# How Biased Are Linear Biases

Adnan Baysal and Orhun Kara

***Abstract*—In this paper we re-visit the Matsui's linear cryptanalysis. The linear attack on the full round DES was the first attack that has been verified experimentally. Matsui extended one-round linear approximations to a linear mask of plaintext-ciphertext pairs by means of his piling-up lemma. The assumption of the lemma, the independence of the random variables in the round approximations, is hopefully fulfilled for the full round DES. So the experiment was successful. However, there exist some ciphers whose linear approximations may have completely different biases than those calculated by the piling-up lemma. We work out a case study where the biases of the linear approximations cannot be calculated through the lemma. We derive the theoretical infrastructures which lead us to compute the overall bias. We verify the theoretical results by performing some experiments on a toy cipher. For the verification, we mount a linear attack on the cipher and construct two linear approximations having the same plaintext-ciphertext masks. We show that the biases of the approximations are different from what the piling-up lemma asserts.**

***Index Terms*—block cipher, linear cryptanalysis, nonlinearity, DES, linear hull, linear approximation**

## I. Introduction

Matsui's linear cryptanalysis is the second successful attack on the full round DES, exploiting the biases of the linear approximations between plaintext, ciphertext and key bits [12]. These linear approximations are constructed by extending one-round linear approximations whose input-output masks cancel out one by one so that there is no interior variable left in the combined linear approximation. Matsui introduces the piling-up lemma to compute the overall bias of the combined linear approximation.

The piling-up lemma works when the random variables in the linear approximations are independent. It is interesting to see that this condition is not fulfilled for all ciphers. Hopefully, Matsui has shown experimentally that his approximations work for an arbitrary key on DES [13].

In this paper, we examine the Matsui's linear cryptanalysis. We construct a set of random variables and calculate the biases between them. We divide the random variables into two sets and assume that any two distinct variables in different sets are independent. On the other hand, the random variables in one set are equal to each other with certain probabilities, and hence we can construct a linear approximation for each set. We compute the biases for the approximations. We show that the biases are not equal to the biases computed by the piling-up lemma even though the random variables are independent. We design a toy cipher and construct two linear approximations for the cipher whose random variables act in accordance with the model we introduce. Finally, we calculate the biases experimentally and verify our theoretical results.

The paper is organized as follows: In Section II, we give a brief overview of the linear cryptanalysis and show how it is mounted on DES. Also, we depict a high level description of DES in this section. We introduce the notion of hull effect and the related works on the hull effect in Section III. In Section IV we describe our case study and give the theoretical infrastructure. We verify the theoretical results by performing some experiments in Section V. Finally we conclude the paper with section VI.

Manuscript received March 26, 2012.

Adnan Baysal and Orhun Kara are with TÜBİTAK BİLGEM Gebze, 41470 Kocaeli Turkey, e-mails: {abaysal,orhun}@uekae.tubitak.gov.tr

## II. An Overview of Linear Attack on DES

Linear attack is one of the most effective cryptanalysis methods on block ciphers. The first, and maybe the most prominent sample of the method is the attack mounted on DES by Matsui [12]. Matsui show that the full round DES is vulnerable to the linear cryptanalysis if the attacker has $2^{47}$ known plaintexts. He also conducted an experiment and implemented the attack successfully [13], verifying his results related to attack complexities and success rates.

The linear cryptanalysis exploits the biased equations between linear combinations of certain plaintext bits and ciphertext bits. Consider a linear equation of the form

$$\begin{aligned} &P[i_1] \oplus \cdots \oplus P[i_m] \oplus C[j_1] \oplus \cdots \oplus C[j_s] \\ &= K[l_1] \oplus K[l_2] \oplus \cdots \oplus K[l_t] \end{aligned} \quad (1)$$

where $P[i]$, $C[i]$ and $K[i]$ are the $i$-th bits of the plaintext, the ciphertext and the key respectively. The operation $\oplus$ is the XOR operation. Let Equation 1 be satisfied with a probability $\frac{1}{2} + \epsilon$. Matsui introduces an algorithm which he calls "Algorithm 1" to reveal one bit information of the key. Assume that $\epsilon > 0$.

If the number of plaintext-ciphertext pairs which make the left hand side of Equation 1 equal to 0 is more than half of all the plaintext-ciphertext pairs then we conclude that

$$K[l_1] \oplus K[l_2] \oplus \cdots \oplus K[l_t] = 0.$$

Otherwise, that is, if the number of plaintext-ciphertext pairs where the right half Equation 1 is equal to 1 is more than half of the all the plaintext-ciphertext pairs, then,

$$K[l_1] \oplus K[l_2] \oplus \cdots \oplus K[l_t] = 1.$$

If the bias, $\epsilon$, is negative, Algorithm 1 complements the results above.

Algorithm 1 retrieves one bit of information from the key which is the value of the linear combination

$$K[l_1] \oplus K[l_2] \oplus \cdots \oplus K[l_t].$$

The success rate depends on the data complexity. It is given as

$$\int_{-2\sqrt{N}|\epsilon|}^{\infty} \frac{1}{\sqrt{2\pi}} \exp(-x^2/2)dx$$

where $N$ is the number of the plaintexts and exp is the Euler function. Let us remark that this success rate is almost one when $N$ is proportional to $\epsilon^{-2}$. For instance, when $N \approx \epsilon^{-2}$ the success rate is around 98 %.

