

Full-round differential attack on DoT block cipher

Manoj Kumar

Scientific Analysis Group

Defence Research and Development Organisation

Metcalfe House Complex

Delhi 110054

India

Abstract

Lightweight block cipher DoT was proposed by Patil, Bansod and Kumar in 2019. It is based on the substitution permutation network (SPN) structure. Its block and key size are 64 bits and 128 bits respectively. In this paper, we analyse the security of DoT against differential attack. We construct differential characteristics for 2 rounds and 6 rounds with probability of 2^{-4} and 2^{-12} respectively. These characteristics are used to construct the full-round differential distinguishers for DoT with probability of 2^{-62} . The diffusion layer of DoT is a combination of byte shuffling, 8-bit permutation (P_8), 32-bit word shuffling and circular shift operations. We analyse the differential attack resistance of DoT without P_8 which proves that its application weakens the differential attack resistance of DoT.

Subject Classification: 94A60.

Keywords: Block cipher, Lightweight block cipher, Differential cryptanalysis, Branch-and-bound algorithm.

1. Introduction

Lightweight cryptography has evolved to provide a secure automatic connection between humans and machines through advanced technologies. Lightweight block ciphers are used to secure these applications e.g. RFID tags, wireless sensor nodes and Internet of Things [14] [15]. Memory and throughput requirements are considered as important design parameters for these applications [3] [6]. DoT is claimed to be a compact and smallest

cipher which is presented as a significant option for low power and compact memory applications [13].

Block cipher designs are either based on Feistel or Substitution Permutation Network (SPN) structure [2] [4]. Round function in each structure is designed to satisfy the confusion and diffusion properties. DoT is based on SPN structure that processes the full input block through its round function in each round. It applies single 4-bit S-box sixteen times in parallel but its diffusion layer is a combination of bit/byte permutation and circular shift operations. S-box is used to provide the confusion and diffusion is achieved by combining the bit/byte/word permutations [10]. We analyse the security of DoT against differential attacks and present a distinguisher for full rounds. We also analyse the diffusion layer of DoT and report our results in this paper.

Differential cryptanalysis was proposed by Biham and Shamir in 1992 [1]. This was the first successful cryptanalytic attempt which reduced the complexity of DES beyond exhaustive search. This attack is considered as the basic cryptanalysis method and it is necessary to provide the security proofs against differential attack for new design proposals [8] [9]. A successful differential attack depends on the existence of high probability characteristics covering the maximum rounds of the cipher. We apply branch-and-bound based algorithm [7] to search the optimal differential characteristics in DoT and present several characteristics for 31 rounds with one active S-box in each round.

Rest part of the paper is organised in the following way. In Section 2, we discuss block ciphers DoT and its key expansion algorithm in brief. In Section 3, we apply branch-and-bound based algorithm to search the differential characteristics and present full-round differential distinguisher for DoT. We analyse the security of DoT without 8-bit permutation in Section 4.

Notations: The following notations are used throughout the paper:

- P : 64-bit input plaintext block
- C : 64-bit output ciphertext block
- P_i^{64} : 64-bit input to round function
- K : 128 bits master key
- UK : 128-bit updated key register
- RK_i : 64-bit round subkey

- T_1^{64} : 64-bit temporary block
- T_L^{32} : Left 32-bit block
- T_R^{32} : Right 32-bit block
- T_1^4, T_2^4 : 4-bit temporary nibbles
- $\oplus$: Bitwise exclusive-OR operation
- $\lll n$: Left cyclic shift by n bits
- $\ggg n$: Right cyclic shift by n bits
- $\parallel$: Concatenation of two n -bit strings
- $[i]_2$: Binary value of integer i

2. Lightweight Block Cipher DoT

DoT was published at advances in intelligent systems and computing 2019 [13]. It is claimed as the compact and smallest design for memory requirement and execution time. It consists of a single S-box, shift operations and XOR gates. We provide a brief description of DoT in this section.

2.1 Description

DoT encrypts a 64-bit message block using the 128-bit master key. First, it divides the input plaintext in 64-bit blocks and encrypts each message block to generate a 64-bit ciphertext block. Each input block is processed through the round function 31 times. In each round, there are parallel applications of single 4-bit S-box and it uses nibble/word shuffling, 8-bit permutation and cyclic shift operations.

