Journal of Theoretical and Applied Information Technology
15th April 2019. Vol.97. No 7
© 2005 – ongoing JATIT & LLS
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AUTOMATIC SECURITY EVALUATION OF SPN-STRUCTURED BLOCK CIPHER AGAINST RELATED-KEY DIFFERENTIAL ATTACKS USING MIXED INTEGER LINEAR PROGRAMMING

[1]HASSAN MANSUR HUSSIEN, [2]SHARIFAH MD YASIN AND, [3]ZAITON MUDA, [4]NUR IZURA UDZIR

[1,2,3,4] Faculty of Computer Science and Information Technology, Universiti Putra Malaysia

E-mail: [1]*hassanalobady@gmail.com;* [2]*ifah@upm.edu.my*, [3]*zaitonm@upm.edu.my* and [4]*izura@upm.edu.my*

ABSTRACT

Block cipher algorithms become an essential domain in Information Technology (IT) due to ever increasing the number of attacks. In point of fact, it is significant to produce a security evaluation of block cipher algorithms to determine a statistical non-random behavior of attacks. In relation to this, a new theoretical attack such as related-key differential cryptanalysis (RDC) could give rise to a more practical technique. Basically, estimating immunity of lower bounds in the substitution-permutation network (SPN) block ciphers structure against RDC attack is essential for providing a secure block cipher algorithm. Currently, the automatic computer tools are not applicable to estimate the immunity against related-key differential attacks for SPN block ciphers structure. We present a searching strategy that determines the lower bounds of SPN block ciphers structure against RDC using the Mixed Integer Linear Programming (MILP). This study also aims to demonstrate the applicability and the efficiency of the MILP technique by examining the security of Rijndael block cipher in RDC attack. We prove this technique through calculate the number of activation S-boxes into Rijndael block cipher. The extended MILP technique is able to provide an automatic security estimation tool by giving accurate results. Overall, it is applicable to an extensive variety of block cipher algorithm that makes it an adaptable tool for industrial purposes and scholarly research.

Keywords: *Related-key Differential Cryptanalysis, Mixed Integer Linear Programming (MILP), SPN-structured Block Cipher, Rijndael, and Automatic Search Tool*

1. INTRODUCTION

Block ciphers have recently been gaining popularity due to many new designs such as RFID tags. The block cipher gave certain criteria in order to provide encryption, integrity and authentication functionalities such as cryptographic hash functions, pseudorandom number generators, and security protocols. Subsequently, block cipher security is of prime importance in almost whole security applications. However, the security of modern block ciphers algorithms might not be accurately proved .It is necessary to provide a security evaluation of block cipher margins. Several methods for evaluation are differential cryptanalysis (DC) and related-key model which were presented for attacking the block cipher algorithm. The differential cryptanalysis (DC) is a method used to discover the non-random behavior of block cipher algorithms. This is done via analyzing the differential of input and output of the block cipher without taking into consideration the key schedule of the block cipher [1] . Whereas related-key differential cryptanalysis (RDC) is the most prevalent technique in the statistical behavior analysis of symmetric-key cryptographic primitives [2]. In the model of related-key attack the adversary encrypts plaintexts or decrypt cipher texts under a set of keys connected via a known relationship. Moreover, the key schedule is part of the primitive over which a differential probability is constructed [3], [4] . The attacker aims to recover the keys and to work only with the sub-keys of the key schedule. This is done by looking for the differences in the differential characteristic (active S-boxes bytes) of a sub-keys byte of the key schedule. Meanwhile, the attacker

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

works only on the class of the sub-key, in which the maximum differential propagation probability of an S-box is the number of ordered pairs with input difference Δ_1 and output difference $\Delta_\circ$ divided by the total number of pairs with the difference between input and output [5] .In the literature, many combinations of differential cryptanalysis and related-key model were introduced to attacks block cipher algorithms. Such as, related keys model combined with the impossible differential [2] , the differential-linear attack [6] and the rectangle attack [7] . Moreover, boomerang combined with a related-key model to attack the AES-128 which is able to reduce the round to five out of ten rounds [8], [9]

The resistence of related-key differential attacks is fundamental in the design of a secure block ciphers. In relation to this, during the procedure of designing a new block cipher, the security estimation of a block cipher occasionally needs to be repeated a few times. Hence, even though not crucial, a good CPU time is a desirable feature. On a more important note, there is a need to design also and implement a technique to make sure that the computation is completed within a logical amount of time. Definitely, this task is hard somehow and probably will be introduced bugs and need to check the correctness or the optimality of the computed solutions might not be so easy. In relation to this, much simpler and more efficient tools have been introduced, particularly named as mixed integer linear programming (MILP) technique [10]–[14] . MILP is an optimization technique that attempts to maximize or minimize a specific objective function consists of numerous variables subjected to linear constraints on that variables. The field of MILP has received extensive study and achieved great success in both academic and industrial worlds. As a result, in recent years MILP technique has remained as a useful tool in cryptographic research.

