On Bias Estimation in Linear Cryptanalysis

Ali Aydın Selçuk

Maryland Center for Telecommunications Research
Department of Computer Science and Electrical Engineering
University of Maryland, Baltimore County
Baltimore, MD, 21250, USA
aselcu1@csee.umbc.edu

Abstract. Security analysis of block ciphers against linear cryptanalysis has virtually always been based on the bias estimates obtained by the Piling-Up Lemma (PUL) method. Despite its common use, and despite the fact that the independence assumption of the PUL is known not to hold in practice, accuracy of the PUL method has not been analyzed to date. In this study, we start with an experimental analysis of the PUL method. The results on RC5 show that the estimates by the PUL method can be quite inaccurate for some non-Feistel ciphers. On the other hand, the tests with SP-structured Feistel ciphers consistently show a much higher degree of accuracy.
In the second part, we analyze several theories for an alternative method for bias estimation, including correlation matrices, linear hulls, and statistical sampling. We show a practical application of the theory of correlation matrices, where better estimates than the PUL method are obtained. We point out certain problems in some current applications of linear hulls. We show that the sample size required for a reliable statistical estimator is an impractically large amount for most practical cases.

1 Introduction

Estimating the bias of a given linear approximation is one of the most important problems in linear cryptanalysis: the success rate of a linear attack is directly related to the bias of the approximation it uses, therefore, security analysis of block ciphers against linear cryptanalysis is exclusively based on the estimation of the bias of their linear approximations.

In practice, estimation of the bias is almost exclusively based on the Piling-Up Lemma (PUL) [11], which is a very practical tool for bias estimation on iterated block ciphers. To estimate the bias of a multi-round approximation, the round approximations are assumed independent and the bias of the combined approximation is calculated by the PUL. We will refer to this application of the PUL as the *PUL method*.

In the first part of this study, we analyze the bias estimates obtained by the PUL method. Although the PUL method has been widely used, and although it is known that this method's assumption of independent round approximations is virtually never true, the accuracy of the estimates obtained by this method

has almost never been the subject of a study.[1] Our analysis concentrates on two cases: DES-like SP-structured Feistel ciphers and RC5. The Feistel ciphers represent the class of ciphers that the PUL method was originally applied on. RC5 represents a cipher that has a totally different structure (which is based on a mixture of arithmetic operations and data-dependent rotations, instead of the traditional substitution and permutation structures). In the study of Feistel ciphers, we analyze the accuracy of the estimated values with respect to various factors, including the number of active s-boxes in a round, presence/absence of a bit expansion function, etc.

The analysis results show that the PUL method gives quite accurate estimates with SP-structured Feistel ciphers, especially for approximations with at most a single active s-box at each round, as long as the estimated values are significantly higher than $2^{-\frac{n}{2}}$. With RC5, the estimates turn out to have a much lesser accuracy.

In the second part of this study, we look for an alternative estimation method which would give more accurate estimates than the PUL method in general (e.g., for non-Feistel ciphers, or for large number of rounds where the PUL method gives too small values). For this purpose, we analyze the theories of correlation matrices, linear hulls, and statistical sampling. We give an example application of correlation matrices for bias estimation, which gives consistently better estimates than the PUL method on RC5. We review the theory of linear hulls, which has also been used as an alternative technique for bias estimation. We point out certain problems with some current applications of linear hulls where the application has no basis in theory. Finally, we look at the prospects of estimating the bias by statistical techniques over a randomly generated sample of plaintext/ciphertext blocks. It turns out that the statistical techniques do not provide any practical solutions for bias estimation, especially when the inverse square of the bias is an impractically large amount for a sample size.

Notation: Throughout the paper, we use n to denote the block size and r to denote the number of rounds in an iterated block cipher. K_i denotes the ith round key, L_i and R_i denote the left and right halves of the round output. p is used for the probability of an approximation, where $|p - 1/2|$ is the bias. Bits in a block are numbered from right to left, beginning with 0. The "$\cdot$" operator denotes the bitwise dot product.

2 Experiments with RC5

During some linear cryptanalysis experiments with small block sizes of RC5, we noticed significant differences between the actual bias of a linear approximation and the values that were estimated by the PUL method. We summarize these findings in this section.

The RC5 encryption function is:

[1] One exception in this regard is [2], where the accuracy of PUL estimates was studied in the specific context of combining two neighbor s-box approximations in DES.

$L_1 = L_0 + K_0$
$R_1 = R_0 + K_1$
for $i = 2$ **to** $2r + 1$ **do**
    $L_i = R_{i-1}$
    $R_i = ((L_{i-1} \oplus R_{i-1}) \lll R_{i-1}) + K_i$

The best currently-known linear approximation of RC5 [8] is

$$R_0[0] \oplus L_{2r}[0] = K_1[0] \oplus K_3[0] \oplus \cdots \oplus K_{2r-1}[0], \tag{1}$$

The probability of this approximation is estimated as $1/2 + 1/2w^{r-1}$ by the PUL method where w is the word size in bits (in RC5, half of a block is called a *word*).

