Cryptanalysis of the Full DES and the Full 3DES Using a New Linear Property

Tomer Ashur[1] and Raluca Posteuca[1]

imec-COSIC, KU Leuven, Leuven, Belgium
[tomer.ashur, raluca.posteuca]@esat.kuleuven.be

Abstract. In this paper we extend the work presented by Ashur and Posteuca in BalkanCryptSec 2018, by designing 0-correlation key-dependent linear trails covering more than one round of DES. First, we design a 2-round 0-correlation key-dependent linear trail which we then connect to Matsui's original trail in order to obtain a linear approximation covering the full DES and 3DES. We show how this approximation can be used for a key recovery attack against both ciphers. To the best of our knowledge, this paper is the first to use this kind of property to attack a symmetric-key algorithm, and our linear attack against 3DES is the first statistical attack against this cipher.

Keywords: linear cryptanalysis, DES, 3DES, poisonous hull

1 Introduction

Linear cryptanalysis is one of the most important tools used in the security evaluation of block ciphers. It was introduced in 1993, by Mitsuru Matsui, and used to attack the DES cipher. The technique became intensively studied, the formalism of linear cryptanalysis being extended in e.g., [Bih94, Nyb94]. It has been proven to be widely applicable and has produced many variants and generalizations such as multiple linear cryptanalysis [JR94, BCQ04], differential-linear cryptanalysis [CV94], zero-correlation linear cryptanalysis [BR11, BR14], etc.

Usually, linear cryptanalysis is used to launch a known-plaintext attack. The hypothesis of a known-plaintext attack is that the attacker has a set of plaintexts and their corresponding ciphertexts, enciphered using the same, fixed, key. The purpose of the attack is to recover information regarding the secret key that was used.

The initial idea behind linear cryptanalysis was to find a linear approximation connecting between a set of plaintext, ciphertext and key bits that holds with a probability different from 0.5. The quality of a linear approximation, usually measured by its correlation or its bias, is one of the open problems in linear cryptanalysis, being directly related to the success rate and the data complexity of the attack.

In order to construct a linear approximation of an iterated cipher, Matsui proposed to sequentially linearize each round of the cipher. The resulting set of linear approximations is called a linear trail. The correlation of a linear trail is computed by using the Pilling-Up Lemma, more precisely, by multiplying the correlations of each 1-round linear approximation.

1.1 Related Work

In [Nyb94] it was first observed that in some cases, there is more than a single linear trail involving the same plaintext and ciphertext bits. The set of all such linear trails, with a fixed set of input and output bits, is called a linear hull. The correlation of a linear hull is computed by summing up all underlying linear trails' correlations. Thus, the correlation of the linear hull may be significantly different from that of any of the underlying trails. When a linear attack is used, both the success rate and the data complexity of the attack are closely related to the hull's correlation and not to that of the trail.

In [AR16], Ashur and Rijmen proved that the linear hull effect can sometimes appear already within a single round of a cipher. All their experiments and key-recovery attacks were applied to the lightweight block cipher SIMON. Following up on this work, Ashur and Posteuca analyzed in [AP18] this phenomenon for the Data Encryption Standard (DES). They showed that under certain constraints, the f-function of DES exhibits 0-correlation key-dependent one-round linear hulls.

1.2 Our Contribution

In this paper we present a new type of linear attack against the full DES and 3DES. The attack uses a 1-round 0-correlation linear hull and embeds it into Matui's 8-round linear trail. This results in a 16-round 0-correlation linear trail for DES and a 48-round linear trail for 3DES, both with correlation zero under certain conditions for particular key bits. We then show how these linear trails can be used for key recovery by exploiting the key-dependent behavior of the correlation.

The contribution of the paper is therefore twofold:

1. We present a new linear trail covering the full DES and 3DES;
2. We show how the key-dependent behavior of a linear trail can be used for key recovery.

To the best of our knowledge, our attack against the full 3DES is the first statistical attack against this cipher, and this paper is the first to ever use a 1-round 0-correlation linear approximation for an attack.

1.3 Structure of this Paper

In section 2, we introduce our notation, revisit some terminology regarding linear cryptanalysis and briefly describe the block ciphers DES and 3DES. In section 3 we introduce 0-correlation linear approximations covering the full DES and 3DES and show how these can be used for key recovery. section 4 concludes the paper and offers future research directions.