For a given cipher, one of the natural questions is how to find equations of the form given in Equation 1, if such equations exist with significant biases. Matsui answered this question in the case of DES and found a linear characteristic with a bias of $\epsilon = -1,49 \cdot 2^{-24}$ for the 16-round DES. To find such a characteristic, Matsui analyzed the "nonlinearity degree" of the S-boxes of DES. He introduced the following definition to measure how nonlinear an S-box is [12]:

*Definition 1:* Let $S$ be an S-box of $n$-bit input, $m$-bit output. For a given $\alpha \in GF(2)^n$ and $\beta \in GF(2)^m$, define the number $N_S(\alpha, \beta)$ as the number of times out of $2^n$ inputs such that an XORed value of the input bits masked by $\alpha$ is equal to an XORed value of the output bits masked by $\beta$. In other words,

$$N_S(\alpha, \beta) = |\{x| \oplus_{i=0}^{n} x[i] \cdot \alpha[i] = \oplus_{j=0}^{m} S(x)[j] \cdot \beta[j]\}|$$

where $\cdot$ is bitwise AND operation.
The values $N_S(\alpha, \beta)$ are expected to be around $2^{n-1}$ for a highly nonlinear S -Box. Otherwise, there are some $\alpha$ masks in the input and $\beta$ masks in the output such that the linear equation given by $N_S(\alpha, \beta)$ would be highly biased, that is, the absolute value of its bias, say $\epsilon$, is quite larger than 0. For instance, the fifth S-Box of DES satisfies $N_{S_5}(16, 15) = 12$ among all the 64 input patterns. That is, the fourth input bit of the S-Box is equal to the sum of all the output bits with a probability $\frac{1}{2} - \frac{20}{64}$ if the input is random.

### A. A Brief Description of DES

DES is one of the most famous block ciphers which has been used worldwide prevalently since 1976. It can be considered as the ancestor of all the modern block ciphers. DES has 64-bit block length and 56-bit key length. It is a Feistel network. That is, the plaintext is divided into two equal part, say the left half and the right half, and then the output of right part through the round function $F$ is XOR'ed to the left part. Then the left and right parts are swapped. This procedure is repeated 16 times where a different round key is incorporated into the round function $F$ in each round.

The round function $F$ first expands the 32-bit input, which is the right part of the internal state, to 48-bit value and then this expansion is XOR'ed with the current round key. The eight $6 \times 4$-bit S-Boxes are then applied. The S-Box outputs are permuted bitwise by a particular permutation to constitute the 32-bit output of the $F$ function. The Feistel structure of DES is depicted in Figure 1.

### B. Linear Cyptanalysis of DES

Matsui introduced several linear characteristics for certain number of rounds of DES. In this section we give one of them. The method to find an input/output mask with a biased equation is to extend the biased linear approximations of $F$ to the full cipher. For example, if $X, K$ are the data and the key inputs to the DES Feistel function $F$, then it is given in [12] that;

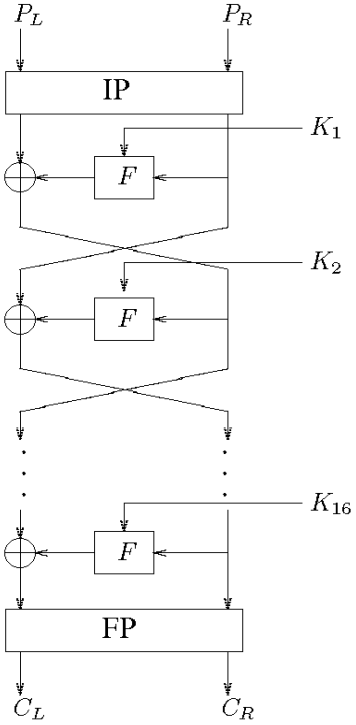


Fig. 1. Feistel structure of DES.

$$A : X[15] \oplus F(X, K)[7, 18, 24, 29] = K[22]$$

with a probability of $\frac{1}{2} - \frac{20}{64}$ due to the fifth S-box of $F$ since $N_{S_5}(16, 15) = 12$. Another one-round characteristic can be given as

$$B : X[27, 28, 30, 31] \oplus F(X, K)[15] = K[42, 43, 45, 46]$$

with a probability $\frac{1}{2} - \frac{10}{64}$. Remark that this one-round approximations is valid for any round so we can construct a linear approximation for several rounds by combining one round approximations like the examples above. A linear approximation for 5-round DES which uses the approximations above is depicted in Figure 2.

Matsui introduced a lemma, piling-up lemma, to compute the bias of the new linear approximation obtained by combining one-round approximations. It is given as

*Lemma 1:* Let $X_i$ be independent random variables for $1 \leq i \leq n$. Let $\Pr(X_i = 0) = \frac{1}{2} + \epsilon_i$. Then

$$\Pr(\oplus_{i=1}^{n} X_i = 0) = \frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} \epsilon_i.$$

Using the piling-up lemma and the 1-round characteristics $A$ and $B$, as in the 5-round characteristic depicted in Figure 2, we get;

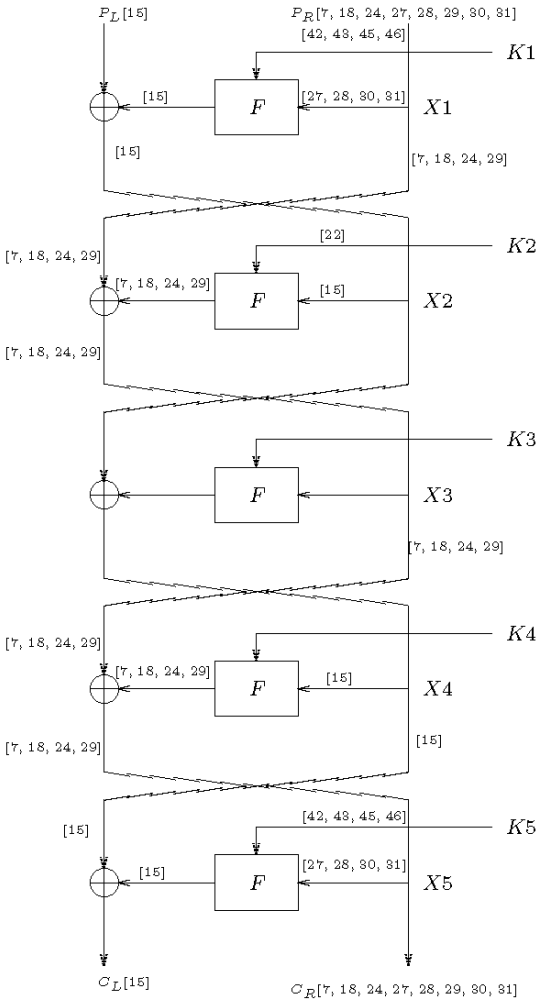


Fig. 2. A five round linear characteristic for DES using above approximations, in the $BA - AB$ form.