2.2 Encryption Process

We describe the encryption algorithm using substitution layer S_B , 8-bit permutation P_8 , shuffling of i^{th} byte B_i and circular shift operations (Algorithm 1 and Fig. 1). Round function applies the substitution layer S_B on 64-bit state value $P_i^{64} \oplus RK_i$ by dividing the 64-bit word into 4-bit nibbles. It applies the 4-bit S-box (Table 1) 16 times in parallel on each nibble. After that, 8-bit permutation P_8 is applied on each byte that outputs a 64-bit value T_1^{64} which is divided into eight bytes (Fig. 2). These bytes are rearranged to produce two 32-bit outputs T_L^{32} and T_R^{32} . Finally, left circular shift by 25 bits is applied on T_L^{32} and right circular shift by

31 bits is applied on T_R^{32} and corresponding outputs are concatenated to produce the 64-bit output P_{i+1}^{64} . These operations are applied 31 times to get the 64-bit ciphertext.

Algorithm 1 : Encryption Algorithm

```

1  Input:  $P = P_1^{64}$  and  $RK_i$  obtained from  $K$ 
2  Output:  $C = P_{32}^{64} \oplus RK_{32}$ 
3  for  $i = 1$  to 31 do
4       $T_1^{64} = P_8(S_B(P_i^{64} \oplus RK_i))$ 
5       $T_1^{64} \rightarrow (B_1 \parallel B_2 \parallel B_3 \parallel B_4 \parallel B_5 \parallel B_6 \parallel B_7 \parallel B_8)$ 
6       $T_L^{32} = (B_1 \parallel B_3 \parallel B_5 \parallel B_7)$ 
7       $T_R^{32} = (B_2 \parallel B_4 \parallel B_6 \parallel B_8)$ 
8       $P_{i+1}^{64} = (T_L^{32} \ll 25) \parallel (T_R^{32} \gg 31)$ 
9  end

```

2.3 Key Expansion

In each round, we need 64-bit round subkey (RK_i) which is obtained from the 128-bit master secret key (K) using the key expansion procedure described in Algorithm 2 [13].

Algorithm 2 : Key Expansion Algorithm

```

1  Input: 128-bit master key  $K$ 
2  Output: 64-bit round subkeys  $RK_i$ 
3  for  $i = 1$  to 31 do
4       $RK_i = 64$  leftmost bits of  $K$ 
5       $UK \leftarrow K \lll 13$ 
6       $T_1^4 = (UK \gg 124) \& 0xF$ 
7       $T_2^4 = (UK \gg 120) \& 0xF$ 
8       $K = S(T_1^4) \ll 124 \parallel S(T_2^4) \ll 120 \parallel ((UK \ll 8) \gg 8) \oplus ([i]_2 \ll 59)$ 
9  end

```

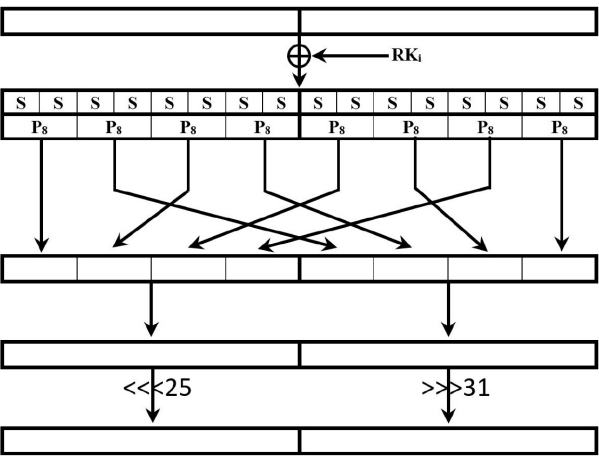


Fig. 1
Round Function of DoT

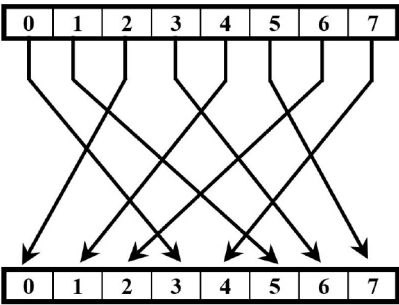


Fig. 2
8-bit Permutation (P_8)

Table 1
S-Box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	3	F	E	1	0	A	5	8	C	4	B	2	9	7	6	D