2 Notation and Terminology

In this section we introduce the notation used throughout this paper and recall some terminology regarding linear cryptanalysis. We also present the DES and the 3DES ciphers.

2.1 Masks and Approximations

Let a be a binary value of length n and let $a^t x = \bigoplus_{i=0}^{n-1} a_i x_i$, where a_i and x_i are the i^{th} bit of a and x, respectively. We then say that a is the mask of x. Given that applying a mask to a number represents, in essence, a selection of bits of x, we will also use the description of a mask as a set of positions:

$$\bar{x} = \{i_1, i_2, ..., i_v\} \Leftrightarrow \begin{cases} x_j = 1, \forall j \in \{i_1, i_2, ..., i_u\} \\ x_j = 0, \forall j \notin \{i_1, i_2, ..., i_u\} \end{cases}$$

The bits in the positions $\{i_1, i_2, ..., i_v\}$ are called *active bits*, while the remaining bits of x are called non-active bits.

Let $R_k(x) = y$ denote the round function of a block cipher, where x, y and k are the plaintext, the ciphertext and the key, respectively. A linear approximation for R_k is a tuple (α, β, κ), where α, β and κ are the input mask, the output mask and the key mask, respectively. Let p be the probability that the equation $\alpha^t x \oplus \beta^t y \oplus \kappa^t k = 0$ holds, then the correlation of the linear approximation (α, β, κ) is defined as $corr(\alpha, \beta, \kappa) = 2p - 1$. In general, both p and $corr(\alpha, \beta, \kappa)$ are key-dependent (see, e.g., [AÅBL12])

A pair of masks (α, β) is called connectable if and only if β can be obtained from α using the rules of propagation of linear trails introduced in [Bih94,CV94]. Otherwise, the pair (α, β) is called non-connectable.

2.2 Linear Hulls and Trails

An iterated block cipher with r rounds is described as $r-1$ compositions of the round function with itself, $Enc_k = R_{k_{r-i}} \circ ... \circ R_{k_0}$, where k_i denotes the round key. A linear trail covering r rounds of a block cipher is a sequence of linear approximations such that the output mask of round i is the same as the input mask of round $i+1$. Hence, a linear trail can be represented as an $(r+1)$-length vector $(m_1, m_2, ...m_{r+1})$, where (m_i, m_{i+1}) represents the input and output masks at round i, respectively. The correlation of the linear trail is computed by multiplying the correlation of all single-round linear approximations:

$$corr(m_1, ...m_{r+1}) = \prod_{i=1}^{r} corr(m_i, m_{i+1})$$

A linear hull covering r rounds is a pair (α, β) and represents the set of all linear trails such as $m_1 = \alpha$ and $m_{r+1} = \beta$ (i.e., the input and output masks are fixed, but intermediate round masks may vary). The correlation of a linear hull is computed by adding the correlations of all linear trails contained by it:

$$corr(\alpha, \beta) = \sum_{m_1=\alpha, m_{r+1}=\beta} corr(m_1, ...m_{r+1})$$

Following [DGV94], the round function of a block cipher can also be viewed as a composition of its atomic operations. Thus, the methods described above for computing the correlation of a linear trail can also be applied on a smaller scale to these atomic operations. In [AR16], the authors observed that, in some cases, it is possible to construct more than a single linear trail inside the round function by applying the method presented above. Likewise, in [AP18], the authors showed that this is also true for DES' f-function, and hence that the linear hull effect may appear already inside one round of DES. This paper uses the latter observation to attack the cipher.

2.3 The DES Cipher

The Data Encryption Standard (DES) [DES] is a block cipher developed by IBM during the early 1970s and was published as an NBS (now NIST) standard in 1977.

DES uses a Feistel structure with a round function which employs a non-linear function f. The overall structure of DES consists of an initial permutation, 16 enciphering rounds and a final permutation. The plaintext and the key are 64-bit each, even though only 56 out of 64 key-bits are actually used by the algorithm.

The input to the round function is a 48-bit round key (denoted by k) and two 32-bit intermediate cipherwords (denoted by x and y).

