Technium Vol. 4, No.10 pp.15-30 (2022)
ISSN: 2668-778X
www.techniumscience.com

Differential Distribution Table implementation DDT: survey

Mohammed Eid Khamees Al-Shammary [1,2], Sufyan Salim Mahmood Al-Dabbagh[1]

[1] Department Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul/Iraq
[2] E-mail: mohammed.20csp84@student.uomosul.edu.iq

Abstract. The security of the transmitted data is one of the important issues that led to improve cryptosystems. Block ciphers as symmetric key cryptosystems are widely implemented in different applications and devices. Many algorithms had been presented that proposed new designs and enhancements for the block ciphers. Most of these papers based on the differential characteristics that provided by the Differential Distribution table DDT. The implementation of DDT had several points of advantages in design, modify and attack block cipher. Even with larger block size of some cipher families, the Partial Differential Distribution Table (PDDT) is implemented to override the big block size. The comparison results showed that both of DDT and PDDT are efficient tools that provide important differential characteristics that may implemented with accompanied of different function and deep learning models.

Keywords. Cryptography, Block cipher, Cryptanalysis, The Differential Distribution Table DDT, PDDT.

1. Introduction

The rapid development of information technology accompanied by internet spread all over the world led to arising of several issued including data security. The cryptosystems are used to maintain the security of the transferred data via internet to avoid unauthorized access and data hacking [1]. Many cryptosystems had been presented in both of its types: Symmetric and Asymmetric ciphers. They were widely implemented in varied fields of businesses to secure the confidential data from an unauthorized access. Thus, the security of the information became an important issue that led implement cryptosystems [2].

The cryptosystems became the common targets for both researchers, and attackers. Many studies had been presented to evaluate the robustness of the cryptosystems and its potentials to face attacks [3]. While attackers had improved their attack strategies to break those cryptosystems. Thus, researchers aimed to improve the robustness of the cryptosystems that are implemented in the data systems [4]. In the scientific search, cryptanalysis is one of the important fields that take more interest of the researchers. Specially, after the development of computers and information technology that allow attackers to break the targeted cryptosystems. Cryptanalysis had developed according to the improvements of the cryptosystems and the attack strategies. Cryptoanalysis simulate attacks to

evaluate the performance of the cryptosystems and discover the weak points that attackers may use them [5].

Block ciphers as a symmetric cryptosystem, is a class of ciphers that are widely used in the many systems such as social applications, communications and many other fields. Many encryption algorithms had been developed and modified to meet the state-of-art. The evaluation based on the results that are obtained from the cryptanalysis. Thus, linear and differential cryptanalysis were used in the proposed studies to evaluate the performance of the proposed block ciphers. Even the cryptanalysis, it had been improved by many proposed studies to increase the efficiency of the cryptanalysis methods [6]. As the result, the differential distribution table DDT is used to detect the status of the Substitution Boxes the block ciphers were built with. In fact, the DDT is an essential step in most of the differential cryptanalysis. Many studies proposed different methods and algorithms to improve the capability of differential cryptanalysis to recover the encryption kyes of the block ciphers [7].

There are several studies that reviewed the DDT implementation on cryptanalysis techniques and methods. In (Sehrawat & Gill, 2018), the authors presented a review paper for the proposed light weight block cipher that may be used in Internet of things (IoT). The reviewed works included some cryptanalysis method that performed to evaluate the performance of the proposed ciphers. Some of the studies delt with DDT in cryptanalysis and rebuilding the block cipher [8]. In (Dey & Ghosh, 2018), the authors illustrated two cryptanalysis methods and proposed another two methods to analyze the relations of the S.Boxes. One of the illustrated methods was differential cryptanalysis that based on DDT. One of the proposed method also was a differential cryptanalysis based on DDT[9]. In (Tentu , 2020), the author presented some of the known attack to evaluate the performance of some common used block ciphers. Some of the illustrated attacks were differential attacks and based on DDT[10].

This paper aims to summarize the proposed papers that presented DDT-based cryptanalysis methods that are recently proposed and illustrates the importance of the DDT implementation in such works. It also provides some comparisons among these proposed methods. The rest of this paper would illustrate the differential cryptanalysis and DDT in section2, the recent DDT-based works in section3, the comparison in section4 and finally the conclusions in Section5.