We computed the bias of Approximation (1) by exhaustively going over all plaintext blocks for various values of w and r. The test results are summarized in Table 1. The results show quite significant differences between the actual and the estimated values of the bias. Another remarkable point is that increasing the number of rounds does not affect the bias after a certain point, and the bias does not get much smaller than 2^{-w-1}. We further discuss these results in Section 4.

r	Bias	PUL
2	$2^{-3.0}$	2^{-3}
3	$2^{-4.5}$	2^{-5}
4	$2^{-5.1}$	2^{-7}
5	$2^{-5.3}$	2^{-9}
10	$2^{-5.3}$	2^{-19}

(a) $w = 4$

r	Bias	PUL
3	$2^{-5.8}$	2^{-7}
4	$2^{-7.7}$	2^{-10}
5	$2^{-8.8}$	2^{-13}
6	$2^{-9.1}$	2^{-16}
10	$2^{-9.2}$	2^{-28}

(b) $w = 8$

r	Bias	PUL
4	$2^{-10.4}$	2^{-13}
5	$2^{-12.1}$	2^{-17}
6	$2^{-14.6}$	2^{-21}
7	$2^{-16.3}$	2^{-25}
10	$2^{-17.3}$	2^{-37}

(c) $w = 16$

Table 1. Average actual bias of Approximation (1) and the bias estimated by the PUL for various values of w and r, with 500 randomly chosen keys for each w and r. The results show a significant difference between the actual bias values and the PUL estimates. The difference increases sharply with increasing number of rounds.

3 Experiments with Feistel Ciphers

Following the findings on RC5 described in Section 2, we performed similar tests with Feistel ciphers, which is the type of cipher the PUL method was originally used for [11]. In this section, we describe these tests and summarize their results.

3.1 Design

The ciphers used in these experiments are Feistel ciphers with 32-bit block sizes. The encryption function of a Feistel cipher is of the following form:

for $i = 1$ **to** r **do**
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

The F function we used in the experiments has a structure similar to that in DES. It has a sequence of key addition, substitution, and permutation stages. In the key addition stage, R_{i-1} is XORed by the round key K_i, with a possible bit expansion before the XOR. The Feistel ciphers used in the experiments include both those with an expansion function E and those without one. In ciphers with a bit expansion, the expansion function E is the equivalent of the expansion function in DES, reduced to 16×24 bits.

The substitution stage is also similar to that in DES, with four parallel distinct s-boxes. The s-boxes are either 4×4 or 6×4, depending on the presence or absence of the bit expansion. The 4×4 s-boxes are chosen from the s-boxes of Serpent [1], and the 6×4 s-boxes are chosen from the s-boxes of DES [6].

The permutation stage uses a 16×16 permutation function P to mix the output bits from the s-boxes. In the Serpent s-boxes, unlike the DES s-boxes [6], there is no distinction among the role of input bits. So, with the Serpent s-boxes we use the following simple permutation P which guarantees that each output bit from an s-box affects a different s-box in the next round: $P = (15\ 11\ 7\ 3\ 14\ 10\ 6\ 2\ 13\ 9\ 5\ 1\ 12\ 8\ 4\ 0)$.[2] With the DES s-boxes, we use the following permutation which guarantees that the output of each s-box has an effect on two outer bits, two inner non-middle bits, and two middle bits (of different s-boxes) in the next round: $P = (12\ 10\ 3\ 6\ 14\ 11\ 4\ 2\ 15\ 9\ 7\ 1\ 13\ 8\ 5\ 0)$.

Notation: Each Feistel cipher used in the tests will be identified by the presence/absence of the expansion in key addition, and by the numbers of the s-boxes used (ordered from left to right). For the numbering of the s-boxes, the numbering in their original ciphers will be used. E.g. $\mathrm{FC}_{NE}0214$ will denote the Feistel cipher with no bit expansion and with the Serpent s-boxes S_0, S_2, S_1, S_4. $\mathrm{FC}_{E}8735$ will denote the Feistel cipher with the bit expansion E and with the DES s-boxes S_8, S_7, S_3, S_5.

We start our experiments with the FC_{NE} ciphers which are the simpler case since there is no issue of duplicate bits. We first look at the approximations with at most a single active s-box at each round. Then we go to the approximations with multiple s-boxes in the same round.

3.2 Approximations with Single Active S-box

First, we look at how the PUL method performs on the approximations with at most a single active s-box at every round, which is the most basic type of linear approximations of an SP-structured Feistel cipher. We denote the round approximations in terms of the s-box approximations, as in [11, 12].

We consider the 4-round iterative approximations of the form ABC–, which can be combined by itself as ABC–CBA–ABC–..., where A, B and C are some

[2] The numbers show the new location of the bits after permutation.

non-trivial approximations of the F function, and "–" denotes the nil approximation. This is the form of the approximations which gave the highest bias on DES [11, 12], and which also gives the highest bias on our FC_{NE} ciphers. Here we present the results for three of our test cases. The results are summarized in Table 2. The bias is denoted by b.

Case 1.1: Cipher: $\mathrm{FC}_{NE}1745$, A: $4{\cdot}x = 11{\cdot}S_1(x)$, $b = 1/4$, B: $8{\cdot}x = 8{\cdot}S_7(x)$, $b = 1/8$, C: $4{\cdot}x = 15{\cdot}S_1(x)$, $b = 1/4$.
Case 1.2: Cipher: $\mathrm{FC}_{NE}6530$, A: $2{\cdot}x = 13{\cdot}S_5(x)$, $b = 1/4$, B: $4{\cdot}x = 4{\cdot}S_3(x)$, $b = 1/8$, C: $2{\cdot}x = 15{\cdot}S_5(x)$, $b = 1/4$.
Case 1.3: Cipher: $\mathrm{FC}_{NE}0214$, A: $4{\cdot}x = 8{\cdot}S_1(x)$, $b = 1/8$, B: $2{\cdot}x = 2{\cdot}S_2(x)$, $b = 1/8$, C: $4{\cdot}x = 12{\cdot}S_1(x)$, $b = 1/8$.