The round function of DES is given by:

$$R_k(x, y) = (y \oplus f(x, k), x).$$

The f-function consists of four layers:

1. *The expansion layer*: the 32-bit input x is expanded into a 48-bit output using the *expansion function* described in Table 1. One may notice that after applying the expansion function, 16 out of 32 input bits are used twice. We will use this property in our analysis. In the sequel, we denote the expansion function by E.
2. *Key addition*: the output of the expansion function is XORed with the 48-bit round key;
3. *The substitution layer*: the output of the key addition is divided into eight 6-bit chunks. Each of these blocks is given as an input to a different 6-to-4 S-box, resulting in eight 4-bit outputs. In Table 2 we describe the first two S-boxes used in DES; the remaining six S-boxes can be found in [DES].
   The S-boxes of DES are applied as follows: for input $x_0x_1x_2x_3x_4x_5$, the output after applying the i^{th} S-box is the value found at the intersection of

Table 1: The expansion function E of DES. We see that 16 out of the 32 input bits appear twice.

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

Table 2: DES' first two S-boxes

S_1																
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2																
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

row x_0x_5 and column $x_1x_2x_3x_4$ of the table S_i. We denote the substitution layer by S.

We note that due to the expansion function a single active input bit may influence two consecutive S-boxes. In this paper, we consider the first and the last S-boxes as consecutive ones (i.e., we view the property of being consecutive as circular).

4. *The permutation layer of DES*: a fixed 32-bit to 32-bit permutation is applied to the output of the substitution layer. This permutation, denoted by P, is described in Table 3.

The key schedule The key schedule of DES is a linear function where the round keys are basically obtained by selecting 48 out of the 56 bits of the master key. For the key schedule we refer the interested reader to [DES].

Decryption Since DES has a Feistel structure, the decryption function, DES^{-1}, uses the same structure as the encryption, but with the keys used in reverse order.

Table 3: The Permutation Layer of DES

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

2.4 The 3DES Cipher

Due to an increase in computation power over the years, a 56-bit key is deemed two short for modern applications. The block cipher 3DES represents a simple solution to increase the key size while avoiding the need to design a completely new block cipher. 3DES performs three iterations of DES, using different and independent keys, more precisely:

$$3DES = DES_{K_1} \circ DES^{-1}_{K_2} \circ DES_{K_3}$$

where K_1, K_2 and K_3 denote the master keys of each application of DES.

2.5 One-Round Key-Dependent Linear Hulls in DES

Following [AP18] a linear trail on the f-function of DES is described by a tuple $(\alpha, \beta, \kappa, \tau, \lambda, \gamma)$, where α, β, κ are the input mask, the output mask and the key mask, respectively. The remaining components of the tuple represent the intermediate masks of the trail: τ is the output mask of the expansion layer, λ and γ are the input and the output mask of the substitution layer, respectively.

Given the manner in which the S-boxes are applied, in order to better describe a linear trail, we consider λ and γ as a concatenation of 8 components of the same size. For example, the input mask $\lambda = (\lambda_1, ..., \lambda_8)$ is viewed as a concatenation of 6-bit components and the output mask $\gamma = (\gamma_1, ...\gamma_8)$ is viewed as a concatenation of 4-bit components.

Figure 1 depicts the propagation of linear masks through the f-function of DES.

The rules of propagation for linear masks (e.g., as described in [Mat93,Bih94, AP18]) impose a series of constraints on the masks of a one-round linear trail:

1. τ, κ and λ must all be the same;
2. each pair (λ_i, γ_i) must represent a connectable pair of input-output masks for the i^{th} S-box, more precisely, the linear approximation table (LAT) of S_i must contain a non-zero value at the intersection of λ_i and γ_i;
3. $\beta = P(\gamma)$.

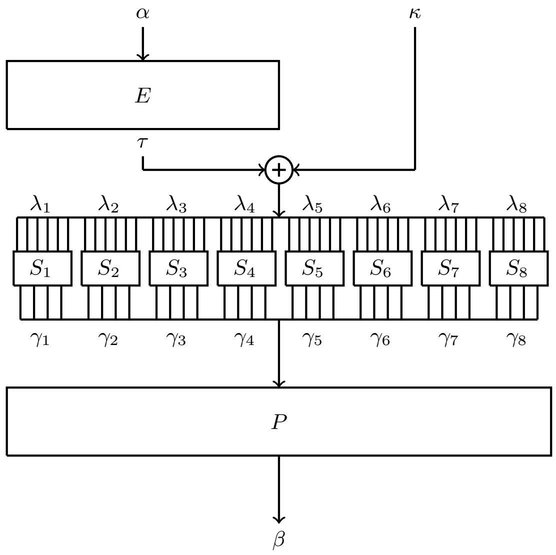

Fig. 1: A linear trail through the f-function of DES

Definition 1. *S_i is an active S-box if and only if the input and the output masks are nonzero, more precisely $\lambda_i, \gamma_i \neq 0$.*

Per [AP18], in the case of DES the linear hull effect may appear within one round if at least one pair of adjacent S-boxes is active. In this paper, we also consider the pair (S_8, S_1) as a pair of adjacent S-boxes.