2. Differential Cryptanalysis

Cryptanalysis is “the science that studies the procedures, processes and methods used to translate or interpret secret writings, as codes and ciphers, for which the key is unknown”. Thus, the goal of cryptanalysis is enabling to analyze cryptosystems to be trusted [11]. Most of presented cryptosystems are based on the pseudo-random permutations PRP to generate the encryption key with acceptable randomness. The randomness of the encryption key increases the robustness of the block cipher. Thus, the robustness of block cipher is almost related with the randomness produced by PRP. Attackers aimed to recover the encryption key by removing the randomness via discover the linear or differential relation between the inputs and the outputs of the cryptosystem [12]. The following subsections would define the Differential cryptanalysis and its types and well-known tool DDT.

2.1. Definition

Differential cryptanalysis can be defined as "the powerful techniques in the analysis of symmetric-key primitives". It had been proved and widely implemented in block and stream ciphers. The following is a definition of the differential cryptanalysis.

A block cipher is a permutation parameterized by an encryption key $K \in F_2^k$, which is a map of for the set of plain_text $P \in F_2^n$, to a set of cipher_text $C \in F_2^n$:

$$E_K: F_2^k \times F_2^n \rightarrow F_2^n \quad . (1)$$

It is known that the block cipher is an iterative cipher, i.e., it is consisted of applying a simple round function for r times:

$$E_K(.) = f_r(.) o \ldots . o\, f_1(.) \quad . (2)$$

In the differential cryptanalysis, either the cryptanalyst or attacker looks at the pairs of plain_texts (p_1, p_2) and the correspondent pairs of cipher_texts (c_1, c_2), then find out the correlations between the differences α and β, where $\alpha = p_1 \oplus p_2$ and $\beta = c_1 \oplus c_2$.

Definition: "A differential is a pair of differences $(\alpha, \beta) \in F_2^n \times F_2^n$."[13]

It is possible to use this correlation as distinguisher for the block cipher if the correlation holds with high probability. It can remove the randomness of permutation and further use this to mount key-recovery attacks.

In fact, there are more detailed definitions of the cryptanalysis. But the previous one is just to notify the truth of the correlation between the pairs of both plain_texts (p_1, p_2) and the correspondent pairs of cipher_texts (c_1, c_2).

2.2. Algorithms for Differential Cryptanalysis

There many differential cryptanalysis algorithms, they are usually known as differential attacks. The following are some of the common algorithms of the differential attacks that had been used to attack the block ciphers.

2.2.1. Higher-order differential cryptanalysis

Higher-order differential cryptanalysis was presented in 1994 as one of the algebraic cryptanalysis algorithms that proved its efficiency in attack of block ciphers with low algebraic degree. The purpose of the naming is the extension of the differences (first-order derivatives).

Let (S, +), (T, +) be Abelian groups. For a function f : S → T, the i-th derivative of f at point (a1, a2, …, ai) is recursively defined as:

$$D_{a_1}^{(i)}, \dots, {}_{a_i} f(x) = D_{a_i}(D_{a_i}^{(i-1)}, \dots, {}_{a_{(i-1)}} f(x)) \quad .(3)$$

where the first derivative at point a, $D_a^{(1)}$ (or D_a for simplicity) is defined by $f(x + a) - f(x)$, with:

$$t_1 - t_2 = t_1 + t_2^{-1}, t_1, t_2 \in T \quad .(4)$$

the 0-th derivative is f(x) itself, and the first-order derivative is simply the difference in differential cryptanalysis [14]

2.2.2. Truncated differential cryptanalysis

Truncated differential cryptanalysis is also used as cryptanalysis in block ciphers. It is one of the differential cryptanalyses and had successfully used against some ciphers. The truncated cryptanalysis traces the propagation of truncated differences during the cipher's rounds. it finds the truncated differential trail with a high sufficient probability p during R rounds. It also has three roles to truncate the differences to perform efficient truncation. Many attacks based on this type of cryptanalysis and many of them had been modified to enhance their performance to recover the key of the block ciphers faster [15].

2.2.3. Impossible differential cryptanalysis

Impossible differential cryptanalysis is a type of differential cryptanalysis. It constructs a differential path with probability (zero) (known as impossible differentials) that eliminates all false predicted keys until the correct key is retrieved. Firstly, the attacker constructs two truncated differentials with probability one from both plaintext and ciphertext directions. The two differentials contradict each other in the middle, then are combined into an impossible differential. Adding more rounds after and/or before this distinguisher, the attacker constructs the attack path. Next, both plain and cipher texts are selected. The round subkeys are guessed [16].

2.2.4. Boomerang attack

Boomerang attack is one of the differential attacks. It was firstly proposed in 1999. This attack includes adaptive chosen plain and cipher texts that are used in attack. The boomerang attack is an effective because it uses two independent differential characteristics .A and B, during less number of rounds with high probability. They can be used as boomerang differential characteristics, if the probability of two independent differential characteristics, P r[A] . P r[B], is greater than 2−i/2 where i is the input length. They can also be used to find the correct quartet when it is found, the boomerang differential characteristic is known as boomerang distinguisher which may lead to key recovery [17].