The aim of this paper is to propose a technique to prove security bounds against related-key differential cryptanalysis (RDC) via applying mixed integer linear programming technique. The focus will be on examining the security of Rijndael-128, Rijndael-192, and Rijndael-256 against an RDC. We show that our MILP is applicable to evaluate the security of SPN- structured cipher with respect to related-key attacks. We demonstrate that the best related-key differential attacks for Rijndael-128, 192, and 256 bits 20, 26, 30 actives-boxes respectively. RDC is applicable to 9-round reduced Rijndael-192 with 3 related keys, 11-round reduced Rijndael-256 with 3 related keys. The paper is organized as follows: In Section 2 we review the related works of automatic security evaluation. In Section 3 we present the proposed scheme alongside to describes the construction of MILP technique on Rijndael block cipher in the related-key attack. In Section 4, we discussed the results of the newly RDC. In Section 5 we conclude the paper.

2. RELATED WORKS

Several studies had been carried out to develop searching algorithms to determine the ability of cryptanalysis. The upper bound on the probability of the best differential characteristics in a block cipher algorithm for intents to give and demonstrate the resistance against differential cryptanalysis (DC). whereas the bound is low for intents to give and demonstrate resistance against related-key differential cryptanalysis (RDC). Three variants of Matsui's algorithm were developed to determine an upper bound and lower bound of activation S-boxes in the byte-oriented (SPN-structured) block ciphers. Matsui's algorithm involves long time computations to determine the differential characteristics [15] . Other methods in [16], [17] used a variation of Dijkstra's algorithm to determine an maximum (differential characteristics) active S-boxes in related-key attacks on SPN-structured block ciphers with an transformation linear function in the number of rounds. Dijkstra's algorithm is quite complex structures algorithm to search for differential characteristics in such an SPN-structured cipher, thus making them impossible to use without first reading through a lengthy explanation from the authors beforehand. In [18], [19] , proposed to use Constraint Programming (CP) model to detect the differential characteristics of the RDC against the standard of SPN-structured ciphers. Constraint programming requires a lot of time either in construction of (CP) model on SPN-structured ciphers or when solving the constraint equations to find the differential characteristics. On a more important note, finding AES related-key differentials is an extremely combinatorial problematic that hardly gauges. For example, the approach of [15] takes some of the megabytes of memory, but it involves several days and several weeks of calculation for AES-128 and AES- 192 respectively. Obviously, each of this problem must be solved only once, and CPU time is not the main issue provided that but, it is a reasonable amount of the time in order to determine the activation of S-boxes. However , the approach of [16] requires about 60 GB of memory for 5 rounds of AES-128 and has not been extended to AES-192 nor AES-256.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

On top of that ,the CP approach of [18], [19] is applicable to find the differential characteristic of SPN-structured block ciphers, but it should be noted that the time to solve the model is requires higher computation to be completed.

Mixed Integer Linear Programming (MILP) technique is utilized to determine the maximum or minimum of the objective function. For example, covering problem and packing problem into new search strategy to find the linear and differential characteristic. The technique has been introduced into linear and differential cryptanalysis by [10] , the following studies have improved the method [11]–[14] base on improvements application for searching of differentials and linear approximations in block cipher algorithms, each of transformation function in particular block cipher can be precisely designated by inequalities classification including non-linear transformation such as substitution-box and addition modular. Using the optimization solver software can speedup finding the feasible and optimized solution. In relation to this, it can search the optimal characteristic for the target block cipher algorithms with a very reasonable amount of time. MILP technique can be utilized to search for differential characteristics of related key model attacks with reasonable time. This is the inspiration for us to do this work. In the approach of [20] , presented an automated tool rely on MILP to find the maximum amount of activation S-boxes in form of SPN-structured block cipher algorithms, but in the secret-key model attacks. On a more important note, the [20] approach not applicable to applied directly either in Feistel cipher block structure in form of bit-oriented block cipher algorithms or in related key attacks . In relation to this, [11] improved this technique to be applicable to block cipher algorithms including - bit-oriented transformation function .By presenting newly symbols of XORing in order to be labeled the bit transformations function. As well as, consider the effects of combined diffusion on substitution-box and bitwise permutations. In [14] uses the improved MILP technique to be given a lower bound of the differential characteristic on the related-key differential attacks which is only in 128-bits key expansion function of AES block cipher.

based on the critical review above-mentioned, the most automatic computer tool requires less programming effort compared with other existing techniques, which is MILP. In this technique, what an investigator needs to write compose a program in order to develop the MILP model with appropriate objective function and constraints appoint to the differential propagation in such block cipher. The rest of the work is to determine either upper or lower bounds might be done by a highly optimized open-source or commercially available software, for example, CPLEX, SCIP, and Gurobi .The approach of [20] used arrangement either of a 0 or 1 variables, which defines the differential propagation out of the rounds transformation function for SPN-structured in form of word-oriented of block cipher algorithms in secret-key model attacks. In addition, the approach of [11] [21] use the MILP to obtain security bounds of a Feistel cipher structure in form of bit-oriented block cipher algorithms, which is applicable for both the secret key attacks and related key attacks. The technique used in this research is considered to be a MILP. On the contrary of two previous approaches, the proposed scheme of this research is applicable to SPN-structured in form of word-oriented of block cipher algorithms in related-key model attacks.