Observation 1. Given the constraints imposed by the rules of propagation for linear masks, two trails that are contained in the same hull (α, β) have the form $(\alpha, \beta, \tau_i, \tau_i, \tau_i, P^{-1}(\beta))$, where P^{-1} represents the inverse of the permutation layer. Thus, the only difference between two trails in the same 1-round linear hull is given by the mask τ. Given that each trail has a different mask after applying the expansion layer, the key masks will also be different, leading to the hull's correlation being key-dependent.

2.6 Zero-Correlation Linear Approximations

Due to the existence of the linear hull effect, different linear trails may interfere with each other, influencing the correlation of the hull in a constructive or destructive manner or, in some cases, even canceling out each other completely. In the latter case, the correlation of the hull will be strictly zero.

An example of a one-round linear hull containing four linear trails was described in [AP18], the correlation of each of these trails having the same absolute value. One can notice that for some particular values of the key, two linear trails can have a positive correlation, while the other two have a negative one. In this case, the value of the hull's correlation will be strictly zero.

In the remaining of this paper we will use the label "poisonous round" for a one-round linear hull that leads, under some particular key values, to a zero correlation. A trail containing at least one "poisonous" round is called a "poisonous trai".

Recall that in order to compute the correlation of a trail, the Piling Up Lemma is used and the individual round correlations are multiplied. The term "poisonous" is used to emphasize that a single "bad" approximation (i.e., a 0-correlation approximation) in a certain round "spoils" this product, resulting in 0-correlation trail.

3 Attacking DES and 3DES

In [Mat93], Matsui presented a linear approximation of the full DES, obtained by using an 8-round iterative linear trail with correlation $2^{-12.71}$. By replacing the linear masks of the first and the last round with locally better ones, a 16-rounds linear approximation with correlation of $2^{-22.42}$ is obtained.

In this section we introduce a new linear trail for DES, containing a key-dependent poisonous round. This linear trail is obtained by replacing the last two rounds in Matsui's iterative trail, where the last round is the poisonous one. This new linear approximation allows to take advantage of the key constraints that are imposed by the poisonous round, thus leading to a key-recovery attack.

3.1 A 2-Round Poisonous Trail for DES

We now introduce a 2-round poisonous trail for DES where the second round of the trail is a poisonous round. Given that the correlation of a linear trail is obtained by multiplying the correlations of each one-round linear approximation, the correlation of the trail described below depends on the correlation of the last round's linear approximation.

To obtain the poisonous round, we used a 1-round linear hull for the f-function of DES. This hull is defined by the input-output masks pair (`0x01CF8000`, `0x00011000`). This hull contains four linear trails of the form

$$(\texttt{0x01CF8000}, \texttt{0x00011000}, \tau_i, \tau_i, \tau_i, \texttt{0x0044000})$$

having S_3 and S_4 as adjacent active S-boxes. The value of τ_i, the correlation of each of these trails and the key bits involved in the computation of the correlation are described in Table 4. The round key has 48 bits, the most significant bit of the key is denoted by k_0 and the least significant key bit by k_{47}.

As always, the correlation of a single trail is computed by multiplying the correlations of each atomic operation of the round function. Given that the expansion layer and the permutation are linear functions, the correlation between their inputs and outputs is 1. For the substitution layer, the correlation

Table 4: The trails within the hull (0x01CF8000, 0x00440000) of the f-function of DES

