Relatório Técnico do INE

Linear cryptanalysis of pseudorandom functions

Daniel Santana de Freitas, Olivier Markowitch,
Jorge Nakahara Jr

Relatório Técnico INE 001/2015

Universidade Federal de Santa Catarina
Departamento de Informática e Estatística

FREITAS, D.S.; MARKOWITCH O.; NAKAHARA JR, J. Linear cryptanalysis of pseudorandom functions. Florianópolis: INE-UFSC, 2015. 6p. (Relatório Técnico, INE 001-2015)

Linear cryptanalysis of pseudorandom functions

Daniel Santana de Freitas[1], Olivier Markowitch[2], Jorge Nakahara Jr[2*]
[1]*Dept. Computer Science, Federal University of Santa Catarina, Brazil*
[2]*Dept. d'Informatique, Université Libre de Bruxelles, Belgium*
santana@inf.ufsc.br, {olivier.markowitch, jorge.nakahara}@ulb.ac.be

Keywords: linear cryptanalysis, Key feedback mode of operation, linear key schedule algorithms.

Abstract: In this paper, we study linear relations propagating across block ciphers from the key input to the ciphertext (for a fixed plaintext block). This is a usual setting of a one-way function, used for instance in modes of operation such as KFB (key feedback). We instantiate the block cipher with the full 16-round DES and s^2-DES, 10-round LOKI91 and 24-round Khufu, for which linear relations with high bias are well known. Other interesting targets include the full 8.5-round IDEA and PES ciphers for which high bias linear relations exist under the assumption of weak keys. Consequences of these findings impact the security of modes of operation such as KFB and of pseudorandom number/bit generators. These analyses were possible due to the linear structure and the poor diffusion of the key schedule algorithms. These findings shall motivate carefull (re)design of current and future key schedule algorithms.

1 INTRODUCTION

The technique of linear cryptanalysis was extensively developed by Matsui (Matsui, 1994a; Matsui, 1994b) in attacks initially aimed at the DES (NIST, 1993) and FEAL (Matsui and Yamaguishi, 1992) block ciphers. These attacks used so called linear relations that are linear combinations of bits from the plaintext, ciphertext and key that hold with high bias (deviation of the linear relation's probability from 0.5). The conventional strategy is to derive these relations piecewise, starting from an S-box or other nonlinear components and then extend the relations into larger components, and further to a full round and then to multiple rounds.

Let a block cipher have signature $E : \mathbb{Z}_2^k \times \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$, where n is the block size and k is the key size. A linear attack in a block cipher setting assumes the key to be fixed but unknown, while the plaintext is variable, so that the cipher behaves as a (pseudorandom) permutation: $E_K : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ for any secret key K. In this paper we analyse the setting in which the plaintext is fixed and randomly chosen, while the key is variable: $E(P) : \mathbb{Z}_2^k \rightarrow \mathbb{Z}_2^n$. In this setting, the plaintext is considered secret.

In this paper we focus only on attacks in the distinguish-from-random setting.

This paper is organized as follows: Sect. 2 studies linear relations across a pseudorandom function based on the full 16-round DES and s^2-DES ciphers, as well as 10-round LOKI91; Sect. 3 studies linear relations across a pseudorandom function based on the IDEA and PES ciphers; Sect. 4 studies linear relations across a pseudorandom function based on variable-round Khufu cipher; Sect. 5 concludes the paper.

2 LINEAR RELATIONS FOR DES, S^2-DES AND LOKI91 FUNCTIONS

In (Matsui, 1994a), Matsui performed a divide-and-conquer analysis to determine the best linear expression for variable-round DES, that is, linear relations covering multiple rounds of DES with the highest possible bias. We adopt the same notation and bit numbering for DES as (Matsui, 1994a): a bitmask will be represented by either Γ or a sequence of numbers between square brackets, for instance, $X[i, j, \ldots, z] = X[i] \oplus X[j] \oplus \ldots \oplus X[z]$. In both cases, the bits '1' in Γ or the numbers between brackets indicate the bits participating in the linear relation. For n-bit strings a and b, the dot (or inner) product is denoted $a \cdot b = \oplus_{i=0}^{n-1} a_i \cdot b_i$ and it gives a parity bit.