$$X_1[27,28,30,31] \oplus F(X_1,K_1)[15] = K_1[42,43,45,46], \epsilon_1$$
$$X_2[15] \oplus F(X_2,K_2)[7,18,24,29] = K_2[22], \epsilon_2$$
$$X_4[15] \oplus F(X_4,K_4)[7,18,24,29] = K_4[22], \epsilon_3$$
$$X_5[27,28,30,31] \oplus F(X_5,K_5)[15] = K_5[42,43,45,46], \epsilon_4$$

Here $\epsilon_i$'s are the biases of each equation and by $A$ and $B$, $\epsilon_1 = \epsilon_4 = -\frac{10}{64}$, and $\epsilon_2 = \epsilon_3 = -\frac{20}{64}$. Using the fact that $X_1 = P_R$, $X_2 = F(X_1,K_1) \oplus P_L$ and for $i \geq 1, X_{i+2} = X_i \oplus F(X_{i+1},K_{i+1})$, we can eliminate the intermediate values at these equations and finally get

$$\begin{aligned} P_L[15] \oplus P_R[7,18,24,27,28,29,30,31] \oplus \\ C_L[15] \oplus C_R[7,18,24,27,28,29,30,31] = \\ K_1[42,43,45,46] \oplus K_2[15] \oplus \\ K_4[15] \oplus K_5[42,43,45,46] \end{aligned} \quad (2)$$

where Equation 2 has bias approximately equal to $2^{-5.71}$. Using this 5-round characteristic and $2^{12}$ plaintext-ciphertext pair, one can recover the right hand side of the Equation 2 with the success probability equal to almost one, using Algorithm 1.

One discussion has been raised about the assumption of Matsui's piling-up lemma. It is a question that the random variables in the one-round linear approximations may not be independent. Hence the actual bias may be quite different than the calculated bias by the piling-up lemma. For example, Selçuk noted for some Feistel networks that, some biases calculated by the piling-up lemma can be quite different than those derived by the experimental results [1].

The independence of the variables in the linear approximations has been studied well. However, the stability of the probabilities for one-round approximations after plunging in the cipher is not examined.

## III. Linear Hull

The definition of approximate linear hull ($ALH$), or simply linear hull, was first introduced by Nyberg [9]. Linear hull appears in the case that there are multiple linear characteristics with the same data mask but different key masks. The opposite of this idea, i.e. benefiting from linear approximations with different data masks and the same key mask (multiple linear approximations) is explained and applied in [2], [3], [4] and [5]. The idea of multiple linear approximations is further improved by Hermelin, Cho, and Nyberg in [10] and [11], and their attack is called as Multidimensional Linear Cryptanalysis.

In [14], Murphy claimed that there is no linear hull effect in the linear cryptanalysis. But, Leander later proved that the linear hull does indeed effect the security of a cipher, and thus should always be taken into account [7]. In his work, Leander claims that calculating the average time complexity of a linear characteristic by using the average over all keys is not appropriate since this average is usually infinite (due to the case that there is at least one key with zero bias). He claims that one should take into account of the median of the complexities to prove the security against linear cryptanalysis [7].

Assume we analyze a block cipher in which there is a linear hull with two linear characteristics whose biases are dominating (i.e other characteristics have negligible biases). Since the input bits (plaintext bits) of these characteristics are the same, there must be a function (such as an S-box) $F$ whose input masks for those characteristics are the same, whereas the output masks are different. Similarly, starting from the ciphertext and going backwards, necessarily there is a function $G$ such that the input masks differ and output masks are the same. Consider a scenario in which there is only one such $F$ and $G$. Also, assume that the linear approximations between these functions are independent. Calling this middle part $U$, we get the model in Figure 3.

For Figure 3, we can assume that the only key difference of the characteristics is caused by the part $U$. Depending on the actual key values which affects this difference, the overall bias of the model changes. The reason behind this effect is studied theoretically in Section IV and practically verified in Section V.

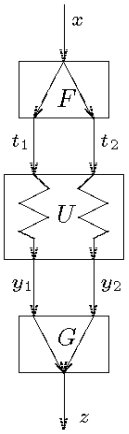


Fig. 3. An example scenario of a linear hull. $x, t_1, t_2, y_1, y_2$ and $z$ represent 1-bit masked values.

## IV. A Case Study

In this section, we define some random variables and the relations between these variables. Then we derive some statements in order to use for the construction of certain linear approximations which are affecting each other. The variables and probabilities are constructed in order to have a better understanding of the linear hull structure depicted in Figure 3.

Let $x, y_1, y_2$ and $z$ be binary random variables. Then

*Proposition 1:* Assume $\Pr(x = y_1) = \frac{1}{2} + \epsilon$ and $\Pr(x = y_2) = \frac{1}{2} - \epsilon$ for some $\epsilon > 0$. Assume also that these events are independent. If $\Pr(z = y_1 | y_1 \neq y_2) = \frac{1}{2}$ which is independent of $x$ and $\Pr(z = y_1 | y_1 = y_2)$ is also independent of $x$, then we have $\Pr(z = x) = \frac{1}{2}$.