3. PROPOSE SCHEME

This section covers the construction of the automatic tool in this study, which is based on Mixed Integer Linear Programming (MILP), to prove the resistance of SPN-structured block cipher in related-key model attacks. The MILP is described in detail alongside with variable representation in the MILP technique followed with each variable for generating the constraints involved in the automatic tool.

3.1 Construction of Mixed Integer Linear Programming Technique on SPN-structured Block Cipher in Related-key Model Attacks.

The mixed integer linear programming (MILP) is a method that attempts to maximising or minimising the objective function of numerous variables subjected to certain linear constraints on that variables. The MILP problem can be formally described to find a vector $x \in zk \times R^{N-k} \sqsubseteq R^n \, with \, A_x \leq b$,(1) such that the linear function $C_1x_1 + C_2x_2 + \cdots + C_nx_n$ is minimized or maximized, where $(c_1, \ldots\ldots, c_n) \in R^n, A \in R^{m\times n}$, and $b \in R^m$.

MILP is a method that refers to this particular arrangement as the 0-1 to describe the variables in SPN structures of a block cipher base on word-oriented construction with respect to related-key model attacks. This particular method automatically evaluates the security of SPN structures of the block cipher. The word-oriented differentials propagating

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

through several rounds out of the linear round transformation and key schedule algorithm in such particular block cipher. These operation transformations represent the variables in an objective function that subject to certain constraints. The mechanism of construction of the MILP is based on generating an equation and solving the problem with free academic optimization software. This study assumed that a block cipher will be composed of the following operations. Firstly, construct the MILP tool on round transformation in the SPN cipher structure includes either of linear or non-linear transformation via using the Equation L: $F_{2^w}^m \rightarrow F_{2^w}^m$. Secondly, construct the MILP tool on the key generations part in SPN cipher block structure includes either of linear or non-linear key schedule via using the equation Xor: $F_2^w \; X \; F_2^w \rightarrow \; F_2^w$. Finally, the Objective function is Minimize of the constraint on the standard linear programming variables includes round transformation and the key generations part variables by using the equation minimize objective function: $\sum \mathrm{F}_2^{\mathrm{w}} \rightarrow \mathrm{F}_2^{\mathrm{w}}$. The construction of the MILP tool based SPN block cipher is shown in Algorithm 1. More importantly, the full source code of tool for this study is available in GitHub https://github.com/hassanalobady

Algorithm 1: MILP Technique

Minimize (Objective function)

Minimize is sum of the variables of activation S-boxes tend to use the following equation $\sum \mathrm{F}_2^{\mathrm{w}} \rightarrow \mathrm{F}_2^{\mathrm{w}}$ that consists of round transformation and the key generations part in SPN block cipher structure.

Subject To (Constraints)

Which is a linear inequalities constraint in the variables of the objective function.
For each linear or non-linear round transformation step (+1 dummy variable) in SPN block cipher structure by using the L: $F_{2^w}^m \rightarrow F_{2^w}^m$.
For each sub-key generation in SPN cipher structure, which consisted of a linear or non-linear key schedule by using Xor Constraint, $\oplus$, $:F_2^w \; X \; F_2^w \rightarrow \; F_2^w$

Binary

All variables / All input variables presented

End

3.1.1 Constrained Variable Generation for Linear and Non-linear Transformation Operations

Generate the constrained variable in MILP tool based on the round transformation of the SPN cipher structure. These variables are taking from either of a linear or non-linear round transformation in such block ciphers. The following equation 1 shown how the variables are taken by mapping the round transformation.

$$\mathrm{L}: F_{2^w}^m \rightarrow F_{2^w}^m \qquad (1)$$

$$BL = \min_{a \neq 0} \{wt(a \| L(a)) : a \in F_{2^w}^m\}$$

Wherever the $wt(a\|L(a))$ is the amount of non-zero entries of the 2m-dimensional vector $a\|L(a) : a \in F_{2^w}^m$.