r	Bias	PUL
4	$2^{-5.00}$	2^{-5}
8	$2^{-9.00}$	2^{-9}
12	$2^{-12.96}$	2^{-13}
16	$2^{-16.51}$	2^{-17}
20	$2^{-17.30}$	2^{-21}
24	$2^{-17.31}$	2^{-25}

(a) Case 1.1

r	Bias	PUL
4	$2^{-5.00}$	2^{-5}
8	$2^{-9.00}$	2^{-9}
12	$2^{-12.86}$	2^{-13}
16	$2^{-16.83}$	2^{-17}
20	$2^{-17.26}$	2^{-21}
24	$2^{-18.28}$	2^{-25}

(b) Case 1.2

r	Bias	PUL
4	$2^{-7.00}$	2^{-7}
8	$2^{-12.94}$	2^{-13}
12	$2^{-16.75}$	2^{-19}
16	$2^{-17.35}$	2^{-25}
20	$2^{-17.84}$	2^{-31}
24	$2^{-17.42}$	2^{-37}

(c) Case 1.3

Table 2. Test results for single-sbox approximations. PUL estimates are quite accurate, as long as they are above $2^{-\frac{n}{2}-1}$. Like the results on RC5, the bias does not go much below $2^{-\frac{n}{2}-1}$.

3.3 Approximations with Multiple S-box

In this section, we look at how having multiple active s-boxes in the same round affects the accuracy of PUL estimation. We focus our experiments on approximations with two s-boxes, because in our miniature ciphers the bias with three or four active s-boxes drop too fast to draw any useful conclusions.

We work with the 3-round iterative approximations of the form AB–, which can be combined by itself as AB–BA–AB–..., where A and B are approximations of the F function with two active s-boxes. Three such approximations are given below. The results are summarized in Table 3.

Case 2.1: Cipher: $\mathrm{FC}_{NE}5614$, A: $(3{\cdot}x = 3{\cdot}S_4(x), b = 1/4)$ AND $(3{\cdot}x = 3{\cdot}S_5(x), b = 1/4)$ B: $(9{\cdot}x = 9{\cdot}S_1(x), b = 1/4)$ AND $(9{\cdot}x = 9{\cdot}S_4(x), b = 1/4)$
Case 2.2: Cipher: $\mathrm{FC}_{NE}4250$, A: $(10{\cdot}x = 10{\cdot}S_0(x), b = 1/4)$ AND $(10{\cdot}x = 10{\cdot}S_5(x), b = 1/4)$ B: $(3{\cdot}x = 3{\cdot}S_4(x), b = 1/4)$ AND $(3{\cdot}x = 3{\cdot}S_5(x), b = 1/4)$
Case 2.3: Cipher: $\mathrm{FC}_{NE}5014$, A: $(3{\cdot}x = 3{\cdot}S_4(x), b = 1/4)$ AND $(3{\cdot}x = 3{\cdot}S_5(x), b = 1/4)$ B: $(9{\cdot}x = 9{\cdot}S_1(x), b = 1/4)$ AND $(9{\cdot}x = 9{\cdot}S_4(x), b = 1/4)$

r	Bias	PUL
3	$2^{-5.00}$	2^{-5}
6	$2^{-8.94}$	2^{-9}
9	$2^{-12.94}$	2^{-13}
12	$2^{-16.99}$	2^{-17}
15	$2^{-17.48}$	2^{-21}
18	$2^{-18.29}$	2^{-25}

(a) Case 2.1

r	Bias	PUL
3	$2^{-5.00}$	2^{-5}
6	$2^{-8.90}$	2^{-9}
9	$2^{-12.90}$	2^{-13}
12	$2^{-16.54}$	2^{-17}
15	$2^{-17.17}$	2^{-21}
18	$2^{-17.04}$	2^{-25}

(b) Case 2.2

r	Bias	PUL
3	$2^{-5.00}$	2^{-5}
6	$2^{-8.91}$	2^{-9}
9	$2^{-12.88}$	2^{-13}
12	$2^{-16.94}$	2^{-17}
15	$2^{-17.19}$	2^{-21}
18	$2^{-17.37}$	2^{-25}

(c) Case 2.3

Table 3. Test results for approximations with two active s-boxes in a round. PUL estimates are somewhat less accurate than those in Table 2 for single-sbox approximations, but still better than those on RC5.

3.4 Approximations with Expansion

Here we look at the effect of having an expansion function at the key addition stage. When there is an expansion at the key addition stage like the E function in DES and our FC$_E$ ciphers, an approximation of an s-box not only affects the input to that active s-box, but also affects the two shared input bits with the neighbor s-boxes. Therefore, the output of the neighbor s-boxes will also be more or less affected by an s-box approximation.

We tested the accuracy of the PUL estimates with certain approximations of the FC$_E$ ciphers. The tests are focused on approximations with a single active s-box at every round, because the bias of approximations with multiple active s-boxes drops too fast in FC$_E$s. The approximations used in the tests are iterative approximations of the form ABC–CBA–ABC–... The tested approximations are listed below, and the results are summarized in Table 4.

Case 3.1: Cipher: FC$_E$5216, A: $16{\cdot}x = 15{\cdot}S_5(x)$, $b = 20/64$, B: $8{\cdot}x = 8{\cdot}S_1(x)$, $b = 4/64$, C: $16{\cdot}x = 14{\cdot}S_5(x)$, $b = 10/64$.

