Security Margin of 5-Round DEAL

Orhun Kara

***Abstract*—DEAL is a block cipher designed by L. Knudsen. It is a Feistel network with 128-bit block and 128-bit, 192-bit and 256-bit keys. The round function of DEAL is DES encryption and the number of rounds is six for 128 and 192 bit key lengths. Knudsen claimed that the 6-round DEAL and the 5-round DEAL provide 121 bit and 88 bit securities respectively. In this paper, we mount a reflection attack to 5-round DEAL with a time complexity of 2^{72} encryptions for 128-bit key length. The attack works approximately 2^{72} keys. We need 2^{65} chosen plaintexts the identify if a key is weak. The attack is mounted only if the key is weak. We have derived a 3-round distinguisher to mount the attack.**

***Index Terms*—block cipher, self similarity, reflection attack, DEAL, weak key**

I. Introduction

DEAL is a block cipher designed by L. Knudsen. It is a Feistel network with a block length of 128-bit and key lengths of 128-bit, 192-bit and 256-bit. The round function of DEAL is DES encryption and the number of rounds is six for 128 and 192 bit key lengths. Knudsen claimed that the 6-round DEAL and the 5-round DEAL provide 121 bit and 88 bit securities respectively [13].

In this paper, we mount a reflection attack on 5-round DEAL to show that 5-round DEAL provides 72 bit security for some keys. The reflection attack on DEAL is given in [10]. While the attack was successful for 6-round DEAL-192 and 8-round DEAL-256, it failed for 6-round DEAL-128 due to the very few number of weak keys in the 128- bit version. Indeed, the attack has been exploited the 5-round distinguisher which imposes too many conditions on round keys. Hence, the cost of the identification step goes far beyond the number of weak keys, rendering the attack unsuccessful.

In this paper, we exploit 3-round distinguisher to increase the number of weak keys dramatically. However, it is not given how to construct a 3-round distinguisher for the classical reflection attack in the original paper, [10]. The statements in [10] are given for the Feistel networks with palindromic round keys where there are at least two pairs of palindromic keys. Hence the reflection attack in [10] works for the ciphers of round numbers more than five and the distinguisher is based on at least 5 rounds. However, we make use of three-round distinguisher to mount an attack on 5-round DEAL. So, we derive a new statement, Theorem 1, which provides a 3-round distinguisher.

We have seen that the probability that one half of the plaintext is equal to one half of the corresponding ciphertext no more deviates from the random pattern. Hence, the conventional reflection attack does not work. However, we derive a new version of the attack by means of Theorem 1 and mounted the attack on 5-round DEAL.

We use 2^{65} chosen plaintexts to identify whether the key is weak. If it is identified as a weak key, then we recover the key with 2^{72} time complexity, using 2^{56} blocks of memory for DEAL-128. The number of weak keys is 2^{72}, which is more then the cost of the identification step.

The paper is organized as follows. We give a brief description of DEAL-128 in the next section. Section III covers the new results on the reflection attack on DEAL. We give the attack on 5-round DEAL in this section. Finally, we conclude the paper with Section VI.

II. Brief Description of DEAL-128

DEAL, submitted to AES contest, is a Feistel network with 128-bit block length [13]. That is, at each round, one half of the input is encrypted by a round function and added to the other half and the result with the half incorporated into the round function together form the output of the round. The round function of DEAL is DES so that the DES encryption chips can be used for DEAL also which provided DEAL an advantage over the other AES contestants for the interoperability.

The key lengths of DEAL are 128-bit, 192-bit and 256-bit. The number of rounds is six for the 128-bit and 192-bit versions whereas it is 8 for the 256-bit version. In this paper we analyze 5-round DEAL for the 128-bit version.

