On Non-Monotonicity of the Success Probability in Linear Cryptanalysis

Ali Aydın Selçuk

Dept. of Computer Engineering
TOBB University of Economics and Technology
Ankara, Turkey
aselcuk@etu.edu.tr

Abstract. Like any other cryptanalytic attack, the success rate of a linear attack is expected to improve as more data becomes available. Bogdanov and Tischhauser (FSE 2013) made the rather surprising claim that the success rate of a linear attack may go down with increasing plaintext amount, after an optimal point. They supported this claim with experimental evidence by an attack on SmallPresent-20. Different explanations have been given to explain this surprising phenomenon. In this note, we give quantitative values regarding when this phenomenon can be observed. We conclude that it should not be an issue for attacks in practice except for those with a tiny bias.

Keywords: Linear cryptanalysis · success probability · non-monotonicity.

1 Introduction

A linear cryptanalytic attack aims to recover a portion of the last round key of a block cipher by trying possible subkey values with a large number, denoted by N, of plaintext-ciphertext blocks in a linear equation ("approximation") [6]. The approximation is a probabilistic binary equation with a non-negligible correlation, with a probability $p \neq 1/2$. Its strength is indicated by its "bias", $\epsilon = p - 1/2$. The traditional assumption in linear cryptanalysis has been that, when the right key is tried over the plaintext sample, the approximation will demonstrate a bias close to ϵ. However, when a wrong key value is tried, it will randomize the outcome of the approximation, and hence the bias observed will be practically 0. This was the traditional "wrong key randomization hypothesis."

Bogdanov and Tischhauser [5] studied the wrong key randomization hypothesis in more detail, and gave a more accurate model of the bias for wrong key values. Using this model, they obtained a more accurate formulation of the success probability, which they validated by experimental results [5, 4].

A more surprising claim in [5] was regarding the non-monotonic behavior of the success probability with an increasing amount of plaintext provided: Using their new formula for the success probability, they calculated a local optimum for the number of plaintexts, N_0, and claimed that the success rate of the attack

would deteriorate when $N > N_0$. They supported this claim by an experimental attack on SmallPresent-20.

Later, Ashur et al. [2, 1] contested this claim. They gave the following explanation for the non-monotonic behavior observed in the experiments of [5]: Let m denote the bit length of the round key portion under attack and a denote the aimed advantage level of the attack. (I.e., the attack's aim is to get the right key value ranked within the top 2^{m-a} out of 2^m key candidates tried.) When the bias of the approximation is so low that the right key's bias is not sufficient to put it within the top 2^{m-a} key candidates (i.e., there are 2^{m-a} or more wrong keys with a random bias that dominate the right key in the approximation), the success rate of the attack will deteriorate with increasing N, as it should. But the non-monotonicity claim is true only for approximations with such a low bias.

More recently, Samajder and Sarkar [7] presented a more complex, statistical analysis of the non-monotonicity phenomenon.

In this paper, we aim to clarify the confusion surrounding the non-monotonicity claim. We point out a misinterpretation in [5]. Our findings support the view of [2], namely that non-monotonicity of the success probability can be an issue only when the approximation has an extremely small bias.

2 Non-Monotonicity of the Success Probability

In the traditional approach in linear cryptanalysis, the bias of an approximation with a wrong key value substituted had been assumed to be 0. This assumption was challenged by Bogdanov and Tischhauser [5] who gave a more accurate model, known as the "adjusted wrong key randomization hypothesis."

Let n be the block length of the cipher, p be the probability of the approximation, and $\epsilon = p - 1/2$ be its bias (taken without the absolute value). Let ϵ_w denote the approximation's bias for a wrong key value, as a random variable with respect to the random wrong key. The adjusted wrong key randomization hypothesis can be summarized as follows:

$$\epsilon_w \sim \mathcal{N}(0, 2^{-n-2}), \tag{1}$$

where $\mathcal{N}(\mu, \sigma^2)$ denotes the normal distribution with mean μ and variance σ^2.

Bogdanov and Tischhauser [5] revised the success probability formula given by Selçuk [8] accordingly and obtained a more accurate formula:

$$P_S \approx \Phi\left(2\sqrt{N}|\epsilon| - \sqrt{1 + \frac{N}{2^n}}\Phi^{-1}(1 - 2^{-a-1})\right). \tag{2}$$

Taking the first derivative of (2) w.r.t. N, they obtained the relative extremum[1],

$$N_0 = \frac{4\epsilon^2 2^{2n}}{(\Phi^{-1}(1 - 2^{-a-1}))^2 - 4\epsilon^2 2^n}. \tag{3}$$

[1] As we checked with the authors [3], the power $2n$ in the denominator was a typo and should instead be n, as we write here.

They interpreted this to be the optimum data amount for a linear attack.