Case 3.2: Cipher: FC$_E$8735, A: $16{\cdot}x = 7{\cdot}S_5(x)$, $b = 8/64$, B: $4{\cdot}x = 2{\cdot}S_8(x)$, $b = 2/64$, C: $16{\cdot}x = 15{\cdot}S_5(x)$, $b = 20/64$.

3.5 Other Approximations

The ciphers and approximations considered in these tests are by no means exhaustive, and in fact there are many different Feistel ciphers and approximations possible. The purpose of the tests is not to exhaustively prove a result about the bias of Feistel ciphers, but to obtain a general view of the accuracy of PUL estimation on Feistel ciphers. As we will discuss in Section 4, these results indeed give a general idea on the subject.

r	Bias	PUL
4	$2^{-6.36}$	$2^{-6.36}$
8	$2^{-11.71}$	$2^{-11.71}$
12	$2^{-16.74}$	$2^{-17.06}$
16	$2^{-17.31}$	$2^{-22.42}$
20	$2^{-17.62}$	$2^{-27.78}$

(a) Case 3.1

r	Bias	PUL
4	$2^{-7.68}$	$2^{-7.68}$
8	$2^{-14.40}$	$2^{-14.36}$
12	$2^{-17.26}$	$2^{-21.03}$
16	$2^{-17.70}$	$2^{-27.71}$
20	$2^{-17.47}$	$2^{-34.39}$

(b) Case 3.2

Table 4. Test results for single-sbox approximations with the expansion E. PUL estimates are slightly less accurate than those without E, given in Table 2.

4 Discussion on the Results

The test results on Feistel ciphers show that the PUL method is quite effective for bias estimation with SP-structured Feistel ciphers, as long as the estimated values are significantly higher than $2^{-\frac{n}{2}}$. The results are best when there is at most a single active s-box in each round approximation, and when there is no bit expansion. When there are more affected s-boxes in a round approximation, the number of bits affected by the approximation increases, and so does the effect it has on the following round approximations (i.e. dependence among round approximations).

The test results on RC5 show that accuracy of the PUL estimates may not be so good with ciphers that are not SP-structured Feistel ciphers. In the test results with RC5, there is a considerable difference between the estimated and actual values even for smaller number of rounds. With larger number of rounds, the bias may be significantly higher than $2^{-\frac{n}{2}}$ even after the estimated values become lower than $2^{-\frac{n}{2}}$. We can say, looking at the test results, that larger differences should be expected in practice with larger block sizes (i.e. with 64- and 128-bit blocks).

It is not easy to explain the difference in the accuracy of the estimates with RC5 and with Feistel ciphers: The source of inaccuracy of a PUL estimate is the dependence between round approximations, which is a factor that has to be neglected by the PUL method by its very definition. Both the RC5 round approximations and the single-sbox FC_{NE} round approximations affect (i.e., give information on) 4 out of 16 bits of R_{i-1}. Moreover, in the FC_{NE} approximations, there are three non-trivial round approximations in every four rounds, whereas in the RC5 approximation there are only two non-trivial approximations in four (half)rounds. So, it would be natural to expect that there would be more dependence and interaction among the FC_{NE} round approximations, which turns out not to be the case. For now, we accept the accuracy of the PUL estimates on Feistel ciphers as an experimental result and do not go into an in-depth analysis of the factors underlying it.

Similarly, we cannot give a simple explanation for why the actual and the estimated bias values for the Feistel ciphers go so closely until they reach the $2^{-\frac{n}{2}}$ threshold, and become so divergent after that point. It is not possible to simply explain this with the accumulation of the dependence affect with more rounds, since a comparison of the test results with low-bias and high-bias approximations suggests that the point where the actual and the estimated values diverge is not determined by the number of rounds, but is mostly determined by the proximity to the $2^{-\frac{n}{2}}$ threshold.

4.1 Stabilization of the Bias

Here we give two theorems related to the stabilization of the bias around $2^{-\frac{n}{2}-1}$. Although the theorems do not explain how the sharp change in accuracy of PUL estimates at $2^{-\frac{n}{2}}$ is related to the dependence between round approximations, they provide some important facts about the stabilization of the bias. The first theorem gives a lower bound for the bias of the best approximation. The second theorem suggests that when the bias of the best approximation approaches the theoretical lower bound, the bias of almost all linear approximations of the cipher should be around $2^{-\frac{n}{2}-1}$. The first theorem follows from Theorem 4 in [4] with $p = q = n$ (see Appendix A). The second theorem is observed in the proof of that theorem. F_k is an n-bit block cipher with key $K = k$; $p_{a,b}$ denotes the probability of the approximation $a \cdot X \oplus b \cdot F_k(X) = 0$.[3]

Theorem 1. *$\exists\ a, b \in \{0,1\}^n$, such that $|p_{a,b} - 1/2| \geq 2^{-\frac{n+1}{2}}$.*

Theorem 2. *$\sum_{a,b \in \{0,1\}^n} |p_{a,b} - 1/2|^2 = 2^{n-2}$.*

5 Alternative Methods for Bias Estimation

In this section, we analyze several theories for an alternative method for bias estimation, including correlation matrices, linear hulls and statistical sampling.

