New potentially 'weak' keys for DES and LOKI (Extended abstract)

Lars Ramkilde Knudsen

Århus University, Denmark

Abstract. In this paper we present several new potentially weak (pairs of) keys for DES, LOKI89 and LOKI91.

1 Introduction

In this paper we consider DES-like iterative ciphers in particular the DES [5] and the LOKI ciphers, LOKI'89[2] and LOKI'91[3]. In these ciphers the ciphertext is calculated by recursively applying a round function to the plaintext. We expect the reader to be familiar with the basic concepts of differential cryptanalysis and refer to [1, 7] for further details.

In this paper we show how to use the '*differential techniques*' to find new classes of weak keys for DES-like iterated ciphers. We found several pairs of keys, **quasi weak keys**, for which there exist a simple relation between the DES-permutations induced by pairs of keys. Furthermore we define **weak hash keys** for DES-like iterated ciphers and show several of these for the LOKI ciphers.

2 DES

The F-function of the DES is defined $F(K_i, R_{i-1}) = P(S(E(R_{i-1}) \oplus K_i))$, where E is an expansion of 32 bits to 48 bits, S consist of 8 S-boxes each substituting a 6 bit value by a 4 bit value, P is a permutation of 32 bits and K_i is a 48-bit round key derived from a key schedule algorithm. In [6] it is shown that to have equal outputs of the F-function with two different inputs using the same key, the inputs must be different in the inputs to at least 3 neighboring S-boxes. We state here a converse result, i.e.

Lemma 1 (DES) *There exist pairs of round keys different in the inputs to only one S-box, s.t. using the same (text)input, equal outputs of the F-function are obtained.*

Proof: Because the keys are added to the input after the expansion, they do not (automatically) affect neighboring S-boxes. □

Furthermore there exist many pairs of 48 bit keys K_i and K_i' different in the inputs to only one S-box, s.t. equal inputs lead to equal outputs in one round of encryption.

We can use Lemma 1 to find what we will call **quasi weak keys** for DES.

2.1 Quasi weak keys for DES

According to Shannons concept of diffusion, there should be no simple relation between the two functions $DES_K(\cdot)$ and $DES_{K^*}(\cdot)$ for any two keys K and K^*. The well-known exceptions are the weak and semi-weak keys, a total of 16 for DES. We show that for several other pairs of keys for the DES there exists a simple relation between the encryption functions, at least for a fraction of all plaintexts.

The key schedule of the DES. The input is a 64 bit key. First the key is permuted and the parity bits are removed. This permutation has no importance for what we are about to show and we assume in the following that the input is a 56 bit (permuted) key. The 56 bits are divided into two blocks C_0 and D_0 of 28 bits each. The round keys K_i for $i = 1, ..., 16$ are defined $K_i = PC2(C_i \parallel D_i)$, where $C_i = LS_i(C_{i-1})$, $D_i = LS_i(D_{i-1})$, $PC2$ is a permutation and where LS_i is a left circular shift by the no. of positions given in Table 1. Alternatively, we could

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
LS_i	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1
$a[i]$	1	2	4	6	8	10	12	14	15	17	19	21	23	25	27	28

Table 1. The circular shifts in the key schedule of DES

define $L_i(C_0 \parallel D_0) = (LS_{a[i]}(C_0) \parallel LS_{a[i]}(D_0))$, where $a[i]$ is the accumulated number of shifts given in Table 1 and then define $K_i = PC2(L_i(K))$, where $K = (C_0 \parallel D_0)$, the 56 bit key. In the following we will use the alternative definition of the key schedule of DES.

Theorem 1 (DES) *For every key K, there exists a key K^*, s.t.*

$$K_{i+1} = K_i^*, \text{ for } i \in \{2, ..., 7\} \cup \{9, ..., 14\}$$

i.e. K and K^* have 12 common round keys.

Proof: Suppose we are given the key K. Set $K^* = L_2(K)$, where L is defined as above. Now it follows easily that

$$K_3 = PC2(L_4(K)) = PC2(L_2(K^*)) = K_2^*.$$

And similarly, $K_{i+1} = K_i^*$ for $i = 2, ..., 7$. Further, $K_9 = PC2(L_{17}(K))$ and $K_8^* = PC2(L_{14}(K^*)) = PC2(L_{16}(K))$. Hereafter the round keys get 're-synchronized', since

$$K_{10} = PC2(L_{17}(K)) = PC2(L_{15}(K^*)) = K_9^*.$$

And $K_{i+1} = K_i^*$ for $i = 9, ..., 14$. □

Theorem 2 (DES) *There exist 256 pairs of keys K and K^*, s.t.*

$$K_{i+1} = K_i^*, \text{ for } i \in \{2, ..., 14\}$$

i.e. K and K^* have 13 common round keys.