Trail No.	τ_i	Correlation	Key masks
Trail 1	(0, 0, 0x39, 0x0F, 0, 0, 0, 0)	$2^{-8} \cdot 5$	$\{12, 13, 14, 17, 20, 21, 22, 23\}$
Trail 2	(0, 0, 0x3B, 0x2F, 0, 0, 0, 0)	$2^{-8} \cdot 5$	$\{12, 13, 14, 16, 17, 18, 20, 21, 22, 23\}$
Trail 3	(0, 0, 0x38, 0x1F, 0, 0, 0, 0)	$2^{-8} \cdot 12$	$\{12, 13, 14, 19, 20, 21, 22, 23\}$
Trail 4	(0, 0, 0x3A, 0x3F, 0, 0, 0, 0)	$-2^{-8} \cdot 2$	$\{12, 13, 14, 16, 18, 19, 20, 21, 22, 23\}$

is given by the LAT's of each active S-box. The correlation of the key addition is $(-1)^{\bigoplus_{i \in \kappa} k_i}$, for k_i's corresponding to the positions of the key mask. The correlations described in Table 4 overlook this key contribution.

Given that the correlation of the hull is computed by summing the correlation of the four trails, the key bits in positions $k_{12}, k_{13}, k_{14}, k_{20}, k_{21}, k_{22}$, and k_{23} (i.e., the key bits shared among all 1-round trails) influence the sign of the correlation, while the key bits in positions k_{16}, k_{17}, k_{18}, and k_{19} (i.e., the key bits defining the individual 1-round trails) influence its magnitude.

The correlation of the hull, depending on the values of the round key, is:

$$corr = \begin{cases} \pm 2^{-8} \cdot 14 & k_{16} \neq k_{18} \\ \pm 2^{-8} \cdot 20 & k_{16} = k_{18} \text{ and } k_{17} = k_{19} \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

In order to connect it to Matsui's trail we extended this 1-round linear hull into a 2-rounds linear trail, where the input mask is one of the masks used in Matsui's trail. The 2-round linear trail is described in Figure 2.

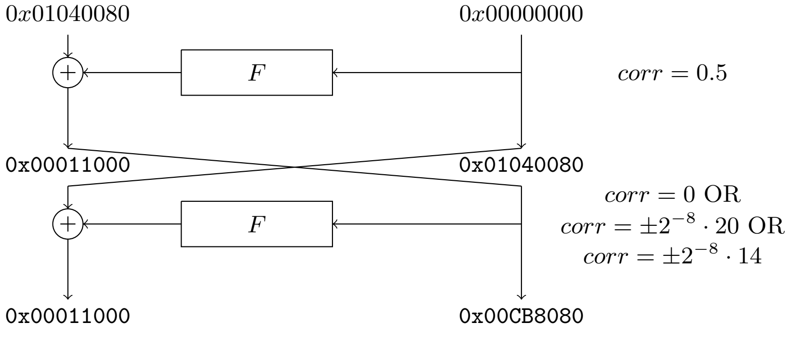

Fig. 2: A 2-round poisonous trail of DES. The last round is the poisonous one.

The correlation for the trail described above, depending on the values of the second round key, is:

$$corr = \begin{cases} \pm 2^{-9} \cdot 14 & k_{16} \neq k_{18} \\ \pm 2^{-9} \cdot 20 & k_{16} = k_{18} \text{ and } k_{17} = k_{19} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

3.2 A Poisonous Trail for DES Based on Matsui's 8-Round Iterative Linear Approximation

We now recall the 8-round iterative linear trail introduced by Matsui in [Mat93] and adapt it into a poisonous trail by replacing two of its rounds with the trail described in subsection 3.1.

Since Matsui's 8-round trail is iterative, it can start in any of the trail rounds and extend naturally for the next 7 rounds. Figure 3 depicts Matsui's 8-round iterative linear trail when circularly moved down by 2 rounds such that the last round of the original trail is now the second round.

Given that the last round of the new trail is a poisonous one, the correlation of the 16-round trail depends on the bits in positions 16, 17, 18 and 19 of the last round key. Taking into account the key schedule of DES, the value of the correlation depends on the bits on positions 51, 0, 1 and 8 of the master key, such as:

$$corr = \begin{cases} \pm 2^{-24.95} & k_{51} \neq k_{1} \\ \pm 2^{-24.42} & k_{51} = k_{1} \text{ and } k_{0} = k_{8} \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

We note that now the last two rounds of the trail presented in Figure 3 have the smallest correlation, and that our 2-round trail from subsection 3.1 has the same input mask. Thus, by replacing the last two rounds with our 2-round poisonous trail we improve the correlation. Whereas the correlation of the two rounds that we just replaced was 0.01953125, the new 2-round trail has a correlation that is 1.38 times better (for some keys).

