whole cipher (the whole cryptographic construction). However, the key changes for each message block. This "hashing method" which constructs the Hash function based on a block cipher, is the same as "on the fly" an approach that implements Key schedule Rijndael. Here, the 11 subkeys have to recompute every new message block. Therefore, the efficiency of the key schedule matters because, the more efficient the key schedule is, the faster the cipher would be. Hence, the hash function that uses the block cipher so-called addressed as the Davies-Meyer hash function is defined as follows:

Take AES (M, K) to be the Tweak AES cipher (only modified in the key expansion function), where M is the message and K is the key.

Then, hash function can be defined as (actually a compression function) H (M, IV) as H (M, IV) = AES (M, IV) + IV.

Thus, the Davies-Meyer construction can be used to create a hash function from a block cipher. Figure 2 is the hash method mentioned in this study; it shows the Davies-Meyer hash function. The measure of efficiency (speed) for newly proposed key schedule will be theoretical and empirical with estimates being based on operational complexity used in AES-128-bits

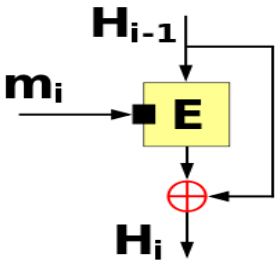

Figure 2. Davies-Meyer hash function

CONCLUSION (PLACEHOLDER1)

This paper presented a method to increase the security of the Rijndael block cipher of 128-bits by changing the current key expansion function , leading to maintain the requirement of bit confusion and diffusion properties. Besides that, this paper also proposed an evaluation of

the resistance of the differential cryptanalysis; that no such related-key differential characteristics exist on the full-round of 128 bits for key size of 128 bits. Currently, the increase in diffusion and confusion is the best solution to make the key expansion Rijndael more secured against attacks. Moreover, by adding non-linear transformation into the key expansion function, which leads to have more differential characteristic (active S-Boxes) proves that the cipher is most likely to be secured against differential attacks in related-key model based on the differential characteristics.

REFERENCES

Biryukov, A., & Khovratovich, D. (2009, December). 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.

Biryukov, A., & Nikolić, I. (2010, May). 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.

Bogdanov, A., Khovratovich, D., & Rechberger, C. (2015). Biclique cryptanalysis of the full AES. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 344-371). Springer Berlin Heidelberg.

Choy, J., Zhang, A., Khoo, K., Henricksen, M., & Poschmann, A. (2011, June). AES variants secure against related-key differential and boomerang attacks. In IFIP International Workshop on Information Security Theory and Practices (pp. 191-207). Springer Berlin Heidelberg.

Daemen, J., & Rijmen, V. (2013). The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media.

Fouque, P. A., Jean, J., & Peyrin, T. (2013). Structural evaluation of AES and chosen-key distinguisher of 9-round AES-128. In Advances in Cryptology–CRYPTO 2013 (pp. 183-203). Springer Berlin Heidelberg.

Gueron, S. (2012). Intel® Advanced Encryption Standard (AES) New Instructions Set. Intel Corporation

Mahmod, R., Ali, S. A., & Ghani, A. A. A. (2009). A shift column with different offset for better Rijndael security. Int. J. Cryptol. Res, 1(2), 245-255.

May, L., Henricksen, M., Millan, W., Carter, G., & Dawson, E. (2002, July). Strengthening the Key Schedule of the AES. In Australasian Conference on Information Security and Privacy (pp. 226-240). Springer Berlin Heidelberg.

Mouha, N., Wang, Q., Gu, D., & Preneel, B. (2012, November). Differential and linear cryptanalysis using mixed-integer linear programming. In International Conference on Information Security and Cryptology (pp. 57-76). Springer Berlin Heidelberg.

Muda, Z., Mahmod, R., & Sulong, M. R. (2010). Key transformation approaches for Rijndael security. Information Technology Journal, 9(2), 290-297.

Muda, Z. Y. (2015). Tshiftcolumn:A New Transformtion in 128-BIT Rijndael Key Expansion To Improve Security Requirements. *Journal of Theorotical &Applied Technology, 73*(1)

Sajadieh, M., Mirzaei, A., Mala, H., & Rijmen, V. (2016). A new counting method to bound the number of active S-boxes in Rijndael and 3D. Designs, Codes and Cryptography, 1-17.

Yan, J., & Chen, F. (2016). An Improved AES Key Expansion Algorithm. International Conference on Electrical, Mechanical and Industrial Engineering (ICMIE 2016)