On Resistance of DES to Related-Key Differential Cryptanalysis

Goce Jakimoski[*][†]and Yvo Desmedt[‡]

Abstract

The key schedule of the Data Encryption Standard is analyzed, and it is shown that the properties of the permuted choice PC-2 transformation and the number of bits that are left shifted during the key generation are critical for the security of the algorithm. More precisely, we were able to mount a low complexity related-key attack on DES with slightly modified key schedule although no related-key attack is known for the original algorithm.

Keywords: DES, differential cryptanalysis, related-key attacks

1 Introduction

DES [5] is a standard published by the National Bureau of Standards in 1977, and it describes the Data Encryption Algorithm used for encryption of commercial or unclassified governmental data. The algorithm is a block cipher that uses 64-bit blocks and a 64-bit key, but eight of the key bits are used for parity checking. Therefore, the actual key length is 56 bits.

Differential cryptanalysis [1, 2] is one of the best known attacks on DES. It is a chosen plaintext attack that exploits the predictability of the propagation of the plaintext difference. Because of its generality, differential cryptanalysis is a powerful tool for assessment of the security of many cryptographic primitives (e.g. encryption algorithms, hash function etc.). Related-key attacks [3, 7, 8] are another class of attacks that can be applied to a vast category of encryption algorithms. In these attacks, it assumed that the adversary can obtain plaintext/ciphertext pairs using different keys. The actual values of the keys are unknown, but the adversary knows some relation between the keys.

Related-key differential cryptanalysis [8, 6] combines these attacks. Namely, the adversary can choose the difference between the keys. One of the keys is randomly selected and the other one is computed based on the value of the first key and the key difference. Now, the attacker can submit for encryption chosen plaintexts to two encryption oracles that use the aforementioned key values. The key schedule of DES is completely linear. Given a key difference, the adversary with probability one can predict what will be the key difference for any round key. However, although the propagation of a key difference is totally predictable and DES can be broken using differential cryptanalysis, there is no known related-key differential attack on DES [8].

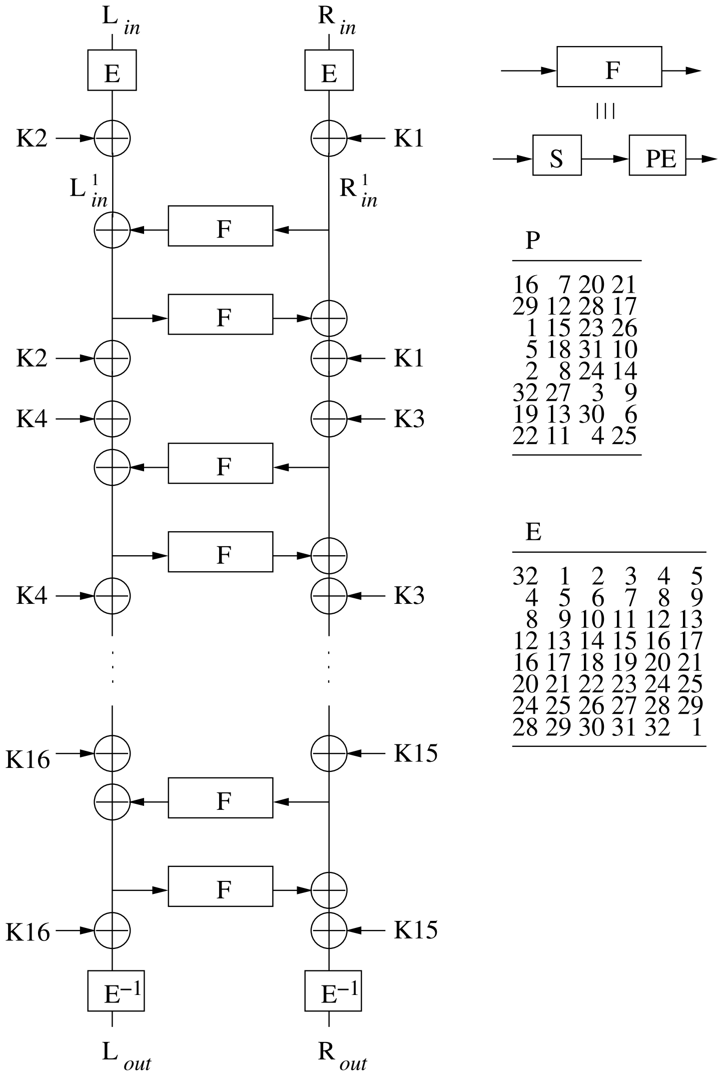
In this paper, we present related-key differential attack on DES variants with modified key schedule. The analysis gives an additional insight in the design of DES, the key scheduling algorithm particularly, by answering some questions about the resistance of the cipher to related-key differential cryptanalysis in spite of the key schedule linearity.