3. Differential Attack on DoT

We exploit the non-uniform relation between the input & output differences in a differential attack. These relations are constructed for few

rounds and extended further by adding more rounds. High probability differential characteristics are the basis for a successful attack. We need automated tools to compute the high probability characteristics covering the maximum number of rounds. There are various automated methods to construct the optimal differential characteristics e.g. branch-and-bound based algorithm [12]. We use branch-and-bound based algorithm presented by Kumar et al in [11] to construct the differential distinguisher for DoT. We describe the process for searching the differential characteristics in Algorithm 3 which takes n -bit block X as input and nibble (S-box) size is taken as m -bit. The input block X is divided in $t(= n / m)$ nibbles, then Difference distribution table (DDT) is applied on each nibble to get the possible output differences with probability p_i . Any non-zero input to DDT contributes towards the probability of characteristics. We start with one non-zero nibble in the input X and track the propagation of this difference. We also tried with two or more non-zero nibbles in the input X and tracked the difference in same way to find out a differential characteristics with better probability. After trying all possible non-zero values for each nibble, we filter out the characteristics containing least number of active S-boxes and having maximum probability.

Algorithm 3 : Branch-and-bound based algorithm for differential characteristics

```

1  Input:  $X$ , S-box size (bits) =  $m$ ,  $least = A$ ,  $optimal = B$  and  $N_{SB} = 0$ 
2  Output: Optimal Differential Trails with best probability  $P_T$ 
3      for  $i = 1$  to  $t$  do
4          for  $j = 1$  to  $2^m - 1$  do
5               $Nibble_i = j; Nibble_{(\neq i)} = 0;$ 
6               $X = (Nibble_1, Nibble_2, \dots, Nibble_t);$ 
7              for  $Round=1$  to  $r$  do
8                  Count ( $\neq$  Non-zero nibbles in  $X$ );
9                   $N_{SB} = N_{SB} + Count;$ 
10                 for  $k_1 = 1$  to 15 do
11                      $p_1 = DDT[Nibble_1][k_1];$ 
12                     If ( $p_1 = 0$ ) continue;
13                 for  $k_2 = 1$  to 15 do
```

```

14           $p_2 = DDT[Nibble_2][k_2];$ 
15          If ( $p_2 = 0$ ) continue;
16          .....
17          for  $k_t = 1$  to 15 do
18               $p_t = DDT[Nibble_t][k_t];$ 
19              If ( $p_t = 0$ ) continue;
20               $Y = (k_1, k_2, \dots, k_t);$ 
21               $X = P_{Layer}(Y);$ 
22               $P_{Round} = p_1 * p_2 * \dots * p_t$ 
23          end
24      end
25  end
26  end
27       $P_T = P_1 * P_2 * \dots * P_r$ 
28      if  $N_{SB} \leq \text{least}$  and  $P_T \leq \text{optimal}$  then
29          return: Optimal differential characteristics with
                    probability  $P_T$ 
30      end
31  end
32 end

```

3.1 Full-round Differential Distinguisher

DoT applies round key addition, 4-bit S-box, permutation P_8 on 8 bits, word shifts and left/right rotations in each round [13]. Word shift, P_8 and rotations are linear operations that always generates a fixed output difference for a particular input difference. We also get the same difference value $\Delta U = U_1 \oplus U_2$ before and after the add round key operation. However, substitute nibble operation does not provide the fix output difference for any input difference due to its non-linearity. Therefore, we need to construct the probabilistic relations for each input and corresponding output differences to S-box. This is tabulated to get a $2^4 \times 2^4$ difference distribution table (DDT) [5] for 4-bit S-box. For any non-zero input ($\Delta_i \neq 0$), we get more than one non-zero outcomes ($\Delta_o \neq 0$). For DoT S-box, there are 256 possible input and output difference pairs (Δ_i, Δ_o) that are presented in the following table.

Table 2
Difference Distribution Table of DoT

$\Delta_o \rightarrow$																
$\Delta_i \downarrow$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2
2	0	0	2	0	0	2	2	2	0	0	2	0	0	2	2	2
3	0	4	2	0	2	0	0	0	2	0	0	0	0	0	2	4
4	0	0	0	4	0	4	0	0	0	2	0	2	0	2	0	2
5	0	0	0	0	4	0	4	0	0	2	0	2	0	2	0	2
6	0	0	2	0	0	2	2	2	0	2	2	2	0	0	2	0
7	0	4	2	0	2	0	0	0	0	0	2	4	2	0	0	0
8	0	0	0	4	0	4	0	0	0	2	0	2	0	2	0	2
9	0	0	0	4	0	0	0	4	2	0	2	0	2	0	2	0
A	0	0	2	0	0	2	2	2	2	0	0	0	2	2	0	2
B	0	4	2	0	2	0	0	0	0	0	2	0	2	4	0	0
C	0	0	0	0	0	0	0	0	4	0	4	0	4	0	4	0
D	0	0	0	4	4	0	4	4	0	0	0	0	0	0	0	0
E	0	0	2	0	0	2	2	2	2	2	0	2	2	0	0	0
F	0	4	2	0	2	0	0	0	2	4	0	0	0	0	2	0

In Table 2, trivial pair (0,0) appears 16 times and any non-trivial pair (Δ_i, Δ_o) appears 0/2/4 times. We use algorithm 3 to construct the differential characteristics and search for the characteristics covering maximum number of rounds with highest probability. It proceeds by dividing the 64-bit input data into sixteen 4-bit nibbles then it performs the characteristics search for all non-zero values of 4-bit nibble. The characteristics with least number of active S-boxes and highest probability are filtered out to get the optimal differential characteristics.