As a classical boomerang attack can be illustrated in a cipher E consisted of two sub_ciphers E0 and E1, which:

$$E = E_1 \circ E_0 \quad .(5)$$

Boomerang attacks work formed a quartet structure depending on a differential a → d for E_0 of p probability and a differential c → b for E_1 of q probability as in following:

$$Pr[\,E^{-1}(E(x) \oplus b) \oplus E^{-1}(E(x \oplus a) \oplus b) = a] = p^2q^2 \quad .(6)$$

The attack on plain_text performed by using a distinguisher with a data complexity according to both (p, q) form selected plain_texts [18].

3. Differential Characteristics and DDT

In order to perform a differential attack on a given block cipher, the attacker seeks for every possible extracted feature from both the plain and the cipher texts. These features are known as Differential characteristics that describe the relations between the plain_text and the ciphered_text. The differences between both of the inputs and the outputs of any given structure of S.Boxes represented a relation between the set of the input bits and the set of the output bits after each substitution. The attackers examine the differential (Δin, Δout) for each S.Box, where:

$$\Delta y = S(x \oplus \Delta x) \oplus S(x) \quad .(7)$$

Based on (7), the resulted differences can be arranged on a table that the columns represent the inputs and the rows represent the outputs. The resulted table known as differential distribution table DTT. Thus, it includes the full characteristics that allows to calculate the probability of the occurrences of the informative plain and ciphered texts that may produce the encryption key. Table.1 showed the DDT for a given cipher with known design of the S.Boxes. The columns represent the inputs and the rows represent the outputs. The values of the table represent the occurrences results and the differential characteristics of the given cipher. The probability *p* of each S.Box is calculated by:

$$p = \frac{current\ occurance}{\max occurance} \quad .(8)$$

The largest value in the table is used to calculate the probability of the expected keys that used in the encryption which is the key recovery process. Thus, the DDT used to either recovering the encryption keys or to describe the capability of the block cipher to face the differential attacks by trying to reduce the values of probability that shown in table.2[19].

Technium Vol. 4, No.10 pp.15-30 (2022)
ISSN: 2668-778X
www.techniumscience.com

Table 1. DDT

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(0)	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S(1)	0	0	0	2	0	2	2	2	0	0	0	2	0	0	4	0
S(2)	0	0	0	0	0	0	0	0	0	2	2	0	2	2	2	4
S(3)	0	2	2	2	0	0	0	2	0	4	0	2	4	0	0	0
S(4)	0	0	0	0	0	0	0	0	0	4	4	0	2	4	4	0
S(5)	0	0	2	0	4	2	0	0	2	0	2	2	0	0	2	0
S(6)	0	2	2	4	0	2	2	4	0	0	0	0	0	0	0	0
S(7)	0	0	2	0	4	2	0	0	2	2	0	2	0	2	0	0
S(8)	0	0	0	2	0	2	2	2	0	0	0	2	0	4	0	0
S(9)	0	2	2	0	0	2	2	0	0	2	2	0	2	2	2	0
S(10)	0	2	2	2	0	0	0	2	0	0	4	2	0	0	0	0
S(11)	0	2	2	0	0	2	2	0	0	0	0	0	2	0	0	4
S(12)	0	2	0	0	4	0	2	0	2	2	0	2	4	2	0	0
S(13)	0	0	0	4	0	0	0	4	4	0	0	0	0	0	0	4
S(14)	0	2	0	0	4	0	2	0	2	0	2	2	0	0	2	0
S(15)	0	2	2	0	0	2	2	0	4	0	0	0	0	0	0	4

Despite the first row and column, the max value of occurrence is 4. The probability of the all S.Boxes are illustrated in table 2.

Table 2. Probability

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(0)	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S(1)	0	0	0	0.125	0	0.125	0.125	0.125	0	0	0	0.125	0	0	0.25	0
S(2)	0	0	0	0	0	0	0	0	0	0.125	0.125	0	0.125	0.125	0.125	0.25
S(3)	0	0.125	0.125	0.125	0	0	0	0.125	0	0.25	0	0.125	0.25	0	0	0
S(4)	0	0	0	0	0	0	0	0	0	0.25	0.25	0	0.125	0.25	0.25	0
S(5)	0	0	0.125	0	0.25	0.125	0	0	0.125	0	0.125	0.125	0	0	0.125	0
0.125	0	0.125	0.125	0.25	0	0.125	0.125	0.25	0	0	0	0	0	0	0	0
S(7)	0	0	0.125	0	0.25	0.125	0	0	0.125	0.125	0	0.125	0	0.125	0	0
S(8)	0	0	0	0.125	0	0.125	0.125	0.125	0	0	0	0.125	0	0.25	0	0
S(9)	0	0.125	0.125	0	0	0.125	0.125	0	0	0.125	0.125	0	0.125	0.125	0.125	0
S(10)	0	0.125	0.125	0.125	0	0	0	0.125	0	0	0.25	0.125	0	0	0	0