3.3 Distinguishing between the Three Correlations

A naive approach to executing this attack is to encrypt the entire codebook. In this case, the expected correlation and the empirical one are the same. However, in the case of DES, encrypting 2^{64} plaintexts is more expensive than recovering the key using an exhaustive search. However, as we see in [Mat93] a more efficient way is to use a sample of the codebook to detect the correlation. Generally speaking, to detect a correlation c, an adversary needs to encrypt roughly $2 \cdot c^{-2}$ plaintexts.

Taking into account that the smallest non-zero correlation of the trail is $2^{-24.95}$, in order to distinguish between the three correlations we need to encrypt

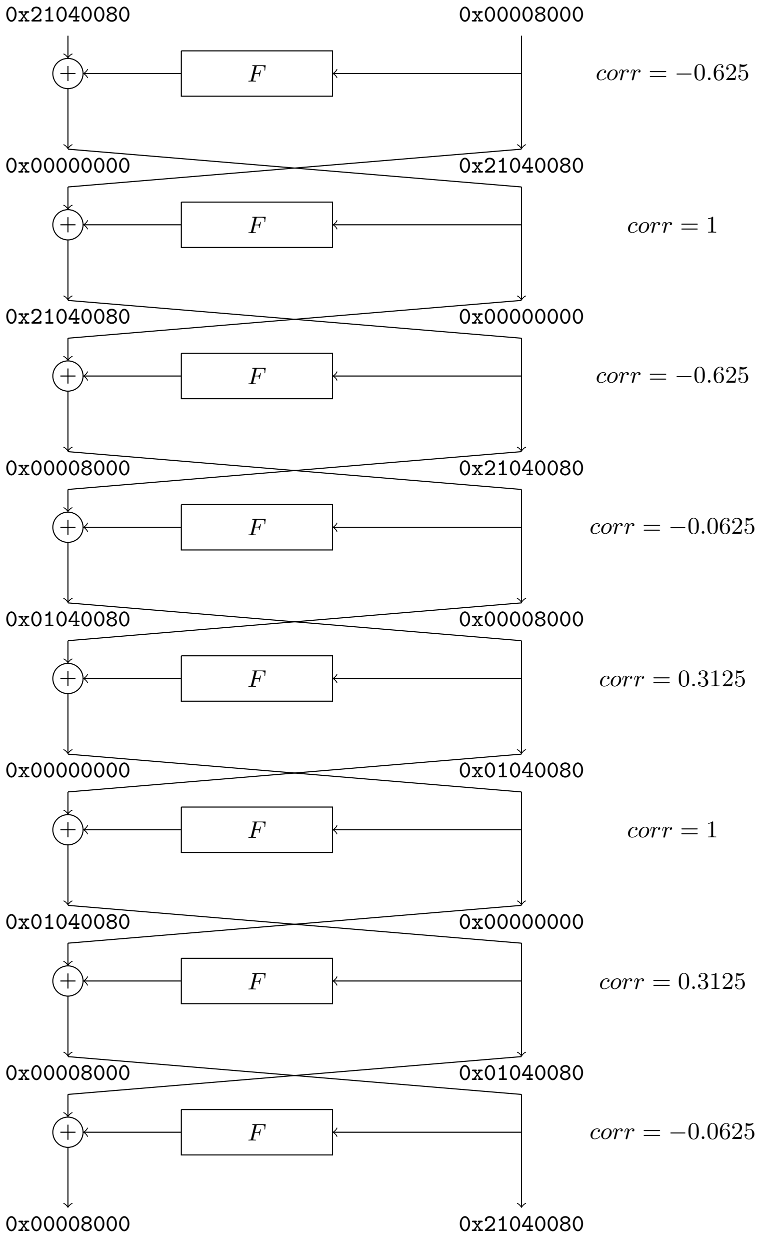

Fig. 3: Matsui's 8-round iterative linear approximation circularly moved with 2 rounds

$2^{50.9}$ random plaintexts.[1] We then compare the empirical correlation we obtained to each of the three expected correlations.

If the correlation is different from zero, the empirical correlation will be close to the expected one, making it easy to identify the right case. For the case of correlation zero, the empirical correlation will be close to the inverse of the squared root of the number of plaintexts that were used. For example, for a data complexity of $2^{50.9}$ the empirical correlation will be close to $2^{-25.45}$. In subsection 3.6 we present an experimental verification on reduced round versions of DES.