We constructed the 31-round differential distinguisher by extending the 2-round and 6-round characteristics that produce an output difference equal to the input difference after 2 and 6 rounds respectively. We start with input difference 00000000 00000050 which results in the output difference 00000000 00000008 after first round with probability of 2^{-2} . This difference is the input difference for the second round which generates the difference 00000000 00000050 after 2 rounds with probability of

Table 3
2-Round Differential Characteristics

Round Index	First Characteristic ΔP_i	Second Characteristic ΔP_i
1	00000000 00000050	00000000 00000080
2	00000000 00000008	00000000 0000000c
3	00000000 00000050	00000000 00000080

Table 4
6-Round Differential Characteristics

Round Index	First Characteristic ΔP_i	Second Characteristic ΔP_i
1	00500000 00000000	00000000 00800000
2	00000000 08000000	00000000 00000c00
3	00000050 00000000	80000000 00000000
4	00000000 00080000	000c0000 00000000
5	00000000 00005000	00000000 80000000
6	08000000 00000000	0000000c 00000000
7	00500000 00000000	00000000 00800000

2^{-2} . In this way, we get 2-round characteristics with probability of 2^{-4} . We also constructed several 6-round characteristics with equal values of input and output difference. We constructed total 37 distinct differential distinguishers for full-round DoT by extending these 2-round and 6-round differential characteristics. Some of these differential characteristics for 2 rounds and 6 rounds are presented in Table 3 and Table 4.

We get thirty seven differential characteristics that serves as full-round differential distinguisher for DoT encryption algorithm with probability of 2^{-62} . We compare the lower bound on the number of active S-boxes in any differential characteristics of DoT with the designers bound (Table 5). This shows that our full-round attack requires 2^{62} chosen plaintexts which is better than security claims provided by the designers of DoT. One of the full-round differential distinguisher is presented in Table 6 with 00000004 00000000 as first-round input difference and output difference after 31 rounds as 00000000 00500000 with probability of 2^{-62} .

Table 5
Lower Bounds on number of active S-boxes

Round Index	#Active S-boxes (Designers Bound)	# Active S-boxes (Our Bound)
2	2	1
6	7	6
30	35	30
31	--	31
Ref.	[13]	This Paper

Table 6
Full-Round Differential Characteristic

Round index	Input Difference ΔP_i	#Active S-box	Prob. $(-\log_2 p_i)$	Prob. $(-\Sigma_i \log_2 p_i)$
1	00000004 00000000	1	2	2
2	00000000 00500000	1	2	4
3	00000000 00000800	1	2	6
4	50000000 00000000	1	2	8
5	00080000 00000000	1	2	10
6	00000000 50000000	1	2	12
7	00000008 00000000	1	2	14
8	00000000 00500000	1	2	16
9	00000000 00000800	1	2	18
10	50000000 00000000	1	2	20
11	00080000 00000000	1	2	22
12	00000000 50000000	1	2	24
13	00000008 00000000	1	2	26
14	00000000 00500000	1	2	28
15	00000000 00000800	1	2	30
16	50000000 00000000	1	2	32
17	00080000 00000000	1	2	34
18	00000000 50000000	1	2	36
19	00000008 00000000	1	2	38
20	00000000 00500000	1	2	40

Contd...