They presented the results of an experimental attack to support this claim: They implemented an attack on SmallPresent-20 using a linear approximation with bias $|\epsilon| = 2^{-10}$, aiming an advantage of $a = 12$ bits. The attack's success rate obtained a peak value of $P_S = 0.0011$ with $N = 2^{18.75}$ plaintexts and then deteriorated with more plaintexts used.

They attributed this non-monotonic behavior of the success probability to the increasing noise with increasing data; "the probability of duplicates increases with N, up to a point where adding more samples to the statistic only amplifies the noise." [5].

3 A More Critical Look

If we look at the denominator of (3) carefully, we see that the denominator will be negative as long as $\Phi^{-1}(1 - 2^{-a-1}) < |\epsilon|\, 2^{n/2+1}$. The inverse normal Φ^{-1} is a very slowly growing function, and in most attacks in practice we will have $\Phi^{-1}(1 - 2^{-a-1}) < 8$. Numeric values of Φ^{-1} are demonstrated in Table 1.

Table 1. Slow increase of Φ^{-1} for exponentially decreasing tail.

q	$\Phi^{-1}(1-q)$
2^{-10}	3.097
2^{-20}	4.763
2^{-30}	6.009
2^{-40}	7.048
2^{-50}	7.956

Provided that the approximation's bias $|\epsilon|$ is significantly greater than $2^{-n/2}$ (e.g., $4\ 2^{-n/2}$ or larger), which is needed anyway to have a viable linear attack, the denominator of (3) and hence the N_0 value obtained will be negative! A similar check of the second derivative reveals it to be positive under these conditions, indicating a relative minimum rather than a maximum.

4 Discussion

As mentioned above, the experiment in [5] used to verify the non-monotonicity claim had parameters $n = 20$, $|\epsilon| = 2^{-10}$, and $a = 12$, yielding a small success probability of at most $P_S = 0.0011$. These results are very much in line with our findings: The attack has a tiny bias, with $|\epsilon| = 2^{-n/2}$, and a small success chance of 0.1%.

At this juncture, we would like to point out that a bias of $2^{-n/2}$ is only slightly above the expected bias of a random approximation, and hence almost trivial:

Given that a random approximation's bias is distributed with $\mathcal{N}(0, 2^{-n-2})$, the mean of its absolute value is,

$$\sqrt{\frac{2}{\pi}}\, 2^{-\frac{n}{2}-1} \;\approx\; 0.4\, 2^{-\frac{n}{2}}.$$

As Ashur et al. [2, 1] argued, such a low bias as in the experiment of [5] was insufficient to rank the right key among the top 2^{m-a} wrong keys. Hence it was just natural that the success rate deteriorated with the increasing number of plaintexts.

As a final remark, we would like to note that the condition for monotonicity of the success probability, $|\epsilon| > 2^{-n/2-1}\Phi^{-1}(1 - 2^{-a-1})$, coincides exactly with that derived by Ashur et al. in Theorem 1 of [2] using a different approach.

5 Conclusion

In this brief note, we tried to clarify the non-monotonicity phenomenon that has been a matter of discussion in linear cryptanalysis over the past couple of years. We conclude that it is an issue only when the bias is so small that $|\epsilon| \leq c\, 2^{-n/2}$, where c is some small coefficient such as 4. Since linear attacks typically use approximations with a bias $|\epsilon| \gg 2^{-n/2}$, non-monotonicity of the success probability should not be an issue for such attacks in practice.

Acknowledgments

I would like to thank Andrey Bogdanov, Cihangir Tezcan, and Fatih Sulak for helpful discussions and constructive comments.

References

1. Ashur, T.: Cryptanalysis of Symmetric-Key Primitives. Ph.D. thesis, K. U. Leuven (12 2017)
2. Ashur, T., Beyne, T., Rijmen, V.: Revisiting the wrong-key-randomization hypothesis. Tech. Rep. 2016/990, IACR Cryptology ePrint Archive (2016)
3. Bogdanov, A.: Personal communication (9 2016)
4. Bogdanov, A., Kavun, E.B., Tischhauser, E., Yalçin, T.: Large-scale high-resolution computational validation of novel complexity models in linear cryptanalysis. J. Computational Applied Mathematics **259**, 592–598 (2014)
5. Bogdanov, A., Tischhauser, E.: On the wrong key randomisation and key equivalence hypotheses in matsui's algorithm 2. In: Fast Software Encryption - FSE 2013, Proceedings. pp. 19–38 (2013)
6. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Advances in Cryptology - EUROCRYPT '93, Proceedings. pp. 386–397 (1993)
7. Samajder, S., Sarkar, P.: Another look at success probability in linear cryptanalysis. Tech. Rep. 2017/391, IACR Cryptology ePrint Archive (2017)
8. Selçuk, A.A.: On probability of success in linear and differential cryptanalysis. J. Cryptology **21**(1), 131–147 (2008)