S(11)	0	0.125	0.125	0	0	0.125	0.125	0	0	0	0	0	0.125	0	0	0.25
S(12)	0	0.125	0	0	0.25	0	0.125	0	0.125	0.125	0	0.125	0.25	0.125	0	0
S(13)	0	0	0	0.25	0	0	0	0.25	0.25	0	0	0	0	0	0	0.25
S(14)	0	0.125	0	0	0.25	0	0.125	0	0.125	0	0.125	0.125	0	0	0.125	0
S(15)	0	0.125	0.125	0	0	0.125	0.125	0	0.25	0	0	0	0	0	0	0.25

In table.2, the occurrence 4 had probability of (0.25). thus the corresponding input and output may recover the expected encryption key of the block cipher [20].

4. DTT based works

This section illustrates the recently proposed papers that either presented attacks on block cipher or implement differential cryptanalysis to improve a presented encryption algorithm. The following papers had been published in the last five years.

In[21], the author presented a process to determine both differential and linear characteristics of two light block cipher families (SIMON and SPECK). These characteristics can be modified in order to enhance the complexity or fasten cipher of these two families. DDT is implemented to identify the differential characteristics and calculate probability of the cipher families. The results showed that the proposed process is efficient in improve the robust of the cipher families toward both linear and differential attacks.

In [22], the authors presented differential cryptanalysis for SKINY cipher. They built DDT table and used MILP to determine the active S.boxes in differential rounds. The differential characteristics showed that the SKINY 64/192 is secured is safe with using proposed method with reduced characteristics after 11-rounds.

In [23], the authors presented an evaluation probability of characteristics extracted from Cypress 256's design. The idea of evaluation arises on nine rounds. In the 1st round the DDT is created from the characteristics of the cipher. The highest probabilities equal ¼ is obtained. Then the rest rounds are based on reasonable required less probabilities. Without the highest probabilities, the characteristics would form he size PDDT with the fast algorithm. The results showed the proposed methods is more accurate than hamming weight in determine the proper probabilities.

In [24], the authors implemented the probability of partial DDT (PDDT) with Nested Monte-Carlo to find the reasonable path and evaluate the performance of ARX and LEA ciphers. Their idea based on dividing the long DDT characteristics to short term PDDT that reduces the search space. Starting from the middle of rounds reduced the its required number. The results showed that implementing PDDT can reduce the search space after 9 rounds for both ciphers.

In [25], the authors analyzed the differential path of SPECK cipher by the differential characteristics of PDDT. Then they determine the round number that they attacked. The selected round has differential characteristics greater than or equal to a pre-defined threshold. Decreasing threshold increases the search space of the cipher. Nested Monte Carlo Search (NMCS) is implemented as heuristic based random sampling method, to find out the shortest paths of the cipher. The authors reduced rounds to 9,10,12,13 and 15 for SPECK32, SPECK48, SPECK64, SPECK96 and SPECK128.

In[26], the authors proposed a cryptanalysis method to evaluate the performance of GIFT cipher family with different block sizes. The DDT is implemented to extract the probability of the GIFT64 and GIFT128 then analyzed by MILP. The proposed method improved key recovery process better than other cryptoanalysis methods.

In[27], the authors presented a cryptanalysis method to determine the minimum number of rounds for the block ciphers. The method based on differences between the inputs and the outputs by DDT. The method aims to check the number of rounds in which the proposed method cannot recover they key using MILP. The results showed that the proposed method enhanced the selection of the minimum required number of rounds.

In [28], the authors presented a hybrid type of attack. It is based on both types (Differential and linear attacks. The proposed attack separated the original cipher E into two sub-ciphers E_0 and E_1. The significant dependency between the two sub-ciphers is the main idea in which, Differential-Linear Connectivity Table (DLCT) I sused to choose the differential characteristics E_0 and linear approximation in E_1 by the Fast Fourier Transform. the proposed attack implemented on ICEPOLE and 8-round DES. The proposed attack had been improved by using DLCT with DDT.