The 0-1 arrangement variable is indicating the word-oriented whether linear or non-linear round transformation. The abovementioned Equation (1) is added in order to keep track of the indices differences between the input and the output. Whereby it is agreed as follows that input and output difference are composed of round transformation into the SPN block cipher structure. To be assumed that $\{\boldsymbol{i_0}, \ldots\ldots, \boldsymbol{i_{n-1}}\}$ as well as $\{\boldsymbol{j_0}, \ldots\ldots, \boldsymbol{j_{n-1}}\}$ are the permutation layer of such a round transformation function $\{\boldsymbol{0}, \ldots\ldots, \boldsymbol{n-1}\}$. Afterward, let X_{ik} , y_{ik} , along with, k are $\in \{0, \ldots\ldots, n-1\}$, As so the variables have been subjected to the follows constraints

$$\begin{cases} \sum_{k=0}^{n-1} \left(\mathrm{X_{i\,k}} + \mathrm{y_{j\,k}} \right) \geq \mathrm{B_L\, d_L} \\ \mathrm{d_L} \geq \mathrm{X_i} \\ \ldots\ldots \\ \mathrm{d_L} \geq \mathrm{X_{i\,n-1}} \\ \mathrm{d_L} \geq \mathrm{y_{j0}} \\ \ldots. \\ \mathrm{d_L} \geq \mathrm{y_{j\,n-1}} \end{cases}$$

Wherever the $\mathbf{d_L}$ variable is a dummy data request whether 0 or 1 in value, or the value of $\mathbf{B_L}\,\mathbf{d_L}$ is the number of branches into the non-linear or linear round transformation.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1.2 Constrained Variable Generation for XOR operation

The constrained variables are generated by the MILP tool based on the key schedule algorithm into SPN block cipher structure. These variables are inspired by each XOR operation to the linear or non-linear key schedule in such block ciphers. The following equation 2 shown how the two input variables are taken by mapping the key schedule algorithm.

$$\text{Xor: } F_2^w \; X \; F_2^w \rightarrow \; F_2^w \qquad (2)$$

Each of those XORs operations it may be having either positive or negative variables in every difference input with respect to related-key attacks. The abovementioned Equation (2) is added into each of the sub-key XOR operations in SPN block cipher structure. This particular variable might have no difference or receive at most one non-zero input difference. Subsequently, the XORs operation may be ignored if only have no effect on the output difference in such constrained variables. Meanwhile, all the XORs operation in a block cipher must take into consideration in the related-key attacks. To be assumed that $A, B \; are \; \in \; f_2^w$ which is composed of the input difference of XORs operations within either a non-linear or linear key schedule algorithm, and AddRoundKey of such block cipher algorithm. Also, $C \; \in \; f_2^w$ if it only has output difference. As so the variables have been subjected to the follows constraints.

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

Where the $\boldsymbol{d}_{\oplus}$ variable is dummy data that takes whether 0 or 1 in value, and the value is the number of branches into a non-linear or linear key schedule algorithm

3.2.3 Constrained Variable Generation for Objective Function(S-box)

The constrained variables are generated by the MILP tool based on round transformation and the key schedule algorithm into SPN block cipher structure. These variables are inspired by the objective function which is minimized of the constraint on the standard linear programming. The following equation 3 shown how the input variables are taken by mapping round transformation function and the key schedule algorithm.

$$\text{Minimize Objective Function} : \sum F_2^w \; \rightarrow \; F_2^w \quad (3)$$

This study presents a new 0-1 arrangement variable A_i to perform the activation of the S-boxes in such SPN block cipher algorithm whether the s-boxes is active or inactive. Whereby each difference input $\Delta_i \in F_2^w$ of the entire SPN block cipher algorithm is minimized by the objective function. For instance, let $A_i = 1$ or $A_i = 0$ for $\Delta_i \neq 0$ or $\Delta_i = 0$, respectively. The full number of activation S-boxes $'\sum_i A_i$ bytes are selected as the objective function to be subjected to constraints variable inspired via the operation function of the SPN block cipher algorithm. On a more important note, an S-box may be active if only it has a difference in the particular input $A_i = 1$.

3.2 Related-key Differential cryptanalysis of Rijndael block cipher

The related-key differential attack RDC is extended method of differential cryptanalysis (DC) that permits the adversary to detect the encryption of different plaintext via different set of keys. Moreover, the key schedule algorithm is part of the primitive over which a differential probability is constructed. The set of keys is initially unknown to the adversary, but he knows that a specific fundamental mathematical relationship that holds between them.

Rijndael round transformation is composed of four different transformations function, which are the SubBytes, ShiftRows, MixColums, and AddRoundKey, as depicted in Figure 1. However, the final round only covers three transformation functions. We develop a tool to search for the best related-key differential probability characteristics of an S-box (differential characteristics) in an SPN for Rijndael 128-bit, 192-bit, 256-bit. On a more important note, constructing of the MILP model on round transformation of Rijndael block cipher can be used vis applying Equation 1: L: $F_{2\,w}^m \rightarrow F_{2\,w}^m$.