The paper is organized as follows. Section 2 briefly describes DES. In Section 3, we present an attack on DES variants. The paper ends with the concluding remarks.

[*] The author is with the Computer Science Department, Florida State University, Tallahassee, FL 32306-4530, USA. (e-mail: jakimosk@cs.fsu.edu)

[†] This work was supported in part by the National Science Foundation under Grant CCR-0209092

[‡] The author is with the Department of Computer Science, University College London, Gower Street, London WC1E 6BT, United Kingdom. (e-mail: y.desmedt@cs.ucl.ac.uk)



P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

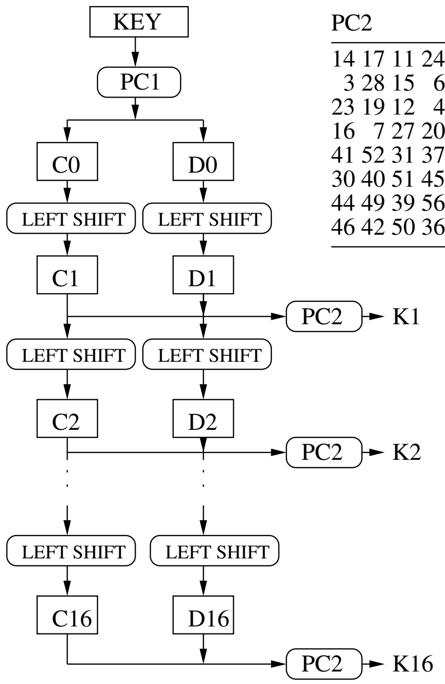
Figure 1: Mixing transformation representation of DES

2 Description of DES

A detailed description of the Data Encryption Algorithm can be found in [5]. By moving the components of the DES encryption rounds (e.g. over fan out point, over bitwise exclusive OR etc.) one can obtain equivalent representations of the DES encryption structure. Davio et al [4] proposed several equivalent representations that can be utilized for cryptanalysis or efficient implementation of DES. Here, we will use the mixing transformation representation depicted in Figure 1. The initial and the final permutation are omitted since they do not contribute to the security of the cipher.

The two 32-bit halves of the plaintext are first expanded to 48 bits using the DES expansion transformation E. The result is processed by a cascade of eight rounds, each round being a conjugate of a key independent nonlinear transformation by a linear transformation accounting for the action of the key[1]. Finally, the 96-bit output block is shrunk to 64 bits using a pseudo-inverse transformation E^{-1}.

[1] Cascades of linear transformations and nonlinear substitutions are also considered in the Shannon's seminal paper [9] under the heading mixing transformations.



PC2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Figure 2: The key schedule

The nonlinear transformation F is a composition of the DES S-box transformation S, permutation function P and the expansion transformation E. The S-box layer consists of eight S-boxes $(S_1, S_2, \ldots, S_8)$. Each S-box takes as input 6 bits of the 48-bit input block and yields 4-bit block as output. The resultant 32-bit block is permuted using the permutation function P. The expansion transformation takes as input the permuted 32 bits and gives as output 48 bits. The permutation P and the expansion transformation E are specified in Figure 1.

The 48-bit round keys K_n $(n = 1, \ldots, 16)$, are derived from a key $\mathcal{K}$ using a key scheduling algorithm KS. The calculation of the n-th round key is shown in Figure 2. The permuted choice PC_1 selects 56 out of 64 bits of $\mathcal{K}$ and permutes them to derive the two 28-bit halves C_0 and D_0. The key bits $8, 16, \ldots, 64$ are used for parity checking, and they are discarded by the permuted choice PC_1. The key generation continues in sixteen rounds. In each round n, the left shift operation rotates C_{n-1} and D_{n-1} by two bits left except in the rounds 1, 2, 9 and 16, when the bits are rotated only one position left. Finally, the permuted choice PC_2 selects 48 out of 56 bits (24 bits from each half) and permutes them to derive the round key. The permuted choice PC_1 has no effect on the security of the encryption algorithm and we skip its description.