*Research funded by INNOVIRIS, the Brussels Institute for Research and Innovation, under the ICT Impulse program CRYPTASC.

A plaintext P for DES is split into its left and right halves as $P = (P_L, P_R)$ and similarly for the ciphertext $C = (C_L, C_R)$.

A linear relation for the full 16-round DES (Matsui, 1994b) without the IP and FP bit permutations, and where the i-th round subkey is denoted K_i, is

$$\begin{aligned} &P_L[7,18,24] \oplus P_R[12,16] \oplus \\ &\quad C_L[15] \oplus C_R[7,18,24,27,28,29,30,31] = \\ &K_1[19,23] \oplus K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22] \oplus \\ &K_8[44] \oplus K_9[22] \oplus K_{11}[22] \oplus K_{12}[44] \oplus K_{13}[22] \oplus \\ &\quad K_{15}[22] \oplus K_{16}[42,43,45,46], \quad (1) \end{aligned}$$

holding with bias $1.49 \cdot 2^{-24}$, which leads to $4 \cdot (1.49 \cdot 2^{-24})^{-2} = 2^{48.84}$ messages for a high success rate distinguishing attack.

In (Junod, 2000), Junod showed experimentally that Matsui's key-recovery attack complexity was pessimistic, that is, Junod's results indicate a high success rate (85%) can be achieved with one eighth of the original attack complexity that is, 2^{43} known plaintexts (KP) instead of 2^{47} KP predicted by Matsui. If the same results apply for a distinguish-from-random setting, then we can expect only about 2^{43} plaintext-ciphertext pairs are needed for a high success rate attack.

Taking into account the key schedule of DES (except that PC1 bit selection transformation is omitted) (NIST, 1993), the right-hand side of (1) can be summarized as $K[8,14,0,54,24,20,46,17,13,39,9,5,51,55,45,39] = K \cdot \Gamma K$, where K stands for the original 56-bit key. Note that the linear relations stretch all across the key schedule up to the original 56-bit key.

Now, unlike the original linear attack setting, let P be fixed to a random value, but the key be variable[2]. We can rewrite (1) as

$$\begin{aligned} &C_L[15] \oplus C_R[7,18,24,27,28,29,30,31] \oplus \\ &K[8,14,0,54,24,20,46,17,13,39,9,5,51,55,45,39] \\ &\quad = P_H[7,18,24] \oplus P_R[12,16], \quad (2) \end{aligned}$$

where the right-hand side is a fixed value. Note that (2) contains the same bits as (1) but some terms were rearranged because now P is fixed instead of K. This means (2) is applied to a random mapping $E(P) : \mathbb{Z}_2^{56} \rightarrow \mathbb{Z}_2^{64}$ instead of a random permutation $E_K : \mathbb{Z}_2^{64} \rightarrow \mathbb{Z}_2^{64}$. This is a typical construction of one-way functions (Winternitz, 1983) and in the KFB mode of operation (Hastad, 2000). Nonetheless, the linear relation still covers the full 16-round DES, with the same bias as before. Note that knowledge of the full 64-bit P is not actually needed, since (2) only relies on one bit: $P_H[7,18,24] \oplus P_R[12,16]$. Since the masks and P are fixed, knowledge of P is not necessary, and the bias of (2) does not change. Only the sign of the deviation changes according to the parity of $P_H[7,18,24] \oplus P_R[12,16]$. Nonetheless, to avoid trivial attacks based on the knowledge of the block cipher, we assume that P is secret.