5.1 Correlation Matrices

For a function $f : \{0,1\}^m \to \{0,1\}^n$, the *correlation matrix* $C^{(f)}$ is a $2^n \times 2^m$ matrix whose (b,a)th entry $c_{ba}^{(f)}$ is the *correlation coefficient* $2P_X(a \cdot X = b \cdot f(X)) - 1$ [7]. The relationship between the correlation coefficients and the bias is straightforward: If F_k is a block cipher with key $K = k$, bias of $a \cdot X \oplus b \cdot F_k(X) = d \cdot K$ (for any d) equals $|c_{ba}^{(F_k)}|/2$. For $f : \{0,1\}^\ell \to \{0,1\}^m$, $g : \{0,1\}^m \to \{0,1\}^n$, we have $C^{(g \circ f)} = C^{(g)} \times C^{(f)}$. So, if F_k is an iterative cipher and f_i is the ith round with its respective round key, we have $C^{(F_k)} = \prod_{i=1}^{r} C^{(f_i)}$. Then $c_{ba}^{(F_k)}$ equals $\sum_{a_1, a_2, \ldots, a_{r-1}} (\prod_{i=1}^{r} c_{a_i a_{i-1}}^{(f_i)})$ where $a_0 = a$, $a_r = b$, and each $\prod_{i=1}^{r} c_{a_i a_{i-1}}^{(f_i)}$

[3] The bias does not depend on the key mask here, because the key is a fixed parameter (which is also the case in a linear attack).

is known as the *correlation contribution coefficient (CCC)* of the *linear trail* $a_0 \to a_1 \to \ldots \to a_r$.

So, the theory of correlation matrices tells that the bias of a linear approximation is equal to the sum of the PUL biases (without absolute value) of all linear trails that lead to the given approximation. Hence, correlation matrices provide a generalization of the PUL method: Instead of using the PUL bias of a single linear trail, the bias can be estimated by summing up the PUL bias of as many linear trails as possible which lead to the given approximation. We will refer to this generalization of the PUL method as the *CM method.*

An Example Application: As an example, we apply the CM method to our RC5 approximation (1). All effective RC5 approximations obtained so far [8, 9, 16, 3] are based on round approximations with a single active input and output bit. To be expandable over multiple rounds, the 1-bit round approximations should be of the form $R_i[m_i] \oplus L_{i-1}[m'_i] = S_i[m_i] \oplus c$ where $m_i, m'_i < \lg w$ and c is a constant. These approximations are analyzed in detail by Borst et al. [3]. Probability of the 1-round approximation

$$R_i[m_i] \oplus L_{i-1}[m'_i] = S_i[m_i] \oplus (m_i - m'_i)[m'_i],$$

where $(m_i - m'_i)[m'_i]$ denotes the m'_ith bit of $(m_i - m'_i) \bmod w$, is equal to $\frac{1}{2} + \frac{1}{w}\left(\frac{1}{2} - \frac{s}{2^{m_i}}\right)$, where s denotes $S_i \bmod 2^{m_i}$. Hence, the correlation coefficient of $R_i[m_i] = L_{i-1}[m'_i]$ is equal to $(-1)^{\delta}\frac{1}{w}\left(1 - \frac{s}{2^{m_i-1}}\right)$, where $\delta = S_i[m_i] \oplus (m_i - m'_i)[m'_i]$. The 1-bit trails that lead to Approximation (1) are those which satisfy,

$$\begin{aligned} &m_1 = 0, \\ &m_i = m'_{i+2} < \lg w, \quad \text{for } i = 3, 5, \ldots, 2r-3, \\ &m_{2r-1} = 0. \end{aligned}$$

We computed the bias by adding up the correlation contribution coefficients of all 1-bit linear trails of this form. The results are given in Figure 1 and are compared to the actual bias and the PUL estimate values.

	Bias		
r	Actual	PUL	CM
2	2^{-5}	2^{-5}	2^{-5}
4	$2^{-10.4}$	2^{-13}	$2^{-12.2}$
6	$2^{-14.6}$	2^{-21}	$2^{-19.2}$
8	$2^{-17.2}$	2^{-29}	$2^{-26.2}$
10	$2^{-17.3}$	2^{-37}	$2^{-33.3}$

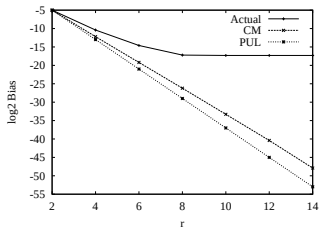

Fig. 1. Comparison of the CM, PUL and actual bias values for $w = 16$ over the key sample used in Table 1. The CM estimates are consistently better than the PUL estimates. But their accuracy too drops exponentially with the number of rounds.

We would like to note that this example application on RC5 is intended to illustrate the practical usage of the theory of correlation matrices; it does not

show the limits of the theory. In fact, it is possible to obtain better estimates than those given in Figure 1 by including multiple-bit trails in bias estimation as well as the single-bit trails. But eventually the accuracy of the estimates should be expected to drop with the increasing number of rounds, since the number of trails that can be considered in bias estimation can be no more than a certain tractable number; but the number of all trails that contribute to the bias of an approximation increases exponentially with the number of rounds.

5.2 Linear Hulls and Correlation Matrices

Like correlation matrices, linear hulls [14] can also be used to combine the bias of linear trails. But unlike correlation matrices, this kind of application of linear hulls is proven specifically for DES-like ciphers[4]. In fact, in the Fundamental Theorem of Linear Hulls (see Appendix B), the summation for the average squared bias is over different key masks, not over linear trails. But since in a DES-like cipher there is a one-to-one correspondence between a linear trail and a key mask, the summation can be transformed into a summation over linear trails (see Theorem 2 in [14]).[5] However, this argument is not equally applicable to all ciphers. For example, for the addition operation $X = Y + K$, the input and output masks for the round are not uniquely determined by the key mask; i.e., for a given $c_i > 1$, there are many values of a_i and b_i such that the approximation $a_i \cdot X = b_i \cdot Y + c_i \cdot K$ has a non-zero bias. So, for example in RC5, there may be many linear trails corresponding to the same key mask c.