We give the high level description of DEAL-128. The other versions are quite similar. For the 128-bit version, the key, K, is divided into two 64-bit parts as K_0 and K_1. The six round keys, $RD_{K_1}, ..., RD_{K_6}$, are computed by using DES. An 56-bit constant value, s, is used as the DES key to produce the round keys. The round keys are then calculated from the 64-bit raw data given as

$$\begin{aligned}
RD-RAW_{K_1} &= DES_s(K_0)\\
RD-RAW_{K_2} &= DES_s(K_1 \oplus RD_{K_1})\\
RD-RAW_{K_3} &= DES_s(K_0 \oplus RD_{K_2} \oplus strng(1))\\
RD-RAW_{K_4} &= DES_s(K_1 \oplus RD_{K_3} \oplus strng(2))\\
RD-RAW_{K_5} &= DES_s(K_0 \oplus RD_{K_4} \oplus strng(4))\\
RD-RAW_{K_6} &= DES_s(K_1 \oplus RD_{K_5} \oplus strng(8))
\end{aligned}$$

where $strng(i)$ denotes the integer i as the bit string. Only 56 bits of each $RD-RAW_{K_i}$ is used in the i-th round of DEAL, yielding to the round key RD_{K_i}. We remark that the final round ends with a swap unlike conventional use of Feistel networks.

There are some theoretical attacks on DEAL. The attack by Knudsen [13] is a meet-in-the-middle attack which requires 2^{168} encryptions with 2^{173} bytes of memory for 6-round

Manuscript received March 10, 2012.

Orhun Kara is with TÜBİTAK BİLGEM Gebze, 41470 Kocaeli Turkey, e-mail: orhun,@uekae.tubitak.gov.tr

DEAL. On the other hand, the impossible differential attack on DEAL requires 2^{121} DES encryption with 2^{70} chosen plaintexts and 2^{68} bytes of memory, utilizing the impossible differentials of 5 round Feistels with bijective round functions [13]. In [15], Lucks uses similar techniques and mounts chosen ciphertext attack instead of chosen plaintext attack on DEAL so as to gain information from the first round key. In [12], Kelsey and Schneier discuss the existence of equivalent keys and mount a related key attack.

III. Reflection Attack on 5-Round DEAL-128

Define the Feistel structure as $x_i = R_{k_{i-1}}(x_{i-1}) \oplus x_{i-2}$ recursively with the initial conditions given by $x = (x_0, x_1)$. The initial condition $x = (x_0, x_1)$ is the plaintext, the function R is the round function of the Feistel network and $\oplus$ is the "XOR" operation. The i-th round operation is defined as

$$(x_i, x_{i+1}) = (x_i, R_{k_i}(x_i) \oplus x_{i-1}) \tag{1}$$

for $i \leq r$. The final output (x_r, x_{r+1}) is the corresponding ciphertext of the plaintext (x_0, x_1). The stream $x_0, x_1, ..., x_r, x_{r+1}$ is called the encryption stream of (x_0, x_1) with respect to K.

The reflection attack in [10] mounted on 6-round DEAL exploits the palindromic properties of the round keys given as

$$RD_{K_2} = RD_{K_6} \tag{2}$$
$$RD_{K_3} = RD_{K_5} \tag{3}$$

However, all the keys do not produce such palindromic round keys. The probability that these equalities hold is roughly 2^{-112}. When Equations 2 and 3 hold, the last five rounds of DEAL has 2^{64} fixed points (without the final swap). Then one can mount a reflection attack given in [10]. However, this attack is not successful for 128-bit DEAL since the number of weak keys, which are the keys producing the subkeys satisfying Equations 2 and 3, is around 2^{16}. So, identifying a weak key costs much more than the number of weak keys. Remark that the total cost of recovering a weak key among several keys, if exists, consists of the cost of identifying the weak key with the cost of recovering it. Hence, the overall complexity exceeds that of exhaustive search.

One natural extension of the attack is to increase the number of weak keys. This can be done by loosing one of the equalities between subkeys. In this section, we introduce a new reflection attack on 5-round DEAL-128 by imposing only one equality on subkeys. Hence the probability of this condition will raise to 2^{-56}. In this case, the number of weak keys is approximately 2^{72} for 128 bit DEAL. Hence we are able to possess a resource of 2^{72} encryptions for the identification.