A similar equation can be derived by fixing the ciphertext block $C = (C_L, C_R)$ and varying the key K (the plaintext P is the output).

$$\begin{aligned} &P_L[7,18,24] \oplus P_R[12,16] \oplus \\ &K[8,14,0,54,24,20,46,17,13,39,9,5,51,55,45,39] \\ &\quad = C_L[15] \oplus C_R[7,18,24,27,28,29,30,31], \quad (3) \end{aligned}$$

which also applies to a random function $E(C_0) : \mathbb{Z}_2^{56} \rightarrow \mathbb{Z}_2^{64}$, where C_0 is a random 64-bit string.

In (Matsui, 1994c), a 2-round iterative linear relation for DES was described[3] with the form $F(X,K)[0,5,10,11,20,25,27] = K[4,5,6,7]$ and probability $1/2 + 2(40/64 - 172)(20/64 - 1/2) = 0.453$, that is, with bias $1/2 - 0.453 = 0.047 \approx 2^{-4.411}$. This is a so called 2-round iterative Type-II linear relation with a single active F function (only the output of F is approximated) every two rounds, with only two active neighbouring S-boxes, S7 and S8, every two rounds. For the full 16-round DES, concatenating the linear relation eight times, the bias becomes $2^7 \cdot 2^{8 \cdot (-4.411)} \approx 2^{-28.289}$. Thus, this bias is smaller than (1). The data complexity for a high success rate becomes $8 \cdot (2^{-28.289})^{-2} = 2^{3+56.579} = 2^{59.579}$ known plaintexts (KP). This is more data than can be expected by operating DES from the key entry (the key input is only 56 bits). Note that even though the original 2-round relation is iterative, when concatenated eight times for the full DES, the resulting linear relation is not iterative because there is no swap of half blocks in the last (sixteenth) round.

Thus, (2) represents a new framework for the linear relation originally applied to the full DES. It was possible because the key schedule of DES is a linear mapping, that is, there are only bit permutations and bit selections but no S-boxes nor other nonlinear components. So, the original key bitmasks for the DES round subkeys could propagate up to the original key K without any bias penalty. This fact demonstrates, once more, the need for the key schedule algorithm to be nonlinear.

The mapping from the key to the ciphertext is not injective. Assuming that a linear relation such as (3) holds with the same bias $2^{-28.289}$ for each fixed key

[2] The mapping from key to plaintext (or from key to ciphertext) is modeled as a random, non-injective mapping, thus not a permutation.

[3] Without the IP and FP bit permutations.

K when the probability is taken over all P, then one gets that (3) holds with bias $2^{-28.289}$ when the probability is taken over P and K. This assumption may not always hold, but is necessary to the analysis in this paper. Taken it as granted, one can, by letting the key vary, generate as much data as needed without worrying about possible collisions between the values $E_K(P)$ for variable K.

In the Key-FeedBack (KFB) mode of operation (Hastad, 2000) proposed for NIST's Advanced Encryption Standard (AES), the ciphertext produced for a fixed plaintext P is fedback as key to the next block cipher instantiation: $C_0 = b_r(E_K(P))$ and $C_i = b_r(E_{g(C_{i-1}}(P))$, were g converts the ciphertext to the appropriate size for the key input, and b_r is the output transformation that extracts hard-core bits for each instantiation of E. In (Hastad, 2000), $b_r(x)$ is the dot product between an n-bit selection vector $r = (r_1, r_2, \ldots, r_n)$ and an n-bit ciphertext block $x = (x_1, x_2, \ldots, x_n)$. Alternatively, the output transformation can be larger than a single bit, leading to a larger throughput per encryption, and is denoted $B_R^m(x)$ corresponding to $m = O(\log n)$ bits selected according to a random $m \times n$ matrix. This matrix is not invertible.