In [29], the authors evaluate the performance of GIFT cipher using boomerang and rectangle attacksto recover both single and related keys. DDT was essentially used to determine the probability from the extracted characteristics of the cipher. The results showed the enhance complexity and increased rounds number of both attacks reduced the number of guessed keys for both types of attacks with two type of GIFT cipher.

In [30], the author had implemented the DDT to understand the bit of S.box and extract differences of the sponge structure of Spook cipher with Shadow-512 premutation. These differences are used to obtain distinguisher by using the impossible attack. The result showed that the extracted characteristics helped to find the nonrandom behavior of the Shadow-512 till 8-rounds.

In [31], the author presented a differential cryptanalysis for the PRESENT cipher based on differential characteristics of the design of S.box structure. The author proposed a dynamic S.box design evaluated by implementation DDT and Active S.boxes of PRESENT structure. The study aimed to enhance the robustness of the cipher against differential attack. The results showed that increasing number of the Active S.Boxes increases the robustness of the dynamic design of PRESNT cipher.

In [32], the authors presented a Deep learning model based on differential characteristics to obtain proper distinguishers of HIGHT, LEA, and SPARX as members of ARX ciphers family. A DNN based

model implement a DDT of the differential characteristics at the model training stage. While, another new DDT are implemented in classification stage. The goal of the model to reduce the round numbers of the targeted ciphers. The result showed that the model reduced HIGHT cipher to 14-round, LEA to 13-Round and SPARX to 11-round.

In[33], the authors presented a method to find all impossible differentials for the light wight block ciphers by implementing DDT. The basic idea of the method is to find the differences in between the inputs and outputs of a given SPN-based block cipher with 64bit of block size. The differential pairs were divided into small groups that produced a possible-differentials set by implementing Mixed-Integer Linear Programming (MILP) model. The search space was decreased by eliminating the groups without impossible differentials. The proposed method had been implemented on SKINY64. The results showed that proposed method had high performance and SKINY64 has no extinguisher. For ciphers with large block size like CRAFT and GIFT, the proposed method has good performance too.

In [34], the authors presented several differential attacks based on statistical analysis with implementing the Gold, the inverse, and the Bracken-Leander as vectorial functions. DDT was implemented as one of these differential attacks that had been used with inverse and gold vectorial functions in order to be compared with other statistical attacks with the same functions. The study aimed to facilitate the boomerang attack and block cipher extinguisher.

In [35], the authors presented a developed S.box design for a block cipher based on differential cryptanalysis. Their idea based on both bitslice-friendly ciphers and bit-permutation ciphers. The proposed design aimed to: a) extend the generalized Feistel networks (EGFN) and its Lilliput that contained Xor layer, b) focus on the chains in matrix of the differences to detect the higher probability differences. The proposed design decreases similar state S.box to enhance the robustness of the block ciphers. The design applied to AES, Lilliput, Midori, and SKINNY block ciphers. The result showed that the level of security increase for AES like ciphers with short chains and effective with the other ciphers.

In [36], the authors presented a differential cryptanalysis to recover the key and the randomness in ultra-low latency cipher (K-Cipher). They achieved attack with the complexity of $2^{29.7}$ for different types of K-Ciphers. The attack consisted of three phases. Each phase is an attack on different parameter of the cipher. Both of DDT and gradient GDDT had been implemented to create the characteristics of the cipher. The result showed that both of the secret key and secret randomizer values had been recovered in 30 minutes for 240 bits using standard desktop machine.

In [37], authors proposed an enhancement for the ANU-II which is also is an ultra-lightweight block cipher. It is a type of cipher that are used in devices with limited resources. MILP is implemented to identify the characteristics of the cipher from the probable differential propagation listed in DDT. The extracted characteristics proved that the standard ANU-II cipher is not safe and need to be modified to face the attacks based on these characteristics. The secret key can be recover using just few pairs of plaintext and $2^{62.4}$ full-round encryptions.

In [38]. The author had implemented DDT to extract the characteristics of WARP cipher in order to build an effective distinguisher. The implemented characteristics provide the capability to recover secret key using 20 boomerang attack based on high probability.

In [39], the authors proposed a Differential Cryptanalysis to recover BORON80/128 block cipher. The DDT had been implemented to produce the characteristics of the ciphers in this category. Nonzero characteristics with high probabilities and active S.boxes. these characteristics provide secret key recover in 9 rounds for BORON 80 and 10 rounds for BORON128.

In [40], the authors evaluated the robustness of the μ^2 light weight block cipher by using impossible attack. The DDT was implemented to calculate the probability of the differential characteristics of the cipher. The highest probable differences were used with Miss-in-the-Middle (MitM) technique to determine the distinguishers. These characteristics showed that the cipher's rounds number can not be reduced less than Ten.