For these pairs of keys we found that there is some connection between the two encryption functions defined by the pair. In the following δ_i and ϵ_j denote 32 bit values. For every pair $\{\delta_i,\ \epsilon_j\}$ a probability $p_{i,j}$ is connected.

Theorem 3 (DES) *Let K and K^* be a pair of keys from Th. 2. Then for all plaintexts, P, there exist a pair $\{\delta_i, \epsilon_j\}$ and a probability $p_{i,j}$, s.t. with*
$P = P_L \,\|\, P_R$ and $P^* = P_R \oplus \delta_i \,\|\, P_L \oplus F(K_1, P_R)$

$$DES(K,P) = C_L \,\|\, C_R \Rightarrow DES(K^*,P^*) = C_R \oplus F(K^*_{16}, C_L \oplus \epsilon_j) \,\|\, C_L \oplus \epsilon_j \quad (1)$$

with probability $p_{i,j}$. Furthermore for the pairs of keys of Th. 2

$$\sum_{i,j} p_{i,j} = 1$$

Proof: Let K and K^* be a pair of keys from Th. 2. Choose a random plaintext $P = P_L \,\|\, P_R$. Encrypt P using K obtaining $C = C_L \,\|\, C_R = DES(K,P)$. Let the right half of P^* be $P_L \oplus F(K_1, P_R)$. The right half inputs (before addition of the keys) to the second round of $DES(K,P)$ and the first round of $DES(K^*,P^*)$ are equal. Let the difference in the round keys be $\Delta K_{2,1} = K_2 \oplus K^*_1$. That is, the difference in the inputs to the S-boxes of respectively the second and first round is $\Delta K_{2,1}$.

It is now easy from the 'pairs xor table' of DES to find a possible xor of the outputs of the respective rounds. Denote the outputs Ψ and Ψ^*, and define $\delta = \Psi \oplus \Psi^*$; the corresponding probability from the xor table is denoted p_δ. Now let the left half of P^* be $P_R \oplus \delta$. Now the right half input to the third round of the encryption with K is $P_R \oplus \Psi$ and the right half of the input to the second round of the encryption with K^* is $P_R \oplus \delta \oplus \Psi^*$, i.e. the inputs are equal, since $P_R \oplus \Psi \oplus P_R \oplus \delta \oplus \Psi^* = 0$. The left halves of the inputs to the corresponding rounds are also equal and since the keys are equal from now on and until the 16'th and 15'th round respectively, according to Theorem 2, it follows that the two encryptions are the same until the last and second last round respectively. For these rounds the right half of the inputs are equal and the xor of keys is $\Delta K_{16,15} = K_{16} \oplus K^*_{15}$. Let ϵ denote a possible xor of the outputs with input xor $\Delta K_{16,15}$ and the corresponding probability p_ϵ.
Now the implication in (1) holds with probability $p_{\delta,\epsilon} = p_\delta \times p_\epsilon$. To complete the proof we notice that for a given plaintext there is only one value for δ and ϵ above and that for all plaintexts there are only a limited number of choices for δ and ϵ, which depend on the keys (K, K^*) and they can easily be identified using the 'pairs xor table'. □

Example 1. Let $K^* = 4020\ 0000\ 1080\ 9080_x$ and $K = 0000\ 0080\ 9080\ 9080_x$ in hexadecimal notation, this pair is one of the pairs from Th. 2. The connection between the round keys of the pair is as follows. $K^*_i = K_{i+1}$ for $i = 2, .., 14$ and

$$K^*_1 \oplus K_2 = 00_x, 20_x, 00_x, 00_x, 00_x, 00_x, 00_x, 00_x$$
$$K^*_{15} \oplus K_{16} = 05_x, 00_x, 00_x, 00_x, 00_x, 00_x, 00_x, 00_x$$

where we have arranged the key bits in 8 groups of 6 bits each (hex). From the 'pairs xor table' of DES we find that for S-box 2, there are 9 possible xor of the outputs with an input xor 20_x. The most likely xor of the outputs is C_x, which has probability $\frac{14}{64}$. Let $\delta_1 = P(0C000000_x)$, where P is the 32-bit permutation at the end of the F-function, and denote the probability p_{δ_1}.
Similarly, we find that there are 14 possible xors of the outputs with an input xor 05_x for S-box 1. The most likely xor of the outputs is (again) C_x, which has probability $\frac{12}{64}$. Let $\epsilon_1 = P(C0000000_x)$ and denote the probability p_{ϵ_1}. With $\delta_i = \delta_1$ and $\epsilon_j = \epsilon_1$ the implication in (1) holds with probability $p_{1,1} = p_{\delta_1} \times p_{\epsilon_1} = \frac{14 \times 12}{64^2} \simeq \frac{1}{24}$. For the two keys in this example there are $9 \times 14 = 126$ pairs $\{\delta_i,\ \epsilon_j\}$ in Th. 3.