In short, we would like to point out that the application of linear hulls to combine bias from linear trails has been proven specifically for DES-like ciphers, and it should not be used with arbitrary ciphers unless a proof is given for that application. In this respect, certain bias studies with linear hulls (e.g. [3, 5]) have no theoretical basis.[6]

Another confusion with the application of linear hulls is that, linear hulls are often taken as the exact analog of differentials in differential cryptanalysis; i.e., it is assumed that $|bias| = \sum_{LT(a,b)} |PUL\ bias|$ where $\sum_{LT(a,b)}$ denotes the summation over all linear trails with plaintext mask a, ciphertext mask b. Obviously, this equation has no basis in the theory of linear hulls.[7] A similar but correct equation is the one given by correlation matrices where bias is taken without absolute value; $bias = \sum_{LT(a,b)} (PUL\ bias)$. So, even though it is wrong to use $\sum_{LT(a,b)} |PUL\ bias|$ for bias estimation, it can be used as an upper-bound for bias in analyzing the security of a cipher against linear cryptanalysis.

[4] For a formal definition of DES-like ciphers for linear hulls, see [14, 13].

[5] This theorem on combining the squared bias of linear trails in a DES-like cipher is recently given an alternative proof by Nyberg [15], which is based on correlation matrices rather than linear hulls.

[6] A mid-solution for these applications can be possible if each trail used in bias estimation can be shown to match a different key mask.

[7] Simply note that every equation in linear hulls is in terms of squared bias rather than the bias itself.

However, the correct reference for this kind of application should be correlation matrices rather than linear hulls.

5.3 Estimation by Sampling

To estimate a parameter of a population where the population is too large to count every member, a random sample from the population can be used to estimate the desired parameter. For a typical block cipher size (e.g. 64 or 128 bits), there are too many plaintext/ciphertext blocks to calculate the actual bias by going over every block; so, a random sample of blocks can be used to estimate the bias. Here we look at a number of alternative statistical estimators for estimating the bias over a random sample of plaintext blocks. Throughout this section, N is the sample size, T is the number of ciphertexts in the sample satisfying the approximation. $E[.]$ denotes the expected value, $Var[.]$ denotes the variance, θ denotes the bias $|p-1/2|$. $\hat{\theta}$ is used for estimators for θ. MSE denotes the mean squared error, $E[(\hat{\theta}-\theta)^2]$.

The UMVUE: One of the most important point estimators in statistics is the uniform minimum variance unbiased estimator (UMVUE), which is the (unique) unbiased estimator that has the minimum variance among all unbiased estimators, under all values of the parameter to be estimated [10]. Regarding the UMVUE, we prove the following negative result:

Theorem 3. *No unbiased estimator exists for $|p-1/2|$ over a random plaintext sample.*

Proof. T is binomially distributed. Assume $\hat{\theta}_N(T)$ is an unbiased estimator[8]:

$$E[\hat{\theta}_N] = \sum_{T=0}^{N} \hat{\theta}_N(T)\binom{N}{T}p^T(1-p)^{N-T} = |p-1/2|, \tag{2}$$

for all $0 \leq p \leq 1$. Now, define $\rho = p/(1-p)$ so that $p = \rho/(1+\rho)$ and $1-p = 1/(1+\rho)$. For $1/2 \leq p < 1$, Equation (2) becomes

$$\sum_{T=0}^{N} \hat{\theta}_N(T)\binom{N}{T}\rho^T = (1+\rho)^{N-1}(\rho-1)/2 = \sum_{T=0}^{N}(\binom{N-1}{T-1} - \binom{N-1}{T})/2\rho^T,$$

$1 \leq \rho < \infty$. A comparison of the coefficients of ρ^T on the left and right sides leads to $\hat{\theta}_N(T) = T/N - 1/2$. Similarly, for $p < 1/2$ we obtain $\hat{\theta}_N(T) = 1/2 - T/N$. Obviously, $\hat{\theta}_N$ cannot satisfy both of these equations. □

Corollary 1. *The UMVUE does not exists for $|p-1/2|$.*

[8] We can denote the estimator as a function of T since T is a sufficient statistics [10] for $|p-1/2|$.

The Sample Bias: It may seem like a good idea to use the sample bias $|T/N - 1/2|$ as an estimator for the actual bias $|p-1/2|$. In this section we show that the sample bias cannot be used to estimate the bias when the sample size is much smaller than $|p-1/2|^{-2}$.