5. Comparison and discussion

The previously illustrated works had a set of common features that explain the advantages of DDT implementation with other function to achieve the goals of those studies. Table.3 showed those common features.

Paper #	Cipher Algorithms	Block Size	Other feature	Strategy	Advantages
[21]	SIMON SPECK	32, 48, 64, 96 or 128 32, 48, 64, 96 or 128	Probability	- Analyze the linear and differential characteristics - Improve the ciphers	Enhance the robustness of the two block ciphers families.
[22]	SKINY	64 – 192	Probability Active S.boxes MILP	Determine the safer number of differential rounds	11-rounds makes SKINY safe.
[23]	Cypress256	256	Partial probability Fast algorithm	Analyze the characteristics of the cipher	The proposed method is more accurate than hamming weight
[24]	LEA ARX	128 64	Partial probability	Find reasonable path	Reduces the search space.
[25]	SPECK32 SPECK48 SPECK64	32, 48, 64, 96, 128	Partial probability	Find Shortest path	Reduces the rounds of the cipher with

	SPECK96 SPECK128		Nested Monte Carlo Search		different block sizes.
[26]	GIFT64 GIFT128	64 128	Probability MILP	Differential attack to recover key	Enhance the differential attack.
[27]	ICEPOLE 8-round DES	128 64	Probability DLCT Fast Fourier Transform	Improve block ciphers	Efficient implementation of DDT with DLCT
[28]	Type-3 Fiestal Cipher	Represented with a number of 4bits s.boxes	Probability MILP	Determine the minimum number of required rounds	Reduction of the required rounds
[29]	GIFT64 GIFT128	64 128	Probability	Evaluates the GIFT60/128. Improves impossible and rectangle attacks	Increased rounds number of both attack to 25 in order to reduce the guessed key number.
[30]	Spook	1 to the length of the plaintext	Probability Impossible Attack Shadow-512	Examines the randomness of Spook with Shadow-512	Non randomness behavior of Shadow-512 till 8-rounds
[31]	PRESENT	64, 80, 128	Probability Dynamic S.box structure Active S.Boxes	Modify S.box structure of the PRESENT Cipher based on Differential characteristics	The robustness of PRESENT cipher increased against Differential attack
[32]	HIGHT LEA SPARX	64 128 64, 128	Probability DNN	Build proper distinguishers Reduce rounds	Reduced number of rounds for all ciphers
[33]	SKINY64 CRAFT GIFT64 Rijndael-192 GIFT-128	64 64 64 192 128	MILP	Detect Impossible Differential by MILP model.	Prove that the cipher has no distinguisher

[34]	Feistel structure ciphers	Not included	Inverse Bracken-Leander Gold	Facilitate Boomerang attack	Enhance Boomerang attack and build proper distinguishers.
[35]	AES Lilliput Midori SKINNY	128 64 64, 128 64, 128	Probability Chains of differences	Reduce high probable chains	Enhanced the AES like cipher with short chains
[36]	K-Cipher	24	Probability Active S.boxes	Recover The parameter of K-cipher	Recovered key with 240bit in 30min.
[37]	ANU-II	64	Probability MILP	Key recovery	Recovered Key and suggest to modify the cipher structure
[38]	WARP	128	Probability Single and related-key	Key recovery	Effective distinguisher
[39]	BORON80 BORON 128	64	Probability Active S.boxes	Key recovery	Recovered key with 9 to 10 rounds
[40]	µ2	64	Probability Miss in the Middle	Reduce the rounds number	Less than 10 rounds cannot resist Impossible attack

The previous table showed the common features of DDT implementation accompanied with other algorithms in order to: a) improve the robustness of the block ciphers against attacks, b) build extinguishers and reduce the round number of the block cipher, c) propose new ciphers, d) develop recently presented attacks or propose new attacks. e) enhance the efficiency of the ciphers.

The DDT provide a set of differential characteristics that allow designers to improve the robustness of their ciphers by modify the S.box structure or increase the number of rounds. the provided characteristics showed the shortest paths and active S.Boxes that may advise the designers to modify their design.

DDT implementation with functions or Deep learning models may facilitate creating proper extinguishers. This would allow to check the robustness of the cipher and the probability of key recovery. It also allows to reduce the rounds of the ciphers till the safe limit.

The provided characteristics by DDT are the base of the cipher design. By which, the designer can expect the robustness of their new ciphers and the required number of rounds. it also can be used to reassess the specification of the modified designs. This implementation increases the compatibility of the new cipher with the international standards.