Consider the 5-round DEAL-128 by revoking the last round. Assume that

$$RD_{K_2} = RD_{K_4}. \tag{4}$$

This happens with a probability of 2^{-56}. We will have a 3-round reflection for the rounds 2, 3 and 4 in this case. However, we can not use the theorems in Section IV of [10] since the theorems are not valid for a 3-round distinguisher. For instance, it is given in [10] that

$$\Pr(x_0 = x_r) = 2^{-\frac{n}{2}}(2 - 2^{-\frac{n}{2}})$$

which is a distinguisher in order to identify a weak key for the Feistel networks with palindromic subkeys and bijective round functions. Because, $\Pr(x_0 = x_r)$ in the case of a weak key is more than twice as much as $\Pr(x_0 = x_r)$ in random case. The conventional reflection attack given in [10] exploits this distinguisher. However, the probability $\Pr(x_0 = x_r)$ will no more be able to be distinguished from the random case when the number of rounds satisfying the palindromic subkeys is three and the round function is a permutation. Therefore, the attack given in [10] will not work in this case.

We derive another statement to mount a reflection attack on 5-round DEAL-128 where there is a 3-round reflection property.

Theorem 1: Let $(x_0, x_1, x_2, x_3, x_4, x_5)$ be the encryption stream of a 4-round n bit block Feistel network whose round function is a random permutation for any key. Assume $k_1 = k_3$. Then we have

a) $x_0 = x_4$ if and only if $x_1 = x_3$.

b) $\Pr(x_0 = x_4) = 2^{n/2}$ (which is random) and $\Pr(R_{k_2}(x_2) = 0 \,|\, x_0 = x_4) = 1$.

Proof: Consider a Feistel network of 4-round with an encryption stream $(x_0, x_1, x_2, x_3, x_4, x_5)$ where $k_1 = k_3$. Assume $x_0 = x_4$. Then $F_{k_1}(x_1) = F_{k_3}(x_3)$ since $x_0 = F_{k_1}(x_1) \oplus x_2$ and $x_4 = F_{k_3}(x_3) \oplus x_2$. On the other hand, F is a permutation by the assumption. So, $x_1 = x_3$. Assume, on the contrary that $x_1 = x_3$. Then,

$$x_4 = F_{k_3}(x_3) \oplus x_2 = F_{k_3}(x_1) \oplus x_2 = F_{k_1}(x_2) \oplus x_2 = x_0.$$

So, we have proved that $x_0 = x_4$ if and only if there is fixed point for the first three rounds. So, $x_0 = x_4$ implies that $R_{k_2}(x_2) = 0$. This fact is given in [7], [16], [17]. Hence $\Pr(R_{k_2}(x_2) = 0 \,|\, x_0 = x_4) = 1$. On the other hand, $x_0 = x_4$ only if $R_{k_2}(x_2) = 0$. Because $x_0 = x_4$ means (x_0, x_1) is a fixed point and a fixed point occurs only if $R_{k_2}(x_2) = 0$. The probability that $R_{k_2}(x_2) = 0$ is roughly $2^{n/2}$ for a random permutation F. Hence $\Pr(x_0 = x_4) = 2^{n/2}$. ■

Corollary 1: Assume $k_1 = k_3$ for a given 4-round n bit block Feistel network with an encryption stream $(x_0, x_1, x_2, x_3, x_4, x_5)$. Assume also that the round functions are all permutations. The equality $x_0 = x_4$ holds if and only if $x_1 = R_{k_4}(x_4) \oplus x_5$.

Proof: Let $(x_0, x_1, x_2, x_3, x_4, x_5)$ be the encryption stream of a 4-round Feistel network with permutation round functions such that $k_1 = k_3$. Assume that $x_0 = x_4$. Then $x_1 = x_3$ by Theorem 1. On the other hand $x_3 = F_{k_4}(x_4) \oplus x_5$. Hence, $x_1 = F_{k_4}(x_4) \oplus x_5$. Conversely, if $x_1 = R_{k_4}(x_4) \oplus x_5$ then $x_1 = x_3$ and hence $x_0 = x_4$ again by Theorem 1. ■

Let us remark that Corollary 1 states that whenever we have an equality between the right part of the plaintext and the left part of the ciphertext, we have an input-output pair for the last round function. This was not always true when the number of rounds is larger than 4. There was a probability that the equality between the right and the left parts of plaintexts and ciphertexts respectively might happen randomly, not due to a fixed point. In this case, the equality $x_1 = R_{k_r}(x_r) \oplus x_{r+1}$ would most probably be not satisfied.