Thus, in an attack using (2), the initial 56-bit key K is secret, but subsequent keys to DES invocations are derived from previous ciphertexts C_i. If a single b_r is used, then a single bit is generated for each DES encryption. Otherwise, up to $\log n$ bits are output per encryption. We assume that some of the coefficients of the B_R^m matrix match the bits $C_L[15] \oplus C_R[7,18,24,27,28,29,30,31]$ in (2). The matrix B_R^m is not secret or we assume it could be chosen by the adversary. Moreover, the fact that $B_R^m(x)$ is not invertible means that the full n-bit plaintext P is not disclosed. Otherwise, if $B_R^m(x)$ was invertible, then knowing two consecutive n-bit ciphertexts, say C_i and C_{i+1}, and knowing the block cipher E, one could easily compute P as $P = E_{C_i}^{-1}(C_{i+1})$.

Starting from the second DES instantiation, there is a nonzero correlation between the key, which is $g(C_0)$ from the previous encryption, and the ciphertext, $B_R^m(E_{g(C_0)}(P))$. This correlation can be detected after collecting 2^{43} keystream bits from this instantiation of KFB.

Similar attacks apply to the full 16-round s^2-DES (Kim, 1991). The s^2-DES cipher operates on 64-bit blocks and has a 56-bit key, just like the DES. In (Tokita et al., 1994), Tokita *et al.* described a linear relation for the full 16-round s^2-DES with bias $1.19 \cdot 2^{-26}$. Denoting the plaintext as $P = (P_L, P_R)$ and the ciphertext as $C = (C_L, C_R)$, the linear relation can be denoted

$$(P_R \oplus C_L)[5,10,11] = (K_2 \oplus K_4 \oplus K_6 \oplus K_8 \oplus K_{10} \oplus K_{12} \oplus K_{14} \oplus K_{16})[4,5,6,7], \quad (4)$$

following the same bit-numbering as in DES. This linear relation is based on a 2-round iterative linear relation $(P_L \oplus C_R)[5,10,11] = K_i[4,5,6,7]$, with a single active F function.

Now, consider that the plaintext P is fixed to a random value, but the key is variable. We can rewrite (4) as

$$C_L[5,10,11] \oplus (K_2 \oplus K_4 \oplus K_6 \oplus K_8 \oplus K_{10} \oplus K_{12} \oplus K_{14} \oplus K_{16})[4,5,6,7] = P_R[5,10,11], \quad (5)$$

where the right-hand side is a fixed value. This means (5) applied to a random mapping $E(P) : \mathbb{Z}_2^{56} \to \mathbb{Z}_2^{64}$ (for a fixed P) instead of a random permutation $E_K : \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{64}$. The data complexity for (4) is $2^{48.3}$ keys.

In (Tokita et al., 1994), Tokita *et al.* also described linear relations for reduce-round variants of LOKI91 (Brown et al., 1991; Sakurai and Furuya, 1997), a Feistel Network cipher operating on 64-bit blocks, under a 64-bit key and iterating 16 rounds. We focus on a 10-round linear relation with bias $2^{-28.24}$ based on the one-round iterative linear relation $(X \oplus F(X))[18,22,26] = K[18,22,26]$, with bias $0.687 \cdot 2^{-5} \approx 2^{-5.54}$.

Denoting the plaintext to LOKI91 as $P = (P_L, P_R)$ and the ciphertext as $C = (C_L, C_R)$, the linear relation can be denoted

$$(P_R \oplus C_R)[18,22,26] = (K_2 \oplus K_3 \oplus K_5 \oplus K_6 \oplus K_8 \oplus K_9)[18,22,26]. \quad (6)$$

This linear relation contains only six active F functions across ten rounds. If we now consider that the plaintext P is fixed to a random value, but the key is variable. This is facilitated by the fact that the key schedule of LOKI91 consists only of bit rotations. There are only linear components in the key schedule.

We can rewrite (6) as

$$(C_R \oplus K_2 \oplus K_3 \oplus K_5 \oplus K_6 \oplus K_8 \oplus K_9)[18,22,26] = P_R[18,22,26], \quad (7)$$

where the right-hand side is a fixed value. This means relation (7) is applied to a random mapping $E(P) : \mathbb{Z}_2^{56} \to \mathbb{Z}_2^{64}$ (for a fixed P) instead of a random permutation $E_K : \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{64}$. The data complexity for (6) is $8 \cdot 2^9 \cdot 2^{-4} \cdot (2^{5.54})^{-6} = 2^{59.48}$ keys.