The expected probabilities of the differences in the block cipher can be used to improve the presented attacks or design new attacks. because the designers depended on the all probabilities produced by the S. Box structure of the block cipher that may be used to enhance the selection of the proper characteristics in attack's design.

The block ciphers efficiency is important to be achieved. Thus, the reduction of the rounds number decreases the required time of encryption process. It also reduces the computational cost by executing less operations on the plain text. But the safety level of the cipher against both linear and differential attacks must be maintained to achieve the efficiency of cipher.

Even in big block size, the PDDT had a great role in providing the partial differential characteristics for big block size of cipher such ARX ciphers family. It showed high efficiency in achieving the purpose behind its implementation.

6. Conclusions

DDT is on of the most important tools that commonly used in design, enhance and attack block ciphers. Many papers had been presented that implement DDT or either PDDT to achieve different goals. The comparison of these implementations showed that DDT or PDDT are very efficient tools that can be used to enhance the encryption algorithms or attack the block ciphers.

DDT or PDDT can be used accompanied with other functions and models to build or modify the differential attacks and build extinguishers that can recover the secret keys and randomness of the ciphers. Thus, it is effective tool to build ciphers and broke them.

It is expected to improve the differential attacks and their techniques that based on DDT. It may threaten previously and new presented block ciphers specially with accompanied Deep learning models.

References

[1] Jameel, Enas Ali, and Sameera Abbas Fadhel. "Digital Image Encryption Techniques: Article Review." Technium Vol. 4, Issue 2 pp.24-35 (2022).

[2] Ezadeen, Shamil, and Auday H. Alwattar. "Survey of Blowfish Algorithm for Cloud." Technium Vol. 4, Issue 6 pp.18-28 (2022).

[3] Wang, Fan, et al. "Resolution Adaptative Network for Cryptanalysis of Asymmetric Cryptosystems." IEEE Access 8 (2020): 187419-187430.

[4] Lee, Ting Rong, et al. "Lightweight Block Cipher Security Evaluation Based on Machine

Learning Classifiers and Active S-Boxes." IEEE Access 9 (2021): 134052-134064.

[5] Zhu, Congxu, Guojun Wang, and Kehui Sun. "Improved cryptanalysis and enhancements of an image encryption scheme using combined 1D chaotic maps." Entropy 20.11 (2018): 843.

[6] Bagane, Pooja Anil, and Sirbi Kotrappa. "Bibliometric Survey for Cryptanalysis of Block Ciphers towards Cyber Security." Library Philosophy and Practice (2020): 1-18.

[7] Guo, Hao, et al. "Differential attacks on CRAFT exploiting the involutory s-boxes and tweak additions." Cryptology ePrint Archive (2020).

[8] Sehrawat, Deepti, and Nasib Singh Gill. "Lightweight block ciphers for IoT based applications: a review." International Journal of Applied Engineering Research 13.5 (2018): 2258-2270.

[9] Dey, Sankhanil, and Ranjan Ghosh. "A review of existing 4-bit crypto S-Box cryptanalysis techniques and two new techniques with 4-bit boolean functions for cryptanalysis of 4-bit crypto S-Boxes." Advances in Pure Mathematics 8.03 (2018): 272.

[10] Tentu, Appala Naidu. "A Review on Evolution of Symmetric Key Block Ciphers and Their Applications." IETE Journal of Education 61.1 (2020): 34-46.

[11] Mariano, Artur. "LUSA: the HPC library for lattice-based cryptanalysis." Cryptology ePrint Archive (2020).

[12] Coggia, Daniel. Techniques of cryptanalysis for symmetric-key primitives. Diss. Sorbonne Université, 2021.

[13] Ankele, Ralph, and Stefan Kölbl. "Mind the gap-A closer look at the security of block ciphers against differential cryptanalysis." International Conference on Selected Areas in Cryptography. Springer, Cham, 2018.

[14] Liu, Yunwen. "Techniques for Block Cipher Cryptanalysis.", Dissertation doctoral, Arenberg Doctoral School,

Faculty of Engineering Science (2018).

[15] Biryukov, Alex, et al. "Automated truncation of differential trails and trail clustering in ARX." International Conference on Selected Areas in Cryptography. Springer, Cham, 2022.

[16] Liu, Ya, et al. "Improved impossible differential cryptanalysis of large-block Rijndael." Science China Information Sciences 62.3 (2019): 1-14.

[17] Hutahaean, I. W., A. A. Lestari, and B. H. Susanti. "A tutorial of boomerang attack on SMALLPRESENT-[4]." Journal of Physics: Conference Series. Vol. 1836. No. 1. IOP Publishing, 2021.