*Proof:* The probability $\Pr(x = z)$ is given as

$$\begin{aligned}
&\Pr(x = z | x = y_1 \text{ and } x = y_2) \Pr(x = y_1 \text{ and } x = y_2) \\
+&\Pr(x = z | x = y_1 \text{ and } x \neq y_2) \Pr(x = y_1 \text{ and } x \neq y_2) \\
+&\Pr(x = z | x \neq y_1 \text{ and } x = y_2) \Pr(x \neq y_1 \text{ and } x = y_2) \\
+&\Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) \Pr(x \neq y_1 \text{ and } x \neq y_2).
\end{aligned}$$

On the other hand we assume that the events $x = y_1$ and $x = y_2$ are independent. Hence the probability $\Pr(x = z)$ will be equal to

$$\begin{aligned}
&\Pr(x = z | x = y_1 \text{ and } x = y_2) \Pr(x = y_1) \Pr(x = y_2) \\
+&\Pr(x = z | x = y_1 \text{ and } x \neq y_2) \Pr(x = y_1) \Pr(x \neq y_2) \\
+&\Pr(x = z | x \neq y_1 \text{ and } x = y_2) \Pr(x \neq y_1) \Pr(x = y_2) \\
+&\Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) \Pr(x \neq y_1) \Pr(x \neq y_2).
\end{aligned}$$

We have

$$\begin{aligned}
&\Pr(x = z | x = y_1 \text{ and } x \neq y_2) \Pr(x = y_1) \Pr(x \neq y_2) \\
+\ &\Pr(x = z | x \neq y_1 \text{ and } x = y_2) \Pr(x \neq y_1) \Pr(x = y_2). \\
=\ &(\frac{1}{2} + \epsilon)^2 (\Pr(x = z | x = y_1 \text{ and } x \neq y_2) \\
+\ &(\frac{1}{2} - \epsilon)^2 (\Pr(x = z | x \neq y_1 \text{ and } x = y_2))
\end{aligned}$$

and

$$\begin{aligned}
&\Pr(x = z | x = y_1 \text{ and } x = y_2) \Pr(x = y_1) \Pr(x = y_2) \\
+\ &\Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) \Pr(x \neq y_1) \Pr(x \neq y_2) \\
=\ &(\frac{1}{4} - \epsilon^2)((\Pr(x = z | x = y_1 \text{ and } x = y_2) + \\
+\ &Pr(x = z | x \neq y_1 \text{ and } x \neq y_2)).
\end{aligned}$$

However

$$\Pr(x = z | x = y_1 \text{ and } x = y_2) =$$

$$\Pr(z = y_1 | x = y_1 = y_2) = \Pr(z = y_1 | y_1 = y_2)$$

since it is independent of $x$, and similarly

$$Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) = \Pr(z \neq y_1 | y_1 = y_2).$$

Hence

$$\begin{aligned}
&\Pr(x = z | x = y_1 \text{ and } x = y_2) \\
&\quad + Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) = 1.
\end{aligned}$$

We conclude that

$$\begin{aligned}
&\Pr(x = z | x = y_1 \text{ and } x = y_2) \Pr(x = y_1) \Pr(x = y_2) \\
+\ &\Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) \Pr(x \neq y_1) \Pr(x \neq y_2) \\
=\ &(\frac{1}{4} - \epsilon^2). \qquad (3)
\end{aligned}$$

On the other hand, it is given that $\Pr(z = y_1 | y_1 \neq y_2) = \frac{1}{2}$. So,

$$\Pr(x = z | x = y_1 \text{ and } x \neq y_2) = \frac{1}{2}$$

and

$$\Pr(x = z | x \neq y_1 \text{ and } x = y_2) = \frac{1}{2}.$$

This gives as

$$\begin{aligned}
&(\frac{1}{2} + \epsilon)^2 (\Pr(x = z | x = y_1 \text{ and } x \neq y_2)) \\
+\ &(\frac{1}{2} - \epsilon)^2 (\Pr(x = z | x \neq y_1 \text{ and } x = y_2)) \\
=\ &\frac{1}{2}((\frac{1}{2} + \epsilon)^2 + (\frac{1}{2} - \epsilon)^2) \\
=\ &\frac{1}{4} + \epsilon^2. \qquad (4)
\end{aligned}$$

Summing the probabilities given in Equation 3 and Equation 4 we conclude that $\Pr(x = z) = \frac{1}{2}$. ■

A similar proposition can be proven as:

*Proposition 2:* Let $\Pr(x = y_1) = \Pr(x = y_2) = \frac{1}{2} + \epsilon$ for some $\epsilon > 0$. Assume that these events are independent. If $\Pr(z = y_1 | y_1 \neq y_2) = \frac{1}{2}$ and $\Pr(z = y_1 | y_1 = y_2) = \sigma$ which are independent of $x$, then we have $\Pr(z = x) = \frac{1}{2} + \epsilon(2\sigma - 1)$.

*Proof:* We give the sketch of the proof since it is similar to the proof of Proposition 1. We have $\Pr(z = x)$ given as

$$\begin{aligned}
&\Pr(x = z | x = y_1 \text{ and } x = y_2) \Pr(x = y_1) \Pr(x = y_2) \\
+&\Pr(x = z | x = y_1 \text{ and } x \neq y_2) \Pr(x = y_1) \Pr(x \neq y_2) \\
+&\Pr(x = z | x \neq y_1 \text{ and } x = y_2) \Pr(x \neq y_1) \Pr(x = y_2) \\
+&\Pr(x = z | x \neq y_1 \text{ and } x \neq y_2) \Pr(x \neq y_1) \Pr(x \neq y_2).
\end{aligned}$$