3 LINEAR RELATIONS FOR IDEA AND PES FUNCTIONS

The IDEA block cipher (Lai et al., 1991) operates on 64-bit blocks, iterates eight rounds plus an output transformation and is parameterized by a 128-bit key. IDEA was designed as an alternative to the DES (NIST, 1993) and is well-known for the use of three incompatible group operations on 16-bit words: bitwise xor, addition modulo 2^{16} and multiplication in GF$(2^{16}+1)$, where $0 = 2^{16}$. The key schedule of IDEA is linear and consists only of bit permutations. All multiplication operations in IDEA involve a round subkey and that is the main feature explored in (Daemen and Vandewalle, 1993). Daemen *et al.* described linear attacks on the full IDEA cipher using weak keys. In this setting, a weak key is a 128-bit key that leads, through the key schedule, to some round subkeys which are either 0 or 1 for the multiplication operations[4]. Note that multiplication (together with addition) are the main nonlinear operations in IDEA. Using weak keys and the (linear) key schedule, Daemen *et al.* were able to determine a series of linear relations, some of which are iterative, across the full 8.5-round IDEA. Due to the use of weak keys, their linear relations hold with maximum bias.

As an example, let $P = (p_1, p_2, p_3, p_4)$ denote a plaintext block, and $C = (c_1, c_2, c_3, c_4)$ the corresponding ciphertext. The i-th round subkeys are denoted $Z_1^i, Z_2^i, \ldots, Z_6^i$, for $1 \le i \le 8$, and $Z_1^9, Z_2^9, Z_3^9, Z_4^9$ for the output transformation. In (Daemen and Vandewalle, 1993), Table 2, Daemen *et al.* provided a listing of all 1-round linear relations: they called them linear factors. Each such relation holds with maximum bias once the weak subkey conditions are satisfied. These conditions imply that some round subkeys should be 0 or 1, so that the corresponding linear trail is satisfied. For instance, $(1,0,1,0) \xrightarrow{1r} (1,1,0,0)$ is a 1-round linear trail that stands for $p_1 \cdot 1 \oplus p_3 \cdot 1 = c_1 \cdot 1 \oplus c_2 \cdot 1$ that holds with maximum bias 2^{-1} once $Z_1^i \in \{0,1\}$. A larger linear relation across the full 8.5-round IDEA has the form $(1,0,1,0) \xrightarrow{8.5r} (0,1,1,0)$ which can be translated into

$$(p_1 \oplus p_3 \oplus c_1 \oplus c_3) \cdot 1 = (Z_3^1 \oplus Z_2^2 \oplus Z_2^3 \oplus Z_3^3 \oplus Z_3^4 \oplus Z_2^5 \oplus Z_2^6 \oplus Z_3^6 \oplus Z_3^7 \oplus Z_2^8 \oplus Z_2^9 \oplus Z_3^9) \cdot 1, \quad (8)$$

so, the right-hand-side of (8) stands for $K \cdot \Gamma K$. It is required that eleven round subkeys be weak: Z_1^1, Z_1^2, Z_5^2, Z_5^3, Z_1^4, Z_1^5, Z_5^5, Z_5^6, Z_1^7, Z_1^8 and Z_5^8. Since the key schedule of IDEA consists simply of bit permutation, this restriction on eleven subkeys can be translated into restrictions on 105 bits of the original 128-bit key. Following (Daemen and Vandewalle, 1993), only the key bits with indices in the ranges 16–28, 72–74 and 111–127 are free of any conditions, which means 23 key bits. In summary, for 2^{23} weak keys, the linear relation (8) holds with maximum bias. This linear attack applies to the setting in which $E_K : \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{64}$ is a permutation with E being the full IDEA and a key $K \in \mathbb{Z}_2^{128}$ with the above restriction on 105 bits. Thus, a distinguishing attack would require about $8 \cdot (2^{-1})^{-2} = 32$ KP and equivalent effort.