3.4 Key Recovery Attack on DES

We now propose a key-recovery attack based on the linear approximation described in subsection 3.2. Since the correlation depends on the values of k_0, k_1, k_8, and k_{51} of the master key, we can infer a relation between these key bits just by looking at the correlation of the trail.

In order to launch an attack, we need a set of $2^{50.9}$ plaintexts and their corresponding ciphertexts, encrypted under a fixed, secret key. We compute the correlation of the trail described above and compare the empirical correlation to each of the three expected values. The expected correlation that is the closest to the empirical correlation indicates the key constraints that are met by the master key. For example, if the correlation is closest to $2^{-24.95}$, then the key satisfies the constraint $k_{51} \neq k_1$.

3.5 Extending the Attack to 3DES

The attack presented above can be trivially extended to the full 3DES. The extension works by concatenating Matsui's iterative trail onto itself three times. This results in a linear trail covering all 48 rounds of 3DES with correlation $2^{-76.26}$. By replacing the last two rounds in a similar manner to what we did in subsection 3.2, we create a key dependent behavior. However, this time, rather than distinguishing between 3 correlations as we did in subsection 3.4, we distinguish between two possible outcomes: either the empirical correlation is strictly zero due to the linear hull effect, or it is not. When computed over the whole codebook, the sample correlation has 0-variance and the empirical correlation coincides with the expected one resulting, in this case, in $\hat{c} = 0$. In the other case (i.e., when the expected correlation is different from 0 since the key constraints were not met), the behavior of the empirical correlation is similar to other linear attacks where not enough data was used: the empirical correlation follows some normal distribution around the expected correlation.

The attack procedure then works as follows: for a given key, encrypt all possible 2^{64} plaintexts and compute the empirical correlation $\hat{c}$. If $\hat{c} = 0$ then

[1] We note that using $c^{-2}, 4 \cdot c^{-2}$, or $8 \cdot c^{-2}$ lead to different success probabilities for the attack. For simplicity, we use $2 \cdot c^{-2}$ but the result can trivially be extended when more or less data is used.

the key-conditions were met and we conclude that for the last master key of 3DES, $k_{51} = k_1$ and $k_0 \neq k_8$; otherwise, the key constraints were not met and we conclude that the last master key satisfies one of the following properties $k_{51} \neq k_1$ or $k_{51} = k_1$ and $k_0 = k_8$.

This attack requires 2^{64} time and data and recovers a single bit of the key. Variants of this distinguisher (e.g., by setting different rounds to be covered by the 1-round 0-correlation linear hull) can be used to recover other key bits. To the best of our knowledge, this is the first statistical attack against the full 3DES.

3.6 Experimental Verification

We performed a series of experiments in order to test the validity of our analysis. Since the data needed to execute the attack on all 16-round trail is too high (i.e., $2^{-50.9}$), we performed our experiments on round-reduced versions of the trail. Therefore, our experiments targeted up to 9 rounds of the trail where all our round-reduced trails having the same, poisonous, last round.

For each experiment we chose a master key that satisfies one of the key constraints imposed by the poisonous round. We then computed the correlation of the round-reduced trail with the appropriate amount of data. The empirical correlation was always very close to the expected one, thus supporting our hypothesis.

In Table 5 we present the results of our experiments on a trail covering 9 rounds using 2^{38} data. The expected correlation of the trail, depending on the bits of the 9^{th} round key is:

$$corr = \begin{cases} \pm 2^{-16.245} & k_{16} \neq k_{18} \\ \pm 2^{-15.714} & k_{16} = k_{18} \text{ and } k_{17} = k_{19} \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

The smallest non-zero correlation of trail is $2^{-16.245}$, thus the minimum amount of data needed is 2^{35}. We chose to use 2^{38} to improve the significance of the results. The weight of the expected and the empirical correlations are given in Table 5.

Table 5: Experimental results of the last 9 rounds from the trail presented in subsection 3.2

Expected correlation	Empirical correlation	Key constraint on RK_9
$-\infty$	-18.608	$k_{16} = k_{18}$ and $k_{17} \neq k_{19}$
-16.245	-16.055	$k_{16} \neq k_{18}$
-15.714	-15.631	$k_{16} = k_{18}$ and $k_{17} = k_{19}$

3.7 Discussion

Matsui's linear attack against DES, and especially Algorithm 1, assumed that the linear hull effect does not apply to DES and that only a single trail underlies the linear hull. In fact, a similar assumption often appears in other works using linear cryptanalysis. The assumption is that the linear hull consists of only a single trail, or alternatively, that it consists of a dominant trail and that the other trails can be treated as noise.