Corollary 2: Assume $k_1 = k_3$ for a given 4-round n bit block Feistel network. For a given x_1, let $P_{x_1} = \{(x_0, x_1)|x_0 \in GF(2^{n/2})\}$. That is, P_{x_1} is the set of plaintexts whose first halves take all the values and second halves equal to a fixed x_1. Then there is only one element (x_0, x_1) of P_{x_1} such that the right half of the ciphertext of the encryption of (x_0, x_1) is x_0 and the ciphertext is $(x1 \oplus F_{k_4}(x_0), x_0)$.

Proof: Let $P_{x_1} = \{(x_0, x_1)|x_0 \in GF(2^{n/2})\}$. Then the left part of P_{x_1} takes all the possible values. On the other hand $x_2 = F_{k_1}(x_1) \oplus x_0$. Hence, x_2 takes all the values possible exactly once. Going on so, $F_{k_2}(x_2)$ takes all the values exactly once since F_{k_2} is a permutation. Hence there exists only one x_2 such that $F_{k_2}(x_2) = 0$. Let x_0 be the left part of the corresponding plaintext for this x_2. Then (x_0, x_1) is a fixed point by Theorem 1. This means that $x_4 = x_0$ and $x_5 = x1 \oplus F_{k_4}(x_0)$. ■

We are ready to mount a reflection attack on 5-round DEAL (WLOG assume there is no final swap). Let $\alpha \in GF(2^{64})$ be any fixed element. Then encrypt all the plaintexts whose right parts are equal to α. If subkeys satisfy, $RD_{K_2} = RD_{K_4}$ then we expect a three-round reflection for the 2nd, the 3rd and the 4th rounds of DEAL. On the other hand there exits x such that (α, x) is expected to be a fixed point by Theorem 1 and Corollary 2. Hence, we observe α at the right half of the ciphertext. Among all the encryptions of 2^{64} chosen plaintext, α is occurred only once as the right half of a ciphertext. In this case, we are sure that a fixed point occurs by Theorem 1.

On the other hand, store the values $(k, DES_k(\alpha))$ sorted by $DES_k(\alpha)$ when k takes all the values. So there are 2^{56} blocks. This can be considered as the pre-computation phase of the attack since it can be performed at any time, particularly before collecting the real data.

Let (x, α) be the plaintext whose encryption is (y, α). Then we have a fixed point for the intermediate three rounds and hence

$$DES_{k_1}(\alpha) \oplus DES_{k_5}(\alpha) = x \oplus y$$

by Theorem 1. Similarly, choose another value β and encrypt all the plaintexts whose right halves are β. Then we have another equation for β:

$$DES_{k_1}(\beta) \oplus DES_{k_5}(\beta) = x \oplus y$$

where the encryption of (x,β) is (y, β). Solve the equation

$$DES_{k_1}(\alpha) \oplus DES_{k_5}(\alpha) = x \oplus y$$

by guessing k_1 and recovering k_5 from the table $(k, DES_k(\alpha))$ sorted by $DES_k(\alpha)$. There are roughly 2^{48} solutions for (k_1, k_5). On the other hand, these solutions must satisfy the equation deduced by β. The right keys always satisfy the equation. Any arbitrary key pair satisfies the equation with a probability of 2^{-64}. Hence, the probability that there is a wrong key pair satisfying both the equations is approximately 2^{-16}.

If there is no key pair satisfying both equations then our assumption is wrong. That is, we have no equality: $RD_{K_2} \neq RD_{K_4}$. In this case we terminate the attack with 2^{65} chosen plaintexts. If there is a key pair satisfying both equations then we conclude that $RD_{K_1} = k_1$. This gives 56 bit information of the main key. Search the remaining 72 bits of the key exhaustively if the key is identified as a weak key. Let us remark that there may be solutions to (k_1, k_5) for some keys even though $RD_{K_2} \neq RD_{K_4}$ since the probability of finding a solution among 2^{112} subkey candidates is 2^{-16} in this case.

The data complexity of the attack is 2^{65} chosen plaintexts. We need a memory of 2^{56} pairs of the form $(k, DES_k(\alpha))$. Each pair is 15 bytes. At the end we recover the key with 2^{72} time complexity if the key is weak. That is, $RD_{K_2} = RD_{K_4}$. The exhaustive search on 72 bits is done only once at 2^{16} identification steps.