Now suppose we operate on $E(P_0) : \mathbb{Z}_2^{128} \to \mathbb{Z}_2^{64}$ for E being the full IDEA, and a fixed plaintext $P_0 \in \mathbb{Z}_2^{64}$. Suppose, we apply once more the linear relation (8), but this time to $E(P_0)$ instead of E_K. This means that the key is variable, while the plaintext is fixed. The new linear relation becomes

$$(c_1 \oplus c_3 \oplus Z_3^1 \oplus Z_2^2 \oplus Z_2^3 \oplus Z_3^3 \oplus Z_3^4 \oplus Z_2^5 \oplus Z_2^6 \oplus Z_3^6 \oplus Z_3^7 \oplus Z_2^8 \oplus Z_2^9 \oplus Z_3^9) \cdot 1 = (p_1 \oplus p_3) \cdot 1. \quad (9)$$

Because of the key restrictions, we have only 2^{23} keys as input. Under any of the weak keys, relation (9) holds with maximum bias. Each time we test it, it shall hold only with probability $\frac{1}{2}$ for a random permutation. Thus, we can efficiently distinguish $E(P_0) : \mathbb{Z}_2^{23} \to \mathbb{Z}_2^{64}$ from a random function over the same domain and range. We estimate that 32 keys will be needed (out of 2^{23}).

A similar analysis can be performed on the predecessor of IDEA, called PES (Proposed Encryption Standard) (Lai and Massey, 1990), since both use the same key schedule algorithm. The PES cipher operates on 64-bit blocks, under a 128-bit key and iterates 8.5 rounds. In (Nakahara Jr et al., 2003), Nakahara *et al.* describe linear relations for large sets of weak keys. For instance, $(0,0,0,1) \xrightarrow{8.5r} (0,0,0,1)$ is an iterative linear relation covering the full PES under the assumption that subkeys Z_6^i, $1 \le i \le 8$ are weak. According to the key schedule of PES, this implies that key bits 0–12, 49–65, 95–108 and 124–127 are unrestricted. In summary, the following linear relation holds[5] for $E(P_0) : \mathbb{Z}_2^{48} \to \mathbb{Z}_2^{64}$ for E being the full 8.5-round PES cipher, and a weak-key class of size 2^{48}:

$$(c_4 \oplus Z_4^1 \oplus Z_4^2 \oplus Z_4^3 \oplus Z_4^4 \oplus Z_4^5 \oplus Z_4^6 \oplus Z_4^7 \oplus Z_4^8 \oplus Z_4^9) \cdot 1 = p_4 \cdot 1. \quad (10)$$

[4] In (Daemen and Vandewalle, 1993), the restriction is that a weak subkey belongs to the set $\{-1, 1\}$

[5] Note the updated domain size.

Thus, we can efficiently distinguish $E(P_0) : \mathbb{Z}_2^{48} \rightarrow \mathbb{Z}_2^{64}$ from a random function over the same domain and range. We estimate that 32 keys will be needed (out of 2^{48}).

The threat of a linear key schedule can be measured by the fact that there is at least one weak key even for 17.5-round PES (Nakahara Jr et al., 2003), using the 1-round iterative linear relation $(0,1,0,1) \rightarrow (0,1,0,1)$. Moreover, there are 2^4 weak keys for 14-round IDEA using a 3-round iterative relation $(1,0,0,1) \rightarrow (0,1,0,1) \rightarrow (0,0,1,1) \rightarrow (1,0,0,1)$.