In subsection 3.6 we presented a 9-round experimental verification for our distinguisher. As can be seen in Table 5, while the empirical correlations are indeed "close enough" to their expected values, they are not quite the same. These small differences may be ignored as sample error (see also [BT13]) but they may also mean that another trail exists within Matsui's hull. As per Ashur and Rijmen in [AR16] ignoring some of the linear trails inside the linear hull leads to an over- or under-estimation of the expected correlation, leading in turn to a different success probability than what the adversary expects.

We stress that our attack uses the same assumptions as the ones used in Matsui's original attack: if indeed only a single trail underlies the linear hull, then both Matsui's and our attack work as advertised; if one or more trails exist and are being ignored, both attacks still work, but the success probability differs from what is advertised; if more than a single trail exists, and all trails are known, the attack can recover more key bits than advertised.

4 Conclusion

In this paper we extended the work presented in [AP18] by designing 0-correlation key-dependent linear trails that cover more than a single round of DES. First, we presented a 2-round linear approximation where the last round may have correlation 0, depending on the key. We showed how to connect these two rounds to Matsui's trail, resulting in 0-correlation key-dependent trails covering the full DES and 3DES ciphers. Finally we proposed new key-recovery attacks on DES and 3DES using the trails introduced in this paper.

The work described can be extended in different directions. For example, it will be interesting to identify other block ciphers that exhibit "poisonous" linear trails and revisit, if exists, the linear attacks published against them. It also remains to be investigated if and how the attacks presented in this paper can be improved in term of both data and time complexity. Future research should also consider the extension of these attacks to the case of multiple linear cryptanalysis.

5 Acknowledgements

The authors would like to thank Vincent Rijmen for all the useful discussions and ideas and to Lars Knudsen whose question sparked the authors' interest in this line of research.

References

AÅBL12. Mohamed Ahmed Abdelraheem, Martin Ågren, Peter Beelen, and Gregor Leander. On the distribution of linear biases: Three instructive examples. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 50–67. Springer, 2012.

AP18. Tomer Ashur and Raluca Posteuca. On linear hulls in one round of DES. *IACR Cryptology ePrint Archive*, 2018:635, 2018.

AR16. Tomer Ashur and Vincent Rijmen. On linear hulls and trails. In Orr Dunkelman and Somitra Kumar Sanadhya, editors, *Progress in Cryptology - INDOCRYPT 2016 - 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings*, volume 10095 of *Lecture Notes in Computer Science*, pages 269–286, 2016.

BCQ04. Alex Biryukov, Christophe De Cannière, and Michaël Quisquater. On multiple linear approximations. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 1–22. Springer, 2004.

Bih94. Eli Biham. On matsui's linear cryptanalysis. In *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, pages 341–355, 1994.

BR11. Andrey Bogdanov and Vincent Rijmen. Zero-correlation linear cryptanalysis of block ciphers. *IACR Cryptology ePrint Archive*, 2011:123, 2011.

BR14. Andrey Bogdanov and Vincent Rijmen. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. *Des. Codes Cryptography*, 70(3):369–383, 2014.

BT13. Andrey Bogdanov and Elmar Tischhauser. On the wrong key randomisation and key equivalence hypotheses in matsui's algorithm 2. In Shiho Moriai, editor, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 19–38. Springer, 2013.

CV94. Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In Santis [San95], pages 356–365.

DES. Fips publication 46-3, data encryption standard (des).

DGV94. Joan Daemen, René Govaerts, and Joos Vandewalle. Correlation matrices. In Bart Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 275–285. Springer, 1994.

JR94. Burton S. Kaliski Jr. and Matthew J. B. Robshaw. Linear cryptanalysis using multiple approximations. In Yvo Desmedt, editor, *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, volume 839 of *Lecture Notes in Computer Science*, pages 26–39. Springer, 1994.

Mat93. Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.

Nyb94. Kaisa Nyberg. Linear approximation of block ciphers. In Santis [San95], pages 439–444.

San95. Alfredo De Santis, editor. *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, volume 950 of *Lecture Notes in Computer Science*. Springer, 1995.