IV. Conclusion

We have analyzed the security margin of 5-round DEAL by means of a self-similarity attack. We have mounted a reflection attack on 5-round DEAL with a time complexity of 2^{72} encryptions if the key is a weak key for DEAL-128. The attack works for approximately 2^{72} keys and we have used 2^{65} chosen plaintexts to identify if the attack works for a given key, before mounting the attack.

We have needed a 3-round distinguisher to mount a reflection attack successfully on 5-round DEAL. However, the reflection attack on Feistel networks given in [10] does not work for a 3-round distinguisher. So, we have derived a new version of the reflection attack for the Feistel networks. This new derivative makes use of 3-round distinguisher and can be successfully mounted on 5-round DEAL faster than the brute force in terms of the overall complexity.

Acknowledgment

We would like to thank the anonymous reviewers for their comments.

References

[1] E. Biham. New Types of Cryptanalytic Attacks Using Related Keys. *J. of Cryptology*, Vol.7, pp.229-246, 1994.

[2] E.Biham, O. Dunkelman and N. Keller. Improved Slide Attacks, In *Proc. FSE'07*, LNCS 4593, pp. 153-166, Springer, 2007.

[3] E.Biham, O. Dunkelman and N. Keller. Related-Key Boomerang and Rectangle Attacks, In *Proc. of EUROCRYPT 2005*, LNCS 3494, pp. 507-525, Springer, 2005.

[4] E.Biham, O. Dunkelman and N. Keller. A Unified Approach to Related-Key Attacks. In *Proc FSE'08*, LNCS 5086, pp73-96, Springer, 2008.

[5] A. Biryukov and D. Wagner. Slide Attacks. In *Proc. FSE'99*, LNCS 1636, pp.245-259, Springer, 1999.

[6] A. Biryukov and D. Wagner. Advanced Slide Attacks. In *Proc. EUROCRYPT 2000*, LNCS 1807, pp.589-606, Springer, 2000.

[7] D. Coppersmith. The Real Reason for Rivest's Phenomenon. In *Proc. CRYPTO'85*, LNCS 218, pp. 535-536, Springer, 1985.

[8] E.K. Grossman and B. Tuckerman. Analysis of a Weakened Feistel-like Cipher. In Proc. *International Conference on Communications*, pp. 46.3.1-46.3.5, Alger Press Limited, 1978.

[9] S. Furuya. Slide Attacks with a Known-Plaintext Cryptanalysis. In Proc. Information and Communication Security 2001, LNCS 2288, pp. 214-225, Springer, 2002.

[10] O. Kara. Reflection Cryptanalysis of Some Ciphers. In *Proc. Indocrypt'08*, LNCS 5365, pp. 294-307, Springer, 2008.

[11] B.S. Kaliski, R.L. Rivest and T. Sherman. Is DES a Pure Cipher? (Results of More Cycling Experiments on DES). In *Proc. CRYPTO'85*, LNCS 218, pp. 212-222, Springer, 1985.

[12] J. Kelsey and B. Schneier. Key-Schedule Cryptanalysis of DEAL. In *Proc. SAC'99*, LNCS 1758 pp.118-134, Springer, 2000.

[13] L. Knudsen. DEAL - a 128-Bit Block Cipher. Avaliable at `http://www.ii.uib.no/ larsr/aes.html`.

[14] L. Knudsen. Cryptanalysis of LOKI91. In *Proc. of AUSCRYPT'92*, LNCS 718, pp 196-208, Springer, 1993.

[15] S. Lucks. On the Security of 128-Bit Block Cipher DEAL. In *Proc. FSE'99*, LNCS 1636, pp.60-70, Springer, 1999.

[16] J.H. Moore and G.J. Simmons. Cycle Structure of the DES with Weak and Semi-Weak Keys. In *Proc. CRYPTO'86*, LNCS 263, pp.9-32, Springer, 1986.

[17] J.H. Moore and G.J. Simmons. Cycle Structure of the DES for Keys Having Palindromic (or Antipalindromic) Sequences of Round Keys. *IEEE Transactions on Software Engineering*, pp. 262-273,No 13,1987.