4 LINEAR RELATIONS FOR KHUFU FUNCTION

Khufu is a block cipher designed by Merkle (Merkle, 1991) for fast software encryption. Khufu is a Feistel Network cipher operating on 64-bit blocks, under a user key of up to 512 bits and iterating $8r$ rounds, for $1 \leq r \leq 8$, where r is called the number of octets. Originally, $r = 2$ was suggested. Khufu operates on 8- and 32-bit words and its internal operations include: exclusive-or, byte rotations and an 8×32-bit S-box. Each S-box is key dependent, represents 2^{13} bits of the secret key and is used for one octet only. Let a plaintext block be denoted $P = (L_0, R_0)$, the S-box by S, a leftwards rotation of a data x by n bits by $x \lll n$ and the least significant n bits of x by $\text{lsb}_n(x)$. Then, the ith round of Khufu outputs (R_i, L_i), where $R_i = L_{i-1} \lll s_i$, where s_i is a fixed rotation amount, multiple of 8 bits, and $L_i = R_{i-1} \oplus S[\text{lsb}_8(L_{i-1})]$. For each round in an octet, the values of s_i are 16, 16, 24, 24, 16, 16, 8 and 8 in this order and repeated cyclically. There is a pre-whitening in which two 32-bit subkeys K_1 and K_2 are xored to the plaintext and an output transformation in which subkeys K_3 and K_4 are xored to the output of the last round.

We will use the 2-round iterative linear analysis of Khufu described in (Nakahara Jr, 2007), with bias 2^{-3}, which holds for a fraction of 5% of the keys. This fraction corresponds to a weak-key class. This 2-round iterative linear relation has the form $L_i \cdot mmmm_x = L_{i+2} \cdot mmmm_x$, for $0 < m \leq 255$, and $mmmm_x$ stands for a 32-bit mask. This mask is rotation invariant, that is, $mmmm_x \lll 8t = mmmm_x$ for any t, because rotations are over multiples of 8 bits.

Repeating this 2-round iterative relation, we can achieve a linear distinguisher for 24-round Khufu with bias $2^{11-12 \cdot 3} = 2^{-25}$, and requiring $8(2^{-25})^{-2} = 2^{53}$ known plaintexts (KP):

$$(L_0 \oplus L_{24}) \cdot mmmm_x = (K_1 \oplus K_3) \cdot mmmm_x, \quad (11)$$

where we include the pre- and post-whitening keys. Fixing the plaintext (L_0, R_0) and making the key variable in (11), we arrive at the following linear relation

$$(L_{24} \oplus K_1 \oplus K_3) \cdot mmmm_x = L_0 \cdot mmmm_x. \quad (12)$$

To match the block size, we assume a key of 64 bits. This means (12) applied to a random mapping $E(P) : \mathbb{Z}_2^{64} \rightarrow \mathbb{Z}_2^{64}$, for a fixed $P = (L_0, R_0)$ instead of a random permutation $E_K : \mathbb{Z}_2^{64} \rightarrow \mathbb{Z}_2^{64}$. The data complexity for a distinguishing attack on (12) is 2^{53} keys.

5 CONCLUSIONS

This paper applied linear analyses originally designed against the full DES, the full s^2-DES, 10-round LOKI91, 24-round Khufu, variable-round IDEA and PES block ciphers under a (pseudo-)random function setting. In other words, instead of applying linear relations from the plaintext input to the ciphertext, under a fixed key, the (same) linear relations were applied from the key input to the ciphertext, under a fixed plaintext. This is possible because the key schedule algorithms are linear mappings, which means the linear approximation through the key schedule framework does not affect the bias of the original linear relation.

These linear relations are a potential threat to applications of such block ciphers in pseudorandom number generators and PRFs, since they provide a linear relationship between the inputs and outputs in a known-input-output setting.

The linear relations emphasize the need for nonlinearity in the key schedule algorithms to avoid linear relations to be applied from the key input to the ciphertext, and holding with the same bias as the original attack from plaintext to ciphertext.

REFERENCES

Brown, L., Kwan, M., Pieprzyk, J., and Seberry, J. (1991). Improving resistance to differential cryptanalysis and the redesign of loki. Technical Report CS38/91, Dept. of Computer Science, Univ. College, Australian Defence Force Academy.