Since this phenomenon is due to only the xor of some round keys of K and K^*, a similar result holds for the complemented pairs of keys $\overline{K}$ and $\overline{K^*}$.
For all pairs of keys, K and K^* from Th. 1, $K_9 \neq K_8^*$ except for the 256 pairs of keys of Th. 2. As shown above the input to the ninth round for encryption with K and the input to the eighth round for encryption with K^* will be equal with some probability δ. That means that the inputxor for the two encryptions will be $(K_9 \oplus K_8^*)$, since the (text)inputs are equal. For about $2^{48.7}$ pairs of keys K and K^*, the input xor $(K_9 \oplus K_8^*)$ will lead to equal outputs for some fraction of all plaintexts. Lemma 1 shows that this is possible for keys that differ in the inputs to only one S-box. For the $2^{48.7}$ pairs of keys this fraction varies from $\frac{1}{4}$ to 2^{-39}. Therefore for these keys we have a parallel to Th. 3.

Theorem 4 (DES) *For $2^{48.7}$ pairs of keys K and K^*, it holds that for a fraction p_{KK^*} of all plaintexts there exist a pair $\{\delta_i, \epsilon_j\}$ and a probability $p_{i,j}$, s.t. for $P = P_L \,||\, P_R$ and $P^* = P_R \oplus \delta_i \,||\, P_L \oplus F(K_1, P_R)$*

$$DES(K, P) = C = C_L \,||\, C_R \Rightarrow DES(K^*, P^*) = C_R \oplus F(K_{16}^*, C_L \oplus \epsilon_j) \,||\, C_L \oplus \epsilon_j$$

with probability $p_{KK^*} \times p_{i,j}$, where $p_{i,j}$ is defined as in Th. 3. Similarly we have

$$\sum_{i,j} p_{i,j} = p_{KK^*}$$

Corollary 1 *There are 2368 pairs of keys for which the fraction P_{KK^*} is $\frac{1}{4}$.*

We conclude that for many pairs of keys in DES there is a simple relation between the encryption functions induced by these keys. This simple relation corresponds to one round of DES encryption and for 256 pairs of keys it holds for all plaintexts. For other $2^{48.7}$ pairs of keys it holds for a fraction of all plaintexts.

Applications. Since the phenomenon of Th. 3 and Th. 4 holds only for a small subset of keys and for most keys only for a fraction of all plaintexts, it is doubtful that the quasi weak keys can be exploited in attacks on the DES itself. However, DES is often used in hash functions where the keys are fixed or can be chosen as part of the (hash) message [9]. In differential attacks on hash functions based on block ciphers one could find two plaintexts, s.t. the (δ, ϵ)'s of Th. 3 are

equal, thereby in a differential the δ's and the rightmost ϵ's in (1) would cancel out. By trying sufficiently many pairs of plaintexts useful differentials (with fixed keys) might be found and used in attacks on hash functions.

3 Weak hash keys

We consider as before DES-like iterated block ciphers. Let the block size of the cipher be m.

Definition 1 *A* **weak hash key K** *is a key for which*

$$P \oplus E_K(P) = \delta \tag{2}$$

with probability $p >> 2^{-m}$ *for fixed* δ.

It is clear that weak hash keys should be avoided in hash modes where the input to the block cipher is added modulo 2 to the output to obtain some kind of one-wayness.

In [4] Coppersmith shows how to find fixpoints for DES used with weak keys, i.e. plaintexts P, s.t. $P = DES_K(P)$. For each weak key in DES (and LOKI) there are 2^{32} fixpoints, therefore a weak key in DES and LOKI is also a weak hash key. In [8] Moore and Simmons generalized the idea of Coppersmith to the case where, for DES, if for some key K, it holds that $K(i) = K(17-i) = E(\sigma)$ where E is the 48 bit expansion of some 32 bit string σ, then there are exactly 2^{32} plaintexts P, s.t. $DES_K(P) \oplus P = \sigma \| \sigma$. For the DES there are only eight keys satisfying this condition [8]. For the LOKI ciphers the keys are added before the expansion and the following result holds for the LOKI ciphers.