On the other hand we have

$$\begin{aligned} & \Pr(x=z|x=y_1 \text{ and } x\neq y_2)\Pr(x=y_1)\Pr(x\neq y_2) \\ + \;& \Pr(x=z|x\neq y_1 \text{ and } x=y_2)\Pr(x\neq y_1)\Pr(x=y_2). \\ = \;& (\frac{1}{2}+\epsilon)^2(\Pr(x=z|x=y_1 \text{ and } x\neq y_2) \\ + \;& (\frac{1}{2}-\epsilon)^2(\Pr(x=z|x\neq y_1 \text{ and } x=y_2)) \\ = \;& (\frac{1}{2}+\epsilon)^2\frac{1}{2}+(\frac{1}{2}-\epsilon)^2\frac{1}{2}=\frac{1}{4}-\epsilon^2 \end{aligned}$$

and

$$\begin{aligned} & \Pr(x=z|x=y_1 \text{ and } x=y_2)\Pr(x=y_1)\Pr(x=y_2) \\ + \;& \Pr(x=z|x\neq y_1 \text{ and } x\neq y_2)\Pr(x\neq y_1)\Pr(x\neq y_2) \\ = \;& (\frac{1}{2}+\epsilon)^2\cdot\sigma+(\frac{1}{2}-\epsilon)^2\cdot(1-\sigma). \end{aligned}$$

Hence we conclude that

$$\begin{aligned} & \Pr(x=z)=(\frac{1}{2}+\epsilon)^2\cdot\sigma+(\frac{1}{2}-\epsilon)^2\cdot(1-\sigma) \\ + \;& \frac{1}{4}-\epsilon^2=\frac{1}{2}+\epsilon(2\sigma-1) \end{aligned}$$

■

Note that if the probabilities $\Pr(z=y_1|y_1\neq y_2)=\frac{1}{2}$ and $\Pr(z=y_1|y_1=y_2)=\sigma$ are swapped, that is, if $\Pr(z=y_1|y_1=y_2)=\frac{1}{2}$ and $\Pr(z=y_1|y_1\neq y_2)=\sigma$ then the results in Proposition 1 and Proposition 2 will also be swapped. That is, we have $\Pr(z=x)=\frac{1}{2}+\epsilon(2\sigma-1)$ in Proposition 1 and $\Pr(z=x)=\frac{1}{2}$ in Proposition 2. The proof is rather knotty. However, it is very similar to the proof of Proposition 1. So, we skip it.

We generalize the statements in Proposition 1 and Proposition 2 to add another pair of random variable, this time loosing the independence condition for the new variables.

*Theorem 1:* For given binary random variables $x,t_1,t_2,y_1,y_2,z$, let $\Pr(x=t_1 \text{ and } x\neq t_2)=\Pr(x\neq t_1 \text{ and } x=t_2)$. Assume $\Pr(t_1=y_1)=\frac{1}{2}+\epsilon$, $\Pr(t_2=y_2)=\frac{1}{2}-\epsilon$ for some $\epsilon>0$ and they are independent of each other and of $x$. Let $\Pr(z=y_1|y_1\neq y_2)=\frac{1}{2}$ which is independent of $x$ and $\Pr(z=y_1|y_1=y_2)$ be also independent of $x$. Then we have $\Pr(z=x)=\frac{1}{2}$.

*Proof:* Let $Pr(x=t_1=t_2)=p_1$, $Pr(x=t_1\neq t_2)=p_2$, $Pr(x=t_2\neq t_1)=p_3$ and $Pr(x\neq t_1=t_2)=p_4$. Recall that we have $p_2=p_3$ by the assumption and $p_1+p_2+p_3+p_4=1$. Also, define $\Pr(z=y_1|y_1=y_2)=p$. Then $\Pr(z\neq y_1|y_1=y_2)=1-p$. With these parameters we write

$$\begin{aligned} & \Pr(z=x)= \\ & p_1(p(\frac{1}{4}-\epsilon^2)+\frac{1}{2}((\frac{1}{2}+\epsilon)^2+(\frac{1}{2}-\epsilon)^2)+(1-p)(\frac{1}{4}-\epsilon^2)) \\ & +p_2(p(\frac{1}{2}+\epsilon)^2+\frac{1}{2}(\frac{1}{4}-\epsilon^2+\frac{1}{4}-\epsilon^2)+(1-p)(\frac{1}{2}-\epsilon)^2) \\ & +p_3(p(\frac{1}{2}-\epsilon)^2+\frac{1}{2}(\frac{1}{4}-\epsilon^2+\frac{1}{4}-\epsilon^2)+(1-p)(\frac{1}{2}+\epsilon)^2) \\ & +p_4(p(\frac{1}{4}-\epsilon^2)+\frac{1}{2}((\frac{1}{2}+\epsilon)^2+(\frac{1}{2}-\epsilon)^2)+(1-p)(\frac{1}{4}-\epsilon^2)). \end{aligned}$$

Hence $\Pr(z=x)$ is given as

$$\begin{aligned} & p_1(\frac{1}{4}-\epsilon^2+\frac{1}{4}+\epsilon^2)+p_2(\frac{1}{2}+\epsilon(2p-1)) \\ + \;& p_3(\frac{1}{2}-\epsilon(2p-1))+p_4(\frac{1}{4}-\epsilon^2+\frac{1}{4}+\epsilon^2) \\ = \;& \frac{p_1+p_4}{2}+p_2(\frac{1}{2}+\epsilon(2p-1)+\frac{1}{2}-\epsilon(2p-1)) \end{aligned}$$

and this equals to $\frac{p_1+p_4}{2}+p_2$ . However, $p_1+2p_2+p_4=p_1+p_2+p_3+p_4=1$. Hence, $\Pr(z=x)=\frac{1}{2}$. ■

Theorem 1 explains how the biases of two characteristics can be perished together. These two characteristics have biases in the opposite directions. The natural question is what the combined bias is when the characteristics have both positive or negative biases. We give the combined biases in the following statement.

*Theorem 2:* For given binary random variables $x,t_1,t_2,y_1,y_2,z$, let $\Pr(x=t_1 \text{ and } x=t_2)-\Pr(x\neq t_1 \text{ and } x\neq t_2)=\rho$. Assume $\Pr(t_1=y_1)=\Pr(t_2=y_2)=\frac{1}{2}+\epsilon$ and they are independent of each other and of $x$. Let $\Pr(z=y_1|y_1\neq y_2)=\frac{1}{2}$ and $\Pr(z=y_1|y_1=y_2)=\sigma$ which are independent of $x$. Then $\Pr(z=x)=\frac{1}{2}+\epsilon\rho(2\sigma-1)$.