The SubBytes transform (SB) applies the same 8-bit to 8-bit bijective S-box S 16 times in parallel on each byte of the state. For example, 8-bit "00000000" is swap into "01100011". In relation to this, the SB do not provide equations or variables in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MILP model, which only require that one S-box (differential characteristics) at least to be active, for which the SubBytes transformation preserves this property.

The ShiftRows transform (SR) simply shifted the variables to ensure that each new column contains one byte from one of the 4 old columns. Thus, it achieves Full diffusion in 2 rounds of Rijndael. In regard to this, SR transformation did not introduce any linear constraints to the MILP-based approach, in which the only permutation of the bytes involves the internal state of Rijndael.

The MixColumns transform (MC), replaces each of the four columns of the state by multiplication M × C where M is a constant 4 × 4 maximum distance separable matrix over GF (2^8). The MC step can also be viewed as a multiplication by a particular Maximum Distance Separable (MDS) matrix in a finite field. In relation to this, the MILP uses 9 equations for every step of MDS property, MC is ensured by posting a constraint on the sum of some variables (+1 dummy variable) and introduced a linear constraint to the MILP.

Rijndael Key schedule algorithm take separate input data that turn a master key of bytes into outputs expanded keys of 16×11, 16×13, and 16×15 bytes respectively, for Rijndael 128-bit, 192-bit, and 256-bit. The expanded keys process is composed of RotWord, SubByte, and Rcon, as depicted in Figure 2 . In relation to this, the process of construct MILP model can be done via applying Equation 2: Xor : $F_2^w \; X \; F_2^w \rightarrow \; F_2^w$. On a more important note, MILP proposed scheme redefined the variables of constraints for XORing transformation in order to prevent invalid characteristics due to an extensive feasible region caused by inaccurate constraints of XOR transformation and accomplished a tighter security bound of differential characteristics. However, AddRoundKey (ARK) operation is combining each byte of the state with the corresponding byte of the subkey using bitwise XOR. From this perspective, it should be noted that ARK is performing Xor bitwise operation, thus ensuring that each byte of Xor bitwise processing is constructed via Equation 2.

AddRoundKey (ARK) and KeySchedule(KS): Both ARK and KS are modeled with XOR constraints, introduces linear constraint into the MILP. This is considering that the XOR $y = x_1 \oplus x_2$ of two variables $x_1, x_2 \in \{0, 1\}$, x_1 perform with sub-keys and x_2 is the round function state. The same holds true for the key expansion function (calculation of round keys).

A practical approach to evaluate the security of a SPN- structured block cipher against related-key differential attacks is to determine the lower bound of the number of active S-boxes of all rounds throughout the cipher and key; hence, proving the resistance of the Rijndael block cipher against related-key differential attacks. This would allow the author to build a differential characteristics on all rounds, for which the Rijndael block cipher have the formal properties as follows:

1) No differential characteristics will occur on the full rounds with a probability higher than 2^{-128}, 2^{-192} and 2^{-256} where k is 128 bits , 192 bits and 256 bits respectively . Certainly, this determination is presented to stop the related-key differential attacks on the full rounds of Rijndael block cipher.

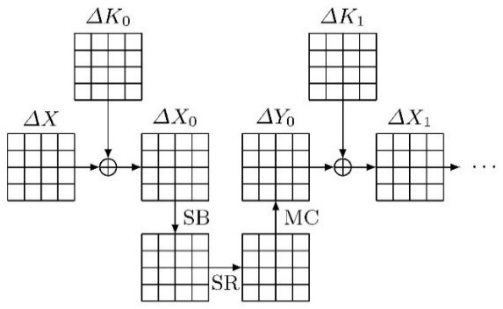
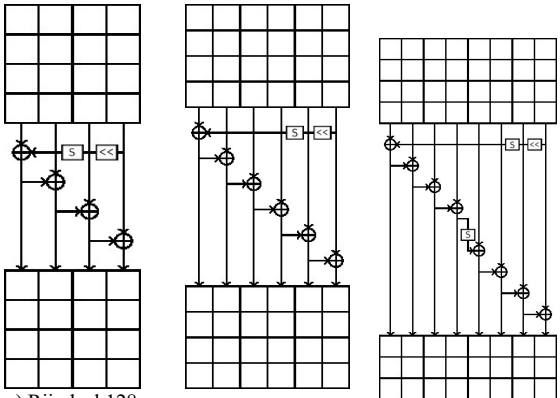