21	00000000 00000800	1	2	42
22	50000000 00000000	1	2	44
23	00080000 00000000	1	2	46
24	00000000 50000000	1	2	48
25	00000008 00000000	1	2	50
26	00000000 00500000	1	2	52
27	00000000 00000800	1	2	54
28	50000000 00000000	1	2	56
29	00080000 00000000	1	2	58
30	00000000 50000000	1	2	60
31	00000008 00000000	1	2	62
--	00000000 00500000	-	-	--

4. Analysis of DoT without P_8 layer

We remove the 8-bit permutation operation P_8 used in diffusion layer of DoT and analyse the differential attack resistance of DoT block cipher without P_8 layer. We apply our differential characteristics search algorithm on modified version of DoT and observe that it provides the better security in comparison to the original DoT block cipher. We found that any 10-round differential characteristics of modified DoT have at least 10 active S-boxes with probability of 2^{-25} while 10-round differential characteristics of original DoT have 10 active S-boxes with probability of 2^{-20} . We have extended the 10-round differential characteristics of DoT to 31 rounds and presented a full-round differential distinguisher for original DoT. But, this is not possible in case of DoT without P_8 permutation. Any 30-round differential characteristics of modified DoT have 30 active S-boxes with probability of 2^{-75} . Therefore, it is not possible to construct a full-round differential distinguisher for DoT without P_8 permutation layer.

5. Conclusion

We analysed a lightweight block cipher DoT against differential attack in this paper. Designers have provided a lower bound of 35 on the number of active S-boxes in any 30-round differential trail. We have reduced this bound to 30 active S-boxes in any 30-round trail. We constructed full-round differential characteristics of DoT with probability of 2^{-62} . We presented

37 differential distinguishers with data complexity of 2^{62} which is the best bound for differential attack on DoT till date. We also analysed the differential attack resistance of DoT without using the 8-bit permutation (P_8) in the diffusion layer. This analysis proves that application of P_8 in diffusion layer of DoT does not contribute to the strength of DoT against differential attack.

Acknowledgements

Author would like to thank Ms. Pratibha Yadav and Dr. Sucheta Chakrabarti for their continuous guidance and encouragement to carry out research in this direction.

References

- [1] Biham, E., Shamir, A., Differential Cryptanalysis of the full 16-round DES, CRYPTO 92, LNCS, Vol. 740, pp. 487-496, Springer, 1992.
- [2] Bogdanov, A., Analysis and Design of Block Cipher Constructions, Ph.D. thesis, 2009.
- [3] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C., PRESENT: An Ultra-Lightweight Block Cipher, CHES 2007, LNCS, Vol. 4727, pp. 450-466, Springer, 2007.
- [4] Daemen, J., Rijmen, V., The Design of Rijndael, Springer-Verlag, 2002.
- [5] Hays, H.M., A Tutorial on Linear and Differential Cryptanalysis, Cryptologia, Vol. 26, No. 3, pp. 188-221, 2002.
- [6] Jangra, M., Singh, B., Performance Analysis of CLEFIA and PRESENT Lightweight Block Ciphers, *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 22, Issue 8, pp. 1489-1499, DOI:10.1080/09720529.2019.1695900, 2019.
- [7] Knudsen, L., Robshaw, M.J.B., Block Cipher Companion, Book Springer, ISBN 978-3-642-17341-7, 2011.
- [8] Kumar, M., Design and Analysis of Symmetric Cryptographic Primitives, Ph.D. thesis, 2019.
- [9] Kumar, M., Pal, S.K., Panigrahi, A., FeW : A Lightweight Block Cipher, *Turkish Journal of Mathematics and Computer Science*, Vol. 11, No. 2, pp. 58-73, 2019.

- [10] Kumar, M., Yadav, P., Pal, S.K., Panigrahi, A., Secure and Efficient Diffusion Layers for Block Ciphers, *Journal of Applied Computer Science and Mathematics*, Vol. 11, Issue 2, pp. 15-20, 2017.
- [11] Kumar, M., Suresh, T. S., Pal, S.K., Panigrahi, A., Optimal Differential Trails in Lightweight Block Ciphers ANU and PICO, *Cryptologia*, Vol. 44, Issue 1, pp. 68-78, DOI:10.1080/01611194.2019.1650844, 2020.
- [12] Matsui, M., On Correlation between the Order of S-boxes and the Strength of DES, *EUROCRYPT 94*, LNCS, Vol 950, pp. 366-375, Springer, 1994.
- [13] Patil, J., Bansod, G., Kumar, S. K., DoT: A New Ultra-Lightweight SP Network Encryption Design for Resource-Constrained Environment, *Advances in Intelligent Systems and Computing* 828, Springer, pp. 249-257, 2019.
- [14] Poschmann, A.Y., Lightweight Cryptography: Cryptographic Engineering for a Pervasive World, Ph.D. thesis, 2009.
- [15] Shahapure, S., Sule, V., Daruwala, R.D., Variation and Security Enhancement of Block Ciphers by Embedding, *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 22, Issue 2, pp. 151-160, DOI:10.1080/09720529.2019.1576336, 2019.

Received January, 2021

Revised May, 2021