$T/N-1/2$ approximately follows a normal distribution with mean $\mu = p-1/2$ and variance $\sigma^2 = p(1-p)/N \approx 1/4N$. For $\hat{\theta} = |T/N - 1/2|$, it can be shown

$$\begin{aligned} E[\hat{\theta}] &= |\mu|(1 - 2\Phi(-|\mu|/\sigma)) + 2\sigma\phi(|\mu|/\sigma) \\ Var[\hat{\theta}] &= \mu^2 + \sigma^2 - E[\hat{\theta}]^2 \\ MSE(\hat{\theta}) &= E[(\hat{\theta} - \theta)^2] \;=\; Var[\hat{\theta}] + (E[\hat{\theta}] - |\mu|)^2 \\ &= \sigma^2 + 4|\mu|^2\Phi(-|\mu|/\sigma) - 4\mu\sigma\phi(|\mu|/\sigma) \end{aligned}$$

where ϕ and Φ denote respectively the probability density function and the cumulative distribution function for the standard normal distribution. As it can be seen from Figure 2, to have the standard error $\sqrt{MSE}$ at least comparable to $|p-1/2|$, a sample size comparable to $|p-1/2|^{-2}$ will be needed. Therefore, when $|p-1/2|^{-2}$ is an intractably large number (which should be the case for a secure cipher), it will not be possible to obtain a reliable estimator from $|T/N - 1/2|$ with any practical sample size.[9]

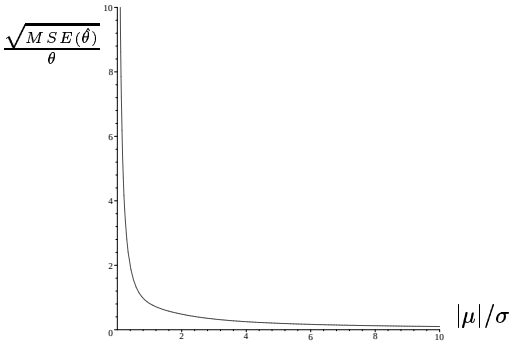

Fig. 2. Standard error rate vs. $|\mu|/\sigma$, for $\hat{\theta} = |T/N - 1/2|$. It converges to $1/(|\mu|/\sigma)$ in both directions. Sample size for a desired error rate $\sqrt{MSE}/\theta \leq e$ can be computed from $|\mu|/\sigma = |p-1/2|\sqrt{4N} \geq 1/e$, hence $N \geq \frac{1}{4e^2}|p-1/2|^{-2}$.

If a sample size much smaller than $|p-1/2|^{-2}$ is used, then $E[\hat{\theta}] \approx 1/\sqrt{2\pi N}$, independent of $|p-1/2|$. As an example, Table 5 gives the results of a computation of the sample bias of the RC5 approximation (1) for $w = 32$ with $N = 10^7$ plaintexts. For this sample size, we have $1/\sqrt{2\pi 10^7} = 2^{-12.95}$, which explains the stabilization of the bias around 2^{-13}.

[9] This sample size requirement should not be confused with the similar plaintext requirement for an attack.

r	2	4	6	8	10	12
Bias	$2^{-6.0}$	$2^{-12.4}$	$2^{-13.0}$	$2^{-13.0}$	$2^{-12.9}$	$2^{-13.0}$

Table 5. Average sample bias of the RC5 approximation (1) for $w = 32$ with 10^7 plaintexts, on 500 randomly chosen keys for each r. The results show an alarmingly high bias for a 64-bit block cipher.

The MLE: Another important point estimator in statistics is the maximum likelihood estimator (MLE). The MLE for $|p - 1/2|$ would be the value $\hat{\theta^*}$ that maximizes the likelihood function

$$L(\hat{\theta}) = \begin{cases} (1/2 - \hat{\theta})^T (1/2 + \hat{\theta})^{N-T} + (1/2 - \hat{\theta})^{N-T} (1/2 + \hat{\theta})^T, & \text{if } \hat{\theta} \neq 0 \\ (1/2)^N, & \text{if } \hat{\theta} = 0 \end{cases} \quad (3)$$

Unfortunately, there is no easy way to compute $\hat{\theta^*}$. Nevertheless, we can obtain a bound on the reliability of the MLE by assuming availability of some extra information, such as whether or not $p > 1/2$. If we know $p > 1/2$, then

$$\hat{\theta^*} = \begin{cases} 0, & \text{if } T < N/2 \\ T/N - 1/2, & \text{otherwise} \end{cases}$$

and vice versa for $p < 1/2$; which is not any more reliable than the sample bias.

6 Conclusions

Looking at the tests summarized in this paper, we conclude that the PUL method gives quite accurate estimates with SP-structured Feistel ciphers, especially for approximations with a single active s-box per round. With increasing number of rounds, the actual bias values follow the PUL estimates quite closely until the PUL estimates become much less than $2^{-\frac{n}{2}}$. After that point the actual bias remains stabilized around $2^{-\frac{n}{2}-1}$ and does not get much lower.

The experiments on RC5 show that the performance of the PUL method may not be as good with other kinds of ciphers. In the case of the RC5 approximation tested, there is a considerable difference between the estimated and actual values even for small number of rounds. At certain cases, the bias is significantly higher than $2^{-\frac{n}{2}}$ even after the estimated values become lower than $2^{-\frac{n}{2}}$. The inaccuracy of the PUL estimates increases with larger block sizes, so even greater differences between actual and estimated values should be expected with 64- and 128-bit blocks.

We analyzed several other techniques for an alternative estimation method that would give more accurate estimates than the PUL method in general. Our attempts to obtain good estimators by statistical techniques from a random sample of plaintext blocks did not provide any useful results, especially when the inverse square of the bias is an impractically large amount for a sample size.

The theory of correlation matrices provides some opportunities for an alternative estimation method. By this theory, it may be possible to obtain improvements over the PUL method by using more than a single trail for bias estimation.

We gave an example of such an application on RC5. The method gave some improvements over the PUL method. But eventually its estimates also fell far from the actual bias values with increasing number of rounds. The main reason for this deviation is that the number of trails that can be considered in bias estimation can be no more than a certain tractable number; but the number of all trails that contribute to the bias of an approximation increases exponentially with the number of rounds.