Figure 1: Illustration of Rijndael round transformation



a) Rijndael 128-bit b) Rijndael 129-bit c) Rijndael 256-bit

Figure 2: Illustration of Rijndael Key schedule algorithm

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4 RESULTS AND DISCUSSION

Mixed integer linear programming performed with construction on three variants of Rijndael block cipher. The focus will be on prove security bounds against related-key differential (RDC) by finding the best differential characteristic for the including both key schedule and main round transformation. The related-key differential characteristics (RDC) of Rijndael 128-bit, Rijndael 192-bit, 256-bit are summarized respectively in Tables 1, 2 and 3. Figure 3 ,4 ,5 visualized the results of Table 1, 2, 3 respectively giving better illustration of the overall RDC results. Mainly, the highlighted maximum differential probability is the highest requirement threshold in order to stop related-key differential attacks on the full rounds of Rijndael block cipher to occur. The MILP equations were generated using C# programming and resolved via optimizer Gurobi run on personal pc (ubuntu 14.04) with Intel Core i7 (2.30GHz, 12 GB RAM).

From Table 1 the MILP equations correspond with complete rounds of Rijndael 128-bit in the related-key attacks (RDC) composed of 0-1 arrangement with 334 variables, 1790 continuous variables, and 3640 constraints. These equations can be solved in 171 seconds which is approximately 3 minutes. The minimum number of differential characteristics (active s-boxes) are 20. Meanwhile, the max differential propagation differential of an S-box in the Rijndael block cipher is $4/256$, which approximately equals 2^{-6} based on the Difference Distribution Table (DDT). In relation to this, the maximise probability on differentials of the Rijndael 128-bit cipher is approximately $2^{-6\,(20)} = 2^{-120}$, which is higher than 2^{-128}. Despite the fact that this is slightly higher than the probability requirement threshold in order to stop related-key differential attacks, we expected that the estimated minimum number of active S-boxes should be greater than 22. On a more important note, the problem of completely proving the security of the complete round of Rijndael 128-bits against related-key differential attack in the face of the cryptographic standards is still an open problem. Therefore, we have proved that Rijndael 128-bit is somehow insecure against related-key differential attack. Figure 3 illustrates that the best differential characteristics for ten rounds of the round transformation and key schedule compared to max differential probability.

For Rijndael 192-bit can gain the results for its reduced round version on 12 rounds in a related-key differential attack. RDC is applicable to 9-round reduced Rijndael-192 with 3 related keys. The executed time to solve the 0-1 arrangement with 591 variables, 3255 continuous variables, with 6442 constraints take 3595 second, which is approximately 1 hour, the results recorded in Table 2. For example, the best related-key differential in terms of valid differential characteristics for 12-round Rijndael 192-bits are minimum bounded by $2^{-6\,(26)} = 2^{-156}$ is higher than the required threshold of 192-bit level of security for the differential probability 2^{-192}. In regard to this, the valid differential characteristics for 12-round Rijndael 192-bit is illustrates in Figure 4 compared to a required threshold of differential probability. This also means that Rijndael 129-bit is unable to archive the higher differential characteristics (active s-boxes) in order to prevent the related-key differential attacks

From these results, Table 3 shows the best related-key differential characteristic probability of full 14-round Rijndael 256-bit is minimum bounded by $2^{-6\ (30)} = 2^{-180}$. RDC is applicable to 11-round reduced Rijndael-256 with 3 related keys. The executed time to solve the 0-1 arrangement 908 variables, 4880 continuous variables, with 10192 constraints take 5593 second, which is approximately 2 hours. However, the probability is success for an exhaustive search in order to reduce the round of 256 Rijndael version. In relation to this, it should be noted that Rijndael 256-bit is insecure against straightforward related-key differential attacks even within full 14-rounds. Figure 5 illustrates the best differential characteristics for full 14-rounds of the round transformation and key schedule compared to best valid differential characteristics probability.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Related-key differential characteristics (RDC) for Rijndael 128-bit

Round	#Variables	#Constraints	Active S-boxes	Timing (in seconds)
1	64 + 80	364	0	1
2	94 + 270	728	1	1
3	124 + 460	1092	3	1
4	154 + 650	1456	9	3
5	184 + 840	1820	11	10
6	214+1030	2184	12	26
7	244+1220	2548	14	36
8	274+1410	3912	17	46
9	304+1600	4276	19	111
10	334+1790	4640	20	171

Table 2: Related-key differential characteristics (RDC) for Rijndael 192-bit

Round	#Variables	#Constraints	Active S-boxes	Timing (in seconds)
1	96+120	546	0	1
2	141+405	1092	1	1
3	186+690	1638	4	2
4	231+975	2184	10	5
5	276+1260	2730	13	13
6	321+1545	3276	14	23
7	336+1830	3822	16	113
8	411+2115	4368	18	185
9	456+2400	4914	19	218
10	501+2685	5460	20	1540
11	546+2970	6006	23	2145
12	591+3255	6442	26	3595