[18] Boura, Christina, and Anne Canteaut. "On the boomerang uniformity of cryptographic sboxes." IACR Transactions on Symmetric Cryptology (2018): 290-310.

[19] Kousalya, R. "Security Analysis against Differential Cryptanalysis using Active S-Boxes." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.13 (2021): 701-709.

[20] Survanto, Yohan, and Muhammad Salman. "6 Round Improbable Differential Characteristic on M-PRESENT Using Undisturbed Bits." 2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS). IEEE, 2019.

[21] Dehnavi, S. (2018). Further Observations on SIMON and SPECK Block Cipher Families.

Cryptography, 3(1), 1. doi:10.3390/cryptography3010001

[22] Zhang, P., & Zhang, W. (2018). Differential cryptanalysis on block cipher skinny with MILP program. Security and Communication Networks, 2018.

[23] Rodinko, M., & Oliynykov, R. (2018). An Approach to Search for Multi-Round Differential Characteristics of Cypress-256. 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). https://doi.org/10.1109/infocommst.2018.8631904

[24] Dwivedi, A. D., & Srivastava, G. (2018). Differential cryptanalysis of round-reduced LEA. IEEE Access, 6, 79105-79113.

[25] Dwivedi, A. D., Morawiecki, P., & Srivastava, G. (2019). Differential cryptanalysis of round-reduced speck suitable for internet of things devices. IEEE Access, 7, 16476-16486.

[26] Cao, M., & Zhang, W. (2019). Related-key differential cryptanalysis of the reduced-round block cipher GIFT. IEEE Access, 7, 175769-175778.

[27] Chatterjee, S., Nath Saha, H., Kar, A., Banerjee, A., Mukherjee, A., & Syamal, S. (2019). Generalised Differential Cryptanalysis Check for Block Ciphers. 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). doi:10.1109/iemcon.2019.8936149

[28] Bar-On, A., Dunkelman, O., Keller, N., & Weizman, A. (2019, May). DLCT: a new tool for differential-linear cryptanalysis. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 313-342). Springer, Cham.

[29] Ji, F., Zhang, W., Zhou, C., & Ding, T. (2020, October). Improved (related-key) differential cryptanalysis on GIFT. In International Conference on Selected Areas in Cryptography (pp. 198-228). Springer, Cham.

[30] Bolel, O. (2021). Impossible and improbable differential cryptanalysis of Spook algorithm (Master's thesis, Middle East Technical University).

[31] Kousalya, R. (2021). Security Analysis against Differential Cryptanalysis using Active S-Boxes. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(13), 701-709.

[32] Pal, D., Mandal, U., Chaudhury, M., Das, A., & Chowdhury, D. R. (2022). A Deep Neural Differential Distinguisher for ARX based Block Cipher. Cryptology ePrint Archive.

[33] Hu, K., Peyrin, T., & Wang, M. (2022). Finding All Impossible Differentials When Considering the DDT. Cryptology ePrint Archive.

[34] Eddahmani, S., & Mesnager, S. (2022). Explicit values of the DDT, the BCT, the FBCT, and the FBDT of the inverse, the gold, and the Bracken-Leander S-boxes. Cryptography and Communications, 1-44.

[35] Todo, Y., & Sasaki, Y. (2022). Designing S-Boxes Providing Stronger Security Against Differential Cryptanalysis for Ciphers Using Byte-Wise XOR. In International Conference on Selected Areas in Cryptography (pp. 179-199). Springer, Cham.

[36] Mahzoun, M., Kraleva, L., Posteuca, R., & Ashur, T. (2022). Differential Cryptanalysis of K-Cipher. Cryptology ePrint Archive.

[37] Fan, T., Li, L., Wei, Y., & Pasalic, E. (2022). Differential cryptanalysis of full-round ANU-II ultra-lightweight block cipher. International Journal of Distributed Sensor Networks, 18(9), 15501329221119398.

[38] Teh, J. S., & Biryukov, A. (2022). Differential cryptanalysis of WARP. Journal of Information Security and Applications, 70, 103316.

[39] Teh, J. S., Tham, L. J., Jamil, N., & Yap, W. S. (2022). New differential cryptanalysis results for the lightweight block cipher BORON. Journal of Information Security and Applications, 66, 103129.

[40] Zhang, K., Lai, X., Guan, J., & Hu, B. (2022). Research on the Security Level of μ 2 against Impossible Differential cryptanalysis. KSII Transactions on Internet and Information Systems (TIIS), 16(3), 972-985.