Another theory used as an alternative method for bias estimation is the theory of linear hulls. In Section 5.2, we pointed out some problems with the current applications of this theory. The main problem with the current practice is that, the theoretical results on linear hulls regarding combining the bias of different linear trails is proven only for DES-like ciphers, whereas in practice these results are used for different kinds of ciphers (e.g., RC5, RC6, SAFER).

We conclude that the PUL method is quite an effective method for bias estimation with SP-structured Feistel ciphers, especially for approximations with at most one active s-box at each round and with a bias considerably higher than $2^{-\frac{n}{2}}$. It is an open problem to find an equally effective method for non-Feistel ciphers and for the ciphers with too many rounds for the PUL method to give a meaningful value.

Acknowledgments

I would like to thank Kaisa Nyberg for her comments on linear hulls, to Erkan Türe for his help with the statistics and especially for reference [10], and to Ali Bıçak, Matt Robshaw, and Lisa Yin for many helpful comments on the paper.

References

[1] Ross Anderson, Eli Biham, and Lars Knudsen. Serpent: A Proposal for the Advanced Encryption Standard. Available from http://www.nist.gov/aes.

[2] Uwe Blöcher and Markus Dichtl. Problems with the linear cryptanalysis of DES using more than one active S-box per round. In *Fast Software Encryption*, 1994.

[3] Johan Borst, Bart Preneel, and Joos Vandewalle. Linear cryptanalysis of RC5 and RC6. In *Fast Software Encryption, 6th International Workshop*, 1999.

[4] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In *Advances in Cryptology—Eurocrypt'94*. Springer-Verlag, 1994.

[5] S. Contini, R. Rivest, M. Robshaw, and L. Yin. The Security of the RC6 Block Cipher. Available from http://www.rsasecurity.com/rsalabs/aes.

[6] Don Coppersmith. The Data Encryption Standard (DES) and its strength against attacks. *IBM Journal of Research and Development*, May(3):243–250, 38 1994.

[7] Joan Daemen, René Govaerts, and Joos Vandewalle. Correlation matrices. In *Fast Software Encryption, Second International Workshop*. Springer-Verlag, 1994.

[8] Burton S. Kaliski Jr. and Yiqun Lisa Yin. On differential and linear cryptanalysis of the RC5 encryption algorithm. In *Advances in Cryptology—Crypto'95*.

[9] Burton S. Kaliski Jr. and Yiqun Lisa Yin. On the security of the RC5 encryption algorithm. Technical Report TR-602, Version 1.0, RSA Laboratories, 1998.

[10] E. L. Lehmann and George Casella. *Theory of Point Estimation*. Springer Texts in Statistics. Springer-Verlag, 2nd edition, 1998.
[11] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology—Eurocrypt'93*. Springer-Verlag, 1993.
[12] Mitsuru Matsui. The first experimental cryptanalysis of the Data Encryption Standard. In *Advances in Cryptology—Crypto'94*. Springer-Verlag, 1994.
[13] Mitsuru Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. In *Fast Software Encryption*, 1996.
[14] Kaisa Nyberg. Linear approximation of block ciphers. In *Advances in Cryptology—Eurocrypt'94*. Springer-Verlag, 1994.
[15] Kaisa Nyberg. Correlation theorems in cryptanalysis. To appear in *Discrete Applied Mathematics*.
[16] Ali Aydın Selçuk. New results in linear cryptanalysis of RC5. In *Fast Software Encryption, 5th International Workshop*. Springer-Verlag, 1998.

A Chabaud-Vaudenay Theorem on Max. Non-Linearity

Theorem 4 (in Chabaud-Vaudenay [4]) *For $K = \{0,1\}$ and $F : K^p \to K^q$,*

$$\Lambda_F \geq \frac{1}{2}\left(3 \times 2^p - 2 - 2\frac{(2^p-1)(2^{p-1}-1)}{2^q-1}\right)^{1/2}$$

where $\Lambda_F = \max_{b \neq 0, a} \left| \, |\{x \in K^p \, : \, a \cdot x \oplus b \cdot F(x) = 0\}| - \frac{|K^p|}{2} \, \right|$.

B Fundamental Theorem of Linear Hulls

Theorem 1 (in Nyberg [14]) *For $X \in \{0,1\}^m$, $K \in \{0,1\}^\ell$, $F : \{0,1\}^m \times \{0,1\}^\ell \to \{0,1\}^n$, if X and K are independent random variables, and K is uniformly distributed, then for all $a \in \{0,1\}^m$, $b \in \{0,1\}^n$*

$$2^{-\ell} \sum_{k \in \{0,1\}^\ell} |P_X(a \cdot X \oplus b \cdot F(X,k) = 0) - \frac{1}{2}|^2 \;\; = \;\; \sum_{c \in \{0,1\}^\ell} |P_{X,K}(a \cdot X \oplus b \cdot F(X,K) \oplus c \cdot K = 0) - \frac{1}{2}|^2$$

During a linear attack, the key K is a fixed parameter, so the bias of interest is the bias on the left side of the equation; i.e., $|P_X(a \cdot X \oplus b \cdot F(X,k) = 0) - \frac{1}{2}|$.[10] The summation on the right is the squared bias with a random-variable key, over all key masks c. For DES-like ciphers, this right-hand side summation can be turned into a summation of the PUL bias over linear trails (Theorem 2 in [14]).

[10] The key mask does not matter here since the key is fixed.