*Proof:* Let $Pr(x=t_1=t_2)=p_1$, $Pr(x=t_1\neq t_2)=p_2$, $Pr(x=t_2\neq t_1)=p_3$ and $Pr(x\neq t_1=t_2)=p_4$. We have $p_1+p_2+p_3+p_4=1$ and it is given that $\Pr(z=y_1|y_1=y_2)=\sigma$. Then $\Pr(z\neq y_1|y_1=y_2)=1-\sigma$. Then

$$\begin{aligned} & \Pr(z=x)= \\ & p_1((\frac{1}{4}-\epsilon^2)+\sigma(\frac{1}{4}+\epsilon^2)+(1-\sigma)(\frac{1}{2}-\epsilon)^2) \\ & +p_2(\frac{1}{2}((\frac{1}{2}+\epsilon)^2+(\frac{1}{2}-\epsilon)^2)+\sigma(\frac{1}{4}+\epsilon^2) \\ & +(1-\sigma)(\frac{1}{4}-\epsilon^2)) \\ & +p_3(\frac{1}{2}((\frac{1}{2}+\epsilon)^2+(\frac{1}{2}-\epsilon)^2)+\sigma(\frac{1}{4}+\epsilon^2) \\ & +(1-\sigma)(\frac{1}{4}-\epsilon^2)) \\ & +p_4((\frac{1}{4}-\epsilon^2)+\sigma(\frac{1}{4}-\epsilon^2)+(1-\sigma)(\frac{1}{2}+\epsilon)^2) \end{aligned}$$

Clearing out the parameters, $\Pr(z=x)$ will be equal to

$$(p_2+p_3)/2+p_1(1/2+\epsilon(2\sigma-1))+p_4(1/2-\epsilon(2\sigma-1)).$$

Then we conclude that

$$\Pr(z=x)=\frac{1}{2}+\epsilon(2\sigma-1)(p_1-p_4)$$

since $p_1+p_2+p_3+p_4=1$. On the other hand $p_1-p_4=\rho$. Hence,

$$\Pr(z=x)=\frac{1}{2}+\epsilon\rho(2\sigma-1).$$

■

## V. Experimental Results

In this section, we analyze a fictious cipher in which there are two linear characteristics with the same data (plaintext and ciphertext) mask but different key masks. This gives the so-called *linear hull* affect [9].

### A. The analyzed cipher

The fictious cipher, depicted in Figure 4, has 32-bit block length. Plaintext is XORed with the whitening key at the beginning of the encryption. Then the round function is applied four times. The cipher is an SPN structure. The round function consists of 4 $8 \times 8$ S-boxes and a bitwise permutation. We apply 6-bit S-boxes after the permutation to the bits which we do not use in the approximations to randomize the passive bits in the input masks. In Figure 4, $S8$ is an 8-bit and $S6_i$'s are 6-bit S-boxes. Bold lines (which are entering to any of the $S6_i$'s) are 6-bit values whereas other data lines are 1 bit variables. Each XORed key part has a length of 8-bits ($K_i$, where $i = 1 \ldots 20$).

The input of the round function is 32-bit data and 32-bit round key. The S-box layer of 8-bit S-boxes, which is also used at the end of the encryption, is applied to the data in the beginning of the round function. Then 7-bit left cyclic rotate operation is applied. After that, a combination of key XORing, 6-bit S-box operation and 6-bit diffusions are applied in the following manner:

Let the data after the 8-bit S-box and 7-bit cyclic rotate be named as $D_1||D_2||D_3||D_4$ where $D_i$'s are 8 bit parts from left to right. These names will also serve as the state at that block in the forthcoming operations. Similarly let $K_{i+1}||K_{i+2}||K_{i+3}||K_{i+4}$ be the round key. First, $K_{i+2}||K_{i+3}$ is XORed to $D_2||D_3$. Then $S6_2$ and $S6_3$ are applied to the rightmost 6-bit parts $D_2$ and $D_3$ respectively. The output of the $S6_2$ is XORed to the rightmost 6-bit of $D_1$, then the resulting value is passed to the $S6_1$. The output of $S6_1$ is XORed to the rightmost 6-bit of the current state at $D_2$. After that, $K_{i+1}$ is XORed to the state at $D_1$. Similar operations applied between $D_3$ and $D_4$.

The analyzed cipher is constructed in a way that there is a linear hull with two dominating linear characteristics. To provide this property, first we draw the paths of these two characteristics, then we construct an 8 bit S-box –namely $S8$– in a way that this S-box have the desired linear approximations with high biases. Bits not entering into these approximations distributed randomly, causing other linear approximations to have smaller biases.

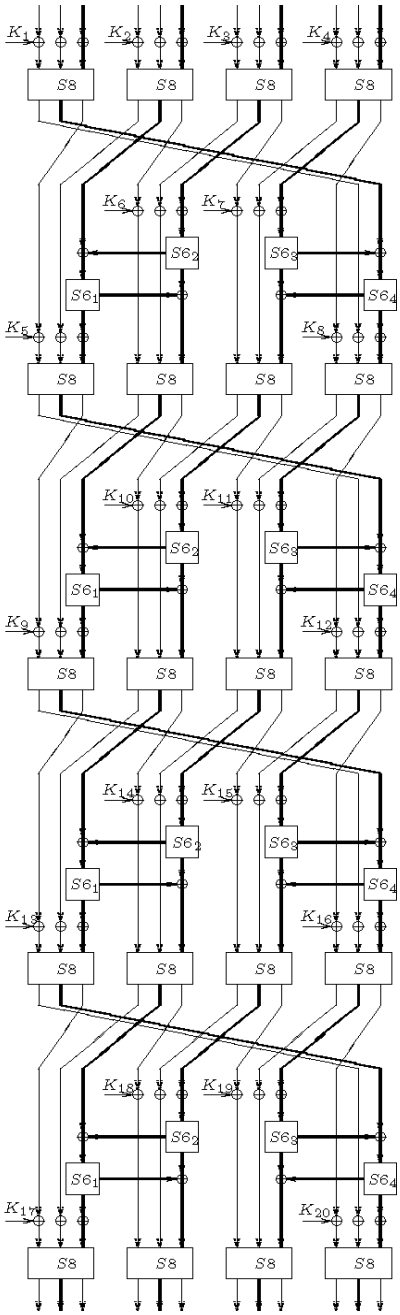


Fig. 4. The fictious block cipher's overall structure.