Theorem 5 (LOKI) *If* $K(i) \oplus K(17-i) = \sigma$ *for all* $i \in \{1, ..., 16\}$ *then* K *is a weak hash key and (2) holds with probability* 2^{-32}.

Note that the inputs to the eighth and ninth round uniquely determine both the plaintext and ciphertext and that the difference will be σ for exactly 2^{32} plaintexts. Also note that although equation (2) holds with probability only 2^{-32} for the above keys, the plain- and ciphertexts, for which (2) holds, can be found using only half an encryption, when the key is known. As for the quasi weak keys, once we have found a weak hash key for LOKI (or DES), the complemented key is also a weak hash key.

Corollary 2 *LOKI'89 has at least* 2^{16} *weak hash keys.*

Proof: It follows from the key schedule of LOKI'89, that the keys $K = K_L \| K_R$, where

$$K_L = vwyzvwyz_x \text{ and } K_R = VWYZVWYZ_x$$

s.t. $v \oplus w \oplus y = z$ and $V \oplus W \oplus Y = Z$ and $v \oplus V = w \oplus W = y \oplus Y$, satisfy the condition in Theorem 5. For LOKI'89 the key $K = K_L \| K_R$ is added (modulo 2) to the plaintext and the 'swapped' key $(K_R \| K_L)$ is added to the ciphertext [2]. The xor of the plaintext and the ciphertext for LOKI'89 (δ in (2)) is $\sigma \oplus c \| \sigma \oplus c$, where $c = K_L \oplus K_R$. □

Corollary 3 *LOKI'91 has at least* 16 *weak hash keys.*

Proof: Let $Rol_n(X)$ be X rotated (bitwise) n places to the left and let h be a hex digit, $h \in \{0,3,5,6,9,A,C,F\}$. From the key schedule of LOKI'91 it follows that the keys $K = K_L \,||\, K_R$, where $K_L = hhhhhhhh_x$ and $K_R = Rol_3(K_L)$ or $K_R = Rol_3(\overline{K_L})$ are weak hash keys. Eight of these keys are also either weak or semi-weak [3], but the other eight are neither weak nor semi-weak.

4 Conclusion and open problems

We defined and found several quasi weak keys for the DES and leave it as an open problem to exploit these keys in hash modes based on DES. We defined and found several weak hash keys for the LOKI ciphers. We strongly believe that both quasi weak keys and weak hash keys pose a threat for hash functions based on DES, LOKI'89 and LOKI'91. This will be a topic for further research. It is an open problem, whether it is possible to find weak hash keys for the DES. For DES versions with a reduced number of rounds it seems possible. But for the full DES it seems much harder than for the LOKI ciphers.

References

1. E. Biham, A. Shamir. *Differential Cryptanalysis of DES-like Cryptosystems.* Journal of Cryptology, Vol. 4 No. 1 1991.
2. L. Brown, J. Pieprzyk, J. Seberry. *LOKI - A Cryptographic Primitive for Authentication and Secrecy Applications.* Advances in Cryptology - AUSCRYPT '90. Springer Verlag, LNCS 453, pp. 229-236, 1990.
3. L. Brown, M. Kwan, J. Pieprzyk, J. Seberry. *Improving Resistance to Differential Cryptanalysis and the Redesign of LOKI.* Advances in Cryptology - Proceedings from ASIACRYPT'91, Springer Verlag, LNCS 739, pp. 36–50, 1993
4. D. Coppersmith. *The real reason for Rivest's phenomenon.* Advances in Cryptology - Proceedings of Crypto 85. Springer Verlag, LNCS 218, pp. 535–536, 1986.
5. *Data Encryption Standard,* Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.
6. Y. Desmedt, J-J. Quisquater, M. Davio. *Dependence of output on input in DES: Small avalanche characteristics.* Advances in Cryptology: Proceedings of CRYPTO 84. Springer Verlag, LNCS 196, pp. 359–376, 1985.
7. X. Lai. *On the Design and Security of Block Ciphers.* Thesis, ETH Zürich, 1992.
8. J.H. Moore and G.J. Simmons. *Cycle structure of the DES with weak and semiweak keys.* Advances in Cryptology - Crypto'86, Springer Verlag, LNCS 263, pp. 9-32, 1987.
9. B. Preneel. *Analysis and Design of Cryptographic Hash Functions.* Thesis, Katholieke Universiteit Leuven, January 1993.

This article was processed using the LaTeX macro package with LLNCS style