3 Analyzing DES variants with modified key schedule

In this section, we will analyze a variant of DES whose key scheduling algorithm is slightly modified. First, the round keys K_i are constructed from C_i and D_i using a modified permuted choice bit selection. The new PC2 is depicted in Figure 3, and it differs from the original in five positions. Second, the number of bits that are shifted left in the key generation rounds 2 and 9 is two instead of one.

Let us consider two keys $\mathcal{K}'$ and $\mathcal{K}''$ such that:

$$\Delta C_1 = C_1' \oplus C_1'' = 0101010101010101010101010101 \tag{1}$$

$$\Delta D_1 = D_1' \oplus D_1'' = 0000000000000000000000000000 \tag{2}$$

modified PC2					
7	17	11	24	1	**10**
3	28	15	6	21	**5**
23	19	12	4	26	8
16	**14**	27	20	13	**9**
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Figure 3: The new permuted choice PC2

where C'_1, D'_1, C''_1 and D''_1 are as depicted in Figure 2 when the round keys are derived from $\mathcal{K}'$ and $\mathcal{K}''$ correspondingly. Note that for any key $\mathcal{K}'$ one can find a key $\mathcal{K}''$ so that ΔC_1 and ΔD_1 have the above values. When the relations (1) and (2) are satisfied, we have:

$$\begin{aligned} \Delta C_1 \lll 2 &= \Delta C_1 \\ \Delta D_1 \lll 2 &= \Delta D_1 \end{aligned}$$

where $\lll 2$ denotes a 2-bit left rotation. Therefore, for $1 \leq i < 16$, it will hold that

$$\begin{aligned} \Delta C_i &= 0101010101010101010101010101, \\ \Delta D_i &= 0000000000000000000000000000, \\ \Delta K_i &= 000101010100001111110100000000000000000000000000 \end{aligned}$$

and, for $2 < i < 16$, it holds that

$$K'_i \oplus K'_{i-2} = K''_i \oplus K''_{i-2}.$$

Consider now two plaintexts X' and X'' submitted for encryption under the keys $\mathcal{K}'$ and $\mathcal{K}''$ respectively such that:

$$\Delta L_{in} = L'_{in} \oplus L''_{in} = 00101010011110100000000000000000, \quad (3)$$

$$\Delta R_{in} = R'_{in} \oplus R''_{in} = 00101010011110100000000000000000. \quad (4)$$

After the expansion transformation E, we have:

$$\begin{aligned} E(L'_{in}) \oplus E(L''_{in}) &= E(L'_{in} \oplus L''_{in}) = E(\Delta L_{in}) = \Delta K_2, \\ E(R'_{in}) \oplus E(R''_{in}) &= E(R'_{in} \oplus R''_{in}) = E(\Delta R_{in}) = \Delta K_1. \end{aligned}$$

After the first key addition, we have:

$$\Delta L^1_{in} = \Delta R^1_{in} = 0,$$

where L^1_{in} (resp., R^1_{in}) denotes the left (resp., right) half of the input to the nonlinear layer of the first round. Since $K'_i \oplus K'_{i-2} = K''_i \oplus K''_{i-2}$ for $2 < i < 16$, the differences ΔL^i_{in} and ΔR^i_{in} will be zero for all subsequent rounds except the last one. The difference at the input of the nonlinear layer of the last round will be:

$$\begin{aligned} \Delta L^8_{in} &= \Delta K_{16} \oplus \Delta K_{14} \\ &= 111111111111111111111111000000000000000000000000 \end{aligned}$$

Assume that the adversary has access to an encryption oracle that uses a secret key $\mathcal{K}'$ and an encryption oracle that uses a secret key $\mathcal{K}''$ so that the relations (1) and (2) are satisfied. According the the previous discussion, one can mount the following related-key differential attack.

1. Select a plaintext X' uniformly at random and compute X'' so that the relations (3) and (4) are satisfied. Submit X' for encryption under the key $\mathcal{K}'$ to derive the ciphertext Y'. Submit X'' for encryption under the key $\mathcal{K}''$ to derive the ciphertext Y''.