Table 3: Related-key differential characteristics (RDC) for Rijndael 256-bit

Round	#Variables	#Constraints	Active S-boxes	Timing (in seconds)
1	128+160	728	0	1
2	188+540	1456	1	5
3	248+700	2184	5	13
4	308+1080	2912	11	15
5	368+1460	3640	14	27
6	428+1840	3468	15	123
7	488+2220	5096	17	1510
8	548+2600	5824	19	1843
9	608+2980	6552	21	3595
10	668+2360	7280	23	3955
11	728+3740	8008	25	4390
12	788+4120	8736	27	4791
13	848+4500	9464	28	5193
14	908+4880	10192	30	5593

Journal of Theoretical and Applied Information Technology
15th April 2019. Vol.97. No 7
© 2005 – ongoing JATIT & LLS
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The best valid differential characteristics probability is illustrated in Figure 3 based on the total number of rounds in the Rijndael 128-bit block cipher. The resistance of Rijndael 128-bit against related-key differential attack is somehow closer to a maximum differential probability in order to reach a required threshold of 2^{-128} level security. The underlying weakness is due to its fewer number of active s-boxes found in this variation of the Rijndael block cipher.

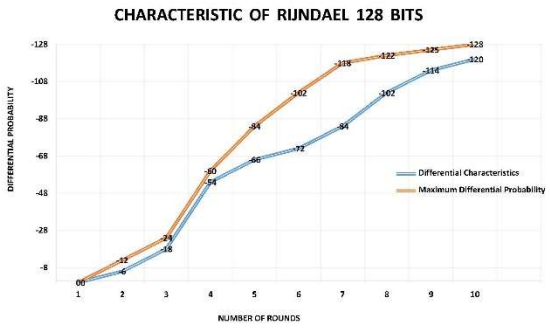


Figure 3: Comparison of best differential characteristics and Maximum differential probability for 10-rounds

Figure 4 illustrates the total number of rounds in the Rijndael 192-bit block cipher analyzed from both the maximum differential probability and the best differential characteristics. Additionally, the line highlighted in blue, are the best valid differential characteristics probability. As a result, the evidence that the Rijndael 192-bit failed to achieve the highest level of security to reach a required threshold of 2^{-192} level security due to its fewer activation of s-boxes are found.

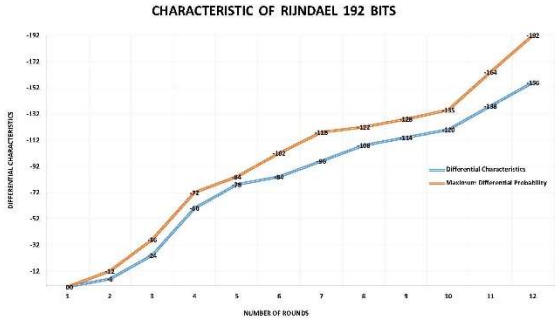


Figure 4: Comparison of best differential characteristics and Maximum differential probability for 12-rounds

The resistance of Rijndael 256-bit is insecure against related-key differential attack. As demonstrated in Figure 5, the analysis results of best valid differential characteristics probability for 14 rounds do not meet the requirement threshold of 2^{-256} level security to prevent the attack from occurring. This is mainly due to less activation of s-boxes are found in this variation of the Rijndael block cipher.

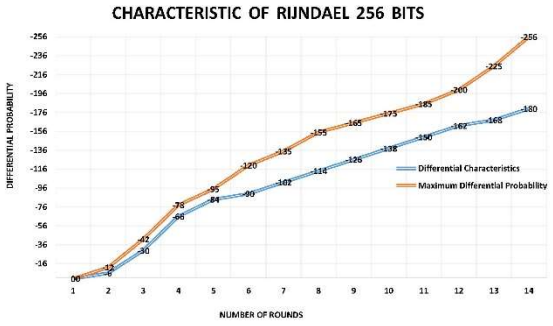


Figure 5: Comparison of best differential characteristics and Maximum differential probability for 14-rounds

5 CONCLUSION

This research aims to develop an automatic tool for the security evaluation of the SPN- structured block cipher in related-key differential cryptanalysis (RDC). Mixed integer linear programming approach is proposed in this research. This method counts the minimum amount of activation S-boxes (finds RDC) in each number of rounds for a block cipher. One significant advantage of the MILP technique that it is applicable to an extensive variety of block cipher algorithms, which is composed of a combination of S-box operation, linear permutation layers and/or exclusive-or (XOR) operations, and less programming effort and less execution time is needed with this technique compared with previous works. Meanwhile, the MILP proposed technique managed to demonstrate Rijndael 128-bit,192-bit and 256-bit have an insufficient amount of activation S-boxes in order to prevent related-key differential cryptanalysis from occurring. Further work is required to investigations this security margin of Rijndael block cipher, someone needs to prove the resistance against related-key differential attack (RDC). The currently proposed tool can be further explored to construct or check others block cipher structures such as ARX-based and Generalized Feistel Networks (GFN) against related-key differential attack.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ACKNOWLEDGMENTS

The authors are thankful to the Ministry of Higher Education (MOHE) for the award of Fundamental Research Grant (FRGS) Scheme Vote No. 5524822, which has supported this research.