Daemen, J.and Govaerts, R. and Vandewalle, J. (1993). Weak keys for idea. In Stinson, D., editor, *Adv. in Cryptology, CRYPTO 93*, LNCS 773, pages 224–231. Springer.

Hastad, J. (2000). Key feedback mode: a keystream generator with provable security. NIST modes of operation workshop.

Table 1: Attack complexities on pseudorandom functions in KFB mode. Memory complexity is negligible.

Function	Block size (bits)	Key size (bits)	Time	Data	Source (Eq.)
16-round DES	64	56	2^{43}	2^{43}	(1)
16-round s^2-DES	64	56	$2^{48.3}$	$2^{48.3}$	(5)
8.5-round IDEA	64	128	32	32	(9)
8.5-round PES	64	128	32	32	(10)
10-round LOKI91	64	64	$2^{59.48}$	$2^{59.48}$	(7)
24-round Khufu	64	≤ 512	2^{53}	2^{53}	(12)

Junod, P. (2000). Linear cryptanalysis of des. Master's thesis, ETH Zurich and EPFL Lausanne.

Kim, K. (1991). Construction of des-like s-boxes based on boolean functions satisfying the sac. In Imai, H., Rivest, R., and Matsumoto, T., editors, *Adv. in Cryptology, Asiacrypt*, LNCS 739, pages 59–72. Springer.

Lai, X. and Massey, J. (1990). A proposal for a new block encryption standard. In Damgård, I., editor, *Adv. in Cryptology, EUROCRYPT*, LNCS 473, pages 389–404. Springer.

Lai, X., Massey, J., and Murphy, S. (1991). Markov ciphers and differential cryptanalysis. In Davies, D., editor, *Adv. in Cryptology, EUROCRYPT*, LNCS 547, pages 17–38. Springer.

Matsui, M. (1994a). The first experimental cryptanalysis of the data encryption standard. In Desmedt, Y., editor, *Adv. in Cryptology, Crypto 1994*, LNCS 839, pages 1–11. Springer.

Matsui, M. (1994b). Linear cryptanalysis method for des cipher. In Helleseth, T., editor, *Adv. in Cryptology, Eurocrypt'93*, LNCS 765, pages 386–397. Springer.

Matsui, M. (1994c). On correlation between the order of s-boxes and the strength of des. In *Adv. in Cryptology, Eurocrypt'94*, LNCS 950, pages 366–375. Springer.

Matsui, M. and Yamaguishi, A. (1992). A new method for known plaintext attack of feal cipher. In Rueppel, R., editor, *Adv. in Cryptology, Eurocrypt 1992*, LNCS 658, pages 81–91. Springer.

Merkle, R. (1991). Fast software encryption functions. In *Adv. in Cryptology, Crypto 1990*, LNCS 537, pages 476–501. Springer.

Nakahara Jr, J. (2007). A linear analysis of blowfish and khufu. In Dawson, E. and Wong, D., editors, *ISPEC*, LNCS 4464, pages 20–32. Springer.

Nakahara Jr, J., Preneel, B., and Vandewalle, J. (2003). A note on weak-keys of pes, idea and some extended variants. In Boyd, C. and Mao, W., editors, *6th Information Security Conference (ISC)*, LNCS 2851, pages 269–279. Springer.

NIST (1993). Fips pub 46-1, data encryption standard. Federal Information Processing Standards Publication 46-2.

Sakurai, K. and Furuya, S. (1997). Improving linear cryptanalysis of loki91 by probabilistic counting method (extended abstract). In Biham, E., editor, *Fast Software Encryption (FSE) Workshop*, LNCS 1267, pages 114–133. Springer.

Tokita, T., Sorimachi, T., and Matsui, M. (1994). Linear cryptanalysis of loki and s^2-des. In Pieprzyk, J. and Safavi-Naini, R., editors, *Adv. in Cryptology, Asiacrypt'94*, LNCS 917, pages 293–303. Springer.

Winternitz, R. (1983). Producing a one-way hash function from des. In *Adv. in Cryptology, Crypto'83*, pages 203–207. Springer.