2. Given Y', Y'', ΔK_{16} and ΔK_{14}, find all possible round keys K_{16} that give a difference ΔR^8_{in} equal to zero. Increment the counter corresponding to each of these keys by one.

3. Repeat the previous two steps until one of the round keys is counted significantly more than the others.

The right key will be counted each time steps one and two are repeated, and the probability that one of the wrong keys will be counted as a right key is significantly smaller. Therefore, the attack requires as little as several pairs of chosen plaintexts. If the counter maintenance is efficiently organized[2], then memory required for the counters is less than 1KB, and the complexity of the attack is about a hundred block encryptions.

The attack is not limited to the modified permuted choice specified in Figure 3.We can mount an analogous attack for any permuted choice PC2 that has the following property: there are differences $\Delta^L_{11}, \Delta^R_{11}, \Delta^L_{12}, \Delta^R_{12} \in \{0,1\}^4$, $\Delta_{21}, \Delta_{22} \in \{0,1\}^{32}$ and $\Delta_{31}, \Delta_{32} \in \{0,1\}^{48}$ so that

$$E(\Delta_{21}) = \mathrm{PC2}(\underbrace{\Delta^L_{11}||\ldots||\Delta^L_{11}}_{7\ \text{times}}||\underbrace{\Delta^R_{11}||\ldots||\Delta^R_{11}}_{7\ \text{times}}) = \Delta_{31}$$
$$E(\Delta_{22}) = \mathrm{PC2}(\underbrace{\Delta^L_{12}||\ldots||\Delta^L_{12}}_{7\ \text{times}}||\underbrace{\Delta^R_{12}||\ldots||\Delta^R_{12}}_{7\ \text{times}}) = \Delta_{32}$$

where Δ^L_{12} (resp., Δ^R_{12}) is derived by rotating Δ^L_{11} (resp., Δ^R_{11}) two bits left.

4 Conclusion

A version of DES with modified key schedule has been analyzed. It is shown that the permuted choice transformation and the number of bits that are left shifted to derive the round keys are critical for the security of DES, and even a small change of these operations can drastically decrease the security of the algorithm. Namely, by modifying these transformations, we were able to mount a related-key differential attack of extremely low complexity although there is no such known attack on DES.

References

[1] E.Biham and A.Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Journal of Cryptology, (1):3-72, 1991.

[2] E.Biham and A.Shamir,*Differential Cryptanalysis of Snefru, Khafre, REDOC II, LOKI, and Lucifer*, Advances in Cryptology, CRYPTO '91 Proceedings, Springer-Verlag, 1992, pp. 156-171.

[3] E.Biham,*New Types of Cryptanalytic Attacks Using Related Keys*, Journal of Cryptology, v. 7, n. 4, 1994, pp. 229-246.

[2] We don't have to try each possible key K_{16}. We can divide the bits of K_{16} into groups of six bits so that the bits that are in the same group affect only one S-box. Then, for each group separately, we can find the right values of the key bits in the group.

[4] M.Davio, Y.Desmedt, M.Fosseprez, R.Govaerts, J.Hulsbosch, P.Neutjens, P.Piret, J.J.Quisquater, J.Vandewalle, P.Wouters, *Analytical Characteristics of the DES*, Advances in Cryptology, Proceedings Crypto'83, pp.171-202.

[5] FIPS PUB 46-2, Data Encryption Standard (DES), http://www.itl.nist.gov/fipspubs/fip46-2.htm

[6] G.Jakimoski and Y.Desmedt, *Related-Key Differential Cryptanlysis of 192-bit Key AES Variants*, Tenth Annual Workshop on Selected Areas of Cryptography, LNCS 3006, pp. 208-221, Springer, 2004.

[7] J.Kelsey, B.Schneier and D.Wagner,*Key-schedule cryptanalysis of IDEA, GDES, GOST, SAFER, and Triple-DES*, Advances in Cryptology, Proceedings Crypto'96, LNCS 1109, pp.237-252.

[8] J.Kelsey, B.Schneier, and D.Wagner,*Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA*, ICICS '97 Proceedings, Springer-Verlag, November 1997, pp. 233-246.

[9] C.E. Shannon,*Communication Theory of Secrecy Systems*, Bell Technical Journal, vol.28(4), pp.656-715, 1949.