### B. Construction of the linear hull

Let the input bits of the $S8$ be written as $x_1||x_2 \ldots ||x_8$, and output bits as $y_1||y_2 \ldots ||y_8$. Then we have:

$$\Pr(x_1 = y_1) = \Pr(x_1 = y_8) = \frac{3}{4},$$
$$\Pr(x_2 = y_1) = \Pr(x_2 = y_8) = \frac{3}{4},$$
$$\Pr(x_1 = y_1 \text{ and } x_1 \neq y_8) = \frac{1}{4},$$
$$\Pr(x_1 = y_8 \text{ and } x_1 \neq y_1) = \frac{1}{4},$$
$$\Pr(y_8 = x_1 | x_1 \neq x_2) = \frac{1}{2},$$

Using the equations above, we construct a pair of linear characteristics. For any data block, $X$, $X[j]$ denotes the leftmost $j-$th bit of $X$, where indices begin at 1. $P$ and $C$ denote the plaintext and ciphertext respectively. The round keys $K_j$'s are assumed to be independent, i.e., the key length of the cipher is 160-bit.

$$P[1] \oplus C[8] = K_1[1] \oplus K_5[1] \oplus K_9[1] \oplus K_{13}[1] \oplus K_{17}[1] \quad (5)$$

$$P[1] \oplus C[8] = K_1[1] \oplus K_8[2] \oplus K_{11}[2] \oplus K_{14}[2] \oplus K_{17}[2] \quad (6)$$

The pair of the linear characteristics given in Equation 5 and Equation 6 is constructed in order to form an example for the model in Figure 3. $F$ can be seen as the leftmost S-box of the first round whereas the leftmost S-box of the final S-box layer plays the role of $G$. $U$, on the other hand, is the middle 3 rounds which are the independent part of our characteristics. Call the right hand side of (5) and (6)–i.e. the key bits– $K_L$ and $K_R$ respectively.

If we call the ouput of the $i^{th}$ cyclic rotate operation by $X_i$ $(i = 1, \ldots 4)$, the variables used in *Theorem* 1 and *Theorem* 2 can be assigned to our case in the following manner:

$$x = P[1], t_1 = X_1[1], t_2 = X_1[26],$$

$$y_1 = X_4[1], y_2 = X_4[2], \text{and } z = C[8].$$

### C. Mounting linear attack

Using the classical assumptions of linear cryptanalysis and the piling-up lemma, we can calculate the overall biases of (5) and (6) as follows;

$$\epsilon_1 = \epsilon_2 = 2^4(2^{-2})^5 = 2^{-6}$$

where $\epsilon_1$ and $\epsilon_2$ are the biases of (5) and (6) respectively. Here, each characteristics have 5 active S-boxes and all active S-boxes have a bias of $2^{-2}$. So both characteristics have probability $\frac{1}{2} + 2^{-6}$ by the piling-up lemma.

We implement Algorithm 1 of [12] and see that the plaintext-ciphertext mask has the bias different then the bias, $2^{-6}$, computed by the piling-up lemma for any key. The actual bias of $P[1] \oplus C[8]$ (the left hand side of the linear characteristics) is around $2^{-5}$ for some keys. We classified these keys. On the other hand, the bias perishes for some other keys. Indeed, when both biases in both characteristics are positive, then the overall bias is increased to $2^{-5}$. Otherwise, it perishes. The results of the experiments are depicted in Table I. The success rate of Algorithm 1 is 50% whereas it is expected to be almost one since we use much more than $2^{12}$ data.

Table I shows that if the linear combination of the key bits of two characteristics are equal then the bias is increased by a factor of two. If the linear combination of the key bits are not equal, then the bias becomes 0.

The case in which the linear combinations of the key bits are not equal is explained through Theorem 1. The difference in the linear combinations of the key bits causes two approximations having biases of opposite signs, i.e., one of them has probability $\frac{1}{2} + \epsilon$, and the other one has $\frac{1}{2} - \epsilon$, where $\epsilon = 2^{-4}$. Other assumptions of the theorem are also satisfied by the S-box. So the overall bias is expected to be zero by Theorem 1. Indeed, the experimental results have been verified the result. We have observed a bias of less then $2^{-10}$ when $2^{20}$ data were used and a bias of less then $2^{-12}$ when $2^{24}$ data were used as in Table I.

TABLE I
EXPERIMENTAL RESULTS ON THE FICTIOUS CIPHER. BIASES ARE COMPUTED ACCORDING TO EQUATION (5), I.E FOR THE EVENT $P[1] \oplus C[8] = K_L$

| | | Biases for ($K_L$,$K_R$) pair (see Sec. V-B) | | | |
|---|---|---|---|---|---|
| **Exp #** | **Data** | **(0,0)** | **(0,1)** | **(1,0)** | **(1,1)** |
| 1 | $2^{20}$ | $2^{-5.0086}$ | $2^{-12.3276}$ | $-2^{-10.2154}$ | $2^{-4.9830}$ |
| 2 | $2^{20}$ | $2^{-5.0192}$ | $2^{-10.3598}$ | $2^{-10.3927}$ | $2^{-4.9866}$ |
| 3 | $2^{20}$ | $2^{-5.0023}$ | $2^{-11.8605}$ | $2^{-11.2252}$ | $2^{-5.0199}$ |
| 4 | $2^{20}$ | $2^{-5.0195}$ | $-2^{-10.8102}$ | $2^{-10.7426}$ | $2^{-5.0207}$ |
| 5 | $2^{24}$ | $2^{-5.0109}$ | $2^{-14.5344}$ | $-2^{-13.8251}$ | $2^{-4.9955}$ |
| 6 | $2^{24}$ | $2^{-5.0093}$ | $2^{-11.8148}$ | $-2^{-13.0028}$ | $2^{-4.9993}$ |
| 7 | $2^{24}$ | $2^{-5.0187}$ | $2^{-12.4594}$ | $-2^{-15.3634}$ | $2^{-4.9877}$ |
| 8 | $2^{24}$ | $2^{-5.0034}$ | $2^{-12.3449}$ | $2^{-12.3276}$ | $2^{-5.0046}$ |