REFERENCES:

[1] D. Gerault, M. Minier, and C. Solnon, "Constraint programming models for chosen key differential cryptanalysis," in *International Conference on Principles and Practice of Constraint Programming*, 2016, pp. 584–601.

[2] G. Jakimoski and Y. Desmedt, "Related-Key Differential Cryptanalysis of 192-bit Key AES Variants," *Springer-Verlag Berlin Heidelb.*, pp. 208–221, 2004.

[3] E. Biham, "New types of cryptanalytic attacks using related keys," *J. Cryptol.*, vol. 7, no. 4, pp. 229–246, 1994.

[4] J. Kelsey, B. Schneier, and D. Wagner, "Related-key cryptanalysis of 3-way, biham-des, cast, des-x, newdes, rc2, and tea," in *International Conference on Information and Communications Security*, 1997, pp. 233–246.

[5] H. M. Hussien, Z. Muda, and Sharifah Md Yasin, "Enhance The Robustness Of Secure Rijndael Key Expansion Function Based On Increment Confusion," *6th Int. Conf. Comput. Informatics*, no. 169, pp. 722–728, 2017.

[6] P. Hawkes, "Differential-linear weak key classes of IDEA," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 1403, pp. 112–126, 1998.

[7] J. Kim, G. Kim, S. Hong, S. Lee, and D. Hong, "The related-key rectangle attack--application to SHACAL-1," in *Australasian Conference on Information Security and Privacy*, 2004, pp. 123–136.

[8] E. Biham, O. Dunkelman, and N. Keller, "Related-key boomerang and rectangle attacks," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2005, pp. 507–525.

[9] A. Biryukov, "The boomerang attack on 5 and 6-round reduced AES," in *International Conference on Advanced Encryption Standard*, 2004, pp. 11–15.

[10] N. Mouha, Q. Wang, D. Gu, and B. Preneel, "Differential and linear cryptanalysis using mixed-integer linear programming," in *International Conference on Information Security and Cryptology*, 2011, pp. 57–76.

[11] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song, "Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES (L) and other bit-oriented block ciphers," in *International Conference on the Theory and Application of Cryptology and Information Security*, 2014, pp. 158–178.

[12] S. Sun, L. Hu, L. Song, Y. Xie, and P. Wang, "Automatic security evaluation of block ciphers with S-bP structures against related-key differential attacks," in *International Conference on Information Security and Cryptology*, 2013, pp. 39–51.

[13] A. Abdelkhalek, Y. Sasaki, Y. Todo, M. Tolba, and M. Youssef, "MILP Modeling for (Large) S-boxes to Optimize Probability of Differential Characteristics," *IACR Trans. Symmetric Cryptol.*, vol. 2017, no. 4, pp. 99–129, 2017.

[14] H. M. Hussien, Z. Muda, and S. Yasin, "New Key Expansion Function of Rijndael 128-Bit Resistance to the Related-Key Attacks," *J. Inf. Commun. Technol.*, vol. 3, no. 3, pp. 409–434, 2018.

[15] A. Biryukov and I. Nikolić, "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*, 2010, pp. 322–344.

[16] P. Fouque, J. Jean, and T. Peyrin, "Structural Evaluation ofAES and Chosen-Key Distinguisher of 9-round AES-128," in *Advances in Cryptology–CRYPTO*, 2013, pp. 183–203.

[17] M. Sajadieh, A. Mirzaei, H. Mala, and V. Rijmen, "A new counting method to bound the number of active S-boxes in Rijndael and 3D," *Des. Codes, Cryptogr.*, vol. 83, no. 2, pp. 327–343, 2017.

[18] D. Gerault, M. Minier, and C. Solnon, "Constraint Programming models for chosen key differential cryptanalysis," *Lect.*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9892 LNCS, pp. 584–601, 2016.

[19] D. Gérault, P. Lafourcade, M. Minier, and C. Solnon, "Revisiting AES Related-Key Differential Attacks with Constraint Programming.," *IACR Cryptol. ePrint Arch.*, p. 139, 2017.

[20] N. Mouha, Q. Wang, D. Gu, and B. Preneel, "Differential and Linear Cryptanalysis using Mixed-Integer Linear Programming," *Int. Conf. Inf. Secur. Cryptol.*, pp. 57–76, 2012.

[21] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song, "Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SIMON, PRESENT, LBlock, DES(L) and Other Bit-Oriented Block Ciphers," in *In International Conference on the Theory and Application of Cryptology and Information Security*, 2014, no. L, pp. 158–178.