When two linear combinations of the key bits are both zero or both one simultaneously, that is, when the biases of the both approximations are positive or negative then we observe an increase of factor two in each bias as given in Theorem 2. We saw that the bias of one approximation is doubled as the theorem states. That is, the overall bias is calculated by summing the biases. In our example, $\rho = \frac{1}{2}, \sigma = 1$ and $\epsilon = 2^{-4}$. So, the overall bias is calculated as $2^{-5}$ as we have observed in the experiments.

## VI. CONCLUSION

In this paper, we examined Matsui's linear cryptanalysis and the bias calculation for the extended linear masks through the piling-up lemma. By introducing a case study, we have proved that the lemma does not work all the time . We also have shown the existence of linear hull in the case study. We have derived new statements to calculate the actual biases for our case study and verified our results by conducting some experiments. To do that, we have designed a toy cipher and mount the linear attack on the cipher, yielding two linear approximations whose random variables comply with the assumptions given in the statements derived for the case study.

## ACKNOWLEDGMENT

We would like to thank Rıdvan Bakkal and Mehmet Sabır Kiraz for their helpful comments.

## REFERENCES

[1] A.A. Selçuk. *On Bias Estimation in Linear Cryptanalysis.* In *Proc. Indocrypt 2000*, LNCS 1977, pp. 52–66, Springer, 2000.

[2] A. Biryukov, C. D. Cannière, and M. Quisquarter. *On Multiple Linear Approximations.* In M. Franklin (Ed.): *Crypto 2004*, LNCS 3152, pp. 1–22, Springer, 2004.

[3] B. Collard, C. D. Cannière, and M. Quisquarter. *Experiments on the Multiple Linear Cryptanalysis of Reduced Round Serpent.* In K. Nyberg (Ed.): *FSE 2008*, LNCS 5086, pp. 382–397, Springer, 2008.
[4] B. S. Kaliski Jr., and M. J. B. Robshaw. *Linear Cryptanalysis Using Multiple Approximations.* In Y. G. Desmedt (Ed.): *Crypto'94*, LNCS 839, pp. 26–39, Springer-Verlag Berlin Heidelberg, 1994.
[5] B. S. Kaliski Jr., and M. J. B. Robshaw. *Linear Cryptanalysis Using Multiple Approximations and FEAL.* In B. Preneel (Ed.): *FSE'94*, LNCS 1008, pp. 249–264, Springer, 1995.
[6] F. Chabaud, S. Vaudenay. *Links Between Differential and Linear Cryptanalysis.* In A. D. Santis (Ed.): *Eurocrypt'94*, LNCS 950, pp. 356–365, Springer, 1995.
[7] G. Leander. *On Linear Hulls,Statistical Saturation Attacks, PRESENT and Cryptanalysis of PUFFIN.* In K. G. Peterson (Ed.): *Eurocrypt 2011*, LNCS 6632, pp. 303–322, Springer, 2011.
[8] J. Nakahara Jr., P. Sepehrdad, B. Zhang, and M. Wang. *Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT.* In J. A. Garay, A. Miyaji, and A. Otsuka (Eds.): CANS 2009, LNCS 5888, pp. 58–75, Springer-Verlag Berlin Heidelberg, 2009.
[9] K. Nyberg. *Linear Approximation of Block Ciphers.* In A. D. Santis (Ed.): *Eurocrypt'94*, LNCS 950, pp. 439–444, Springer, 1995.
[10] M. Hermelin, J. Y. Cho, and K. Nyberg. *Multidimensional Extension of Matsui's Algorithm 2.* In O. Dunkelman (Ed.): *FSE 2009*, LNCS 5665, pp. 209–227, Springer, 2009.
[11] M. Hermelin, J. Y. Cho, and K. Nyberg. *Multidimensional Linear Cryptanalysis of Reduced Round Serpent.* In Y. Mu, W. Susilo, and J. Seberry (Eds.): *ACISP 2008*, LNCS 5107, pp. 203-215, Springer-Verlag Berlin Heidelberg, 2008.
[12] M. Matsui. *Linear Cryptanalysis Method of DES Cipher.* In *Proc. EUROCRYPT'93*, LNCS 765, pp. 386–397, Springer, 1994.
[13] M. Matsui. *The First Experimental Cryptanalysis of the Data Encryption Standard.* In *Proc. CRPTO'94*, LNCS 839, pp. 1–11, Springer, 1994.
[14] S. Murphy. *The Effectiveness of the Linear Hull Effect.* Technical Report, RHULMA-2009-19 (2009).
[15] S. Murphy. *The Independence of Linear Approximations in Symmetric Cryptanalysis.* In *IEEE Transactions on Information Theory*,Vol. 22, N0. 12, December 2006.
[16] W. Meier and O. Staffelbach. *Nonlinearity Criteria for Cryptographic Functions.* In *Proc. EUROCRYPT'89*, LNCS 434, pp. 548–562, Springer, 1989.
[17] V. Rijmen, *Cryptanalysis and Design of Iterated Block Ciphers,* Doctoral Dissertation, K.U. Leuven, 1997.