Blondeau, Celine; Nyberg, Kaisa

Improved Parameter Estimates for Correlation and Capacity Deviates in Linear Cryptanalysis

Published in:
IACR Transactions on Symmetric Cryptology

DOI:
10.13154/tosc.v2016.i2.162-191

Published: 01/01/2017

Document Version
Publisher's PDF, also known as Version of record

Improved Parameter Estimates for Correlation and Capacity Deviates in Linear Cryptanalysis

Céline Blondeau and Kaisa Nyberg

Department of Computer Science, Aalto University School of Science, Finland
celine.blondeau@aalto.fi,kaisa.nyberg@aalto.fi

Abstract. Statistical attacks form an important class of attacks against block ciphers. By analyzing the distribution of the statistics involved in the attack, cryptanalysts aim at providing a good estimate of the data complexity of the attack. Recently multiple papers have drawn attention to how to improve the accuracy of the estimated success probability of linear key-recovery attacks. In particular, the effect of the key on the distribution of the sample correlation and capacity has been investigated and new statistical models developed. The major problem that remains open is how to obtain accurate estimates of the mean and variance of the correlation and capacity. In this paper, we start by presenting a solution for a linear approximation which has a linear hull comprising a number of strong linear characteristics. Then we generalize this approach to multiple and multidimensional linear cryptanalysis and derive estimates of the variance of the test statistic. Our simplest estimate can be computed given the number of the strong linear approximations involved in the offline analysis and the resulting estimate of the capacity. The results tested experimentally on SMALLPRESENT-[4] show the accuracy of the estimated variance is significantly improved. As an application we give more realistic estimates of the success probability of the multidimensional linear attack of Cho on 26 rounds of PRESENT.

Keywords: block cipher · linear cryptanalysis · key-recovery attack · multidimensional linear attack · multiple linear attack · key-dependency · correlation · capacity · known plaintext · distinct known plaintext · statistical model.

1 Introduction

1.1 Background and Previous Work

Statistical cryptanalysis of block ciphers have traditionally used sampling models under the hypothesis of statistical equivalence of keys. On the other hand, many modern ciphers have been shown not to obey this hypothesis, which causes doubts about the validity of the cryptanalytic results. In order to compute accurate cryptanalysis estimates the statistical models must be improved, and, in addition to the data, also the key must be integrated in the statistical model of the cipher.

Such development has taken place also for linear cryptanalysis and its extensions. Previously, most statistical models used in linear attacks determine and exploit distributions of the observed correlation with a fixed key and taking only the data as random variable. Then it is assumed that for all cipher keys, the distributions for wrong key candidates are identical, and similarly, that the distributions obtained with the correct key are identical. This practice may be due to the fact that for most ciphers, it is feasible to compute the expected value of a linear correlation, but estimating the variance is difficult. Previously, in [DR06, DR07] the authors provide experiments to show that also significant variances occur, and stress that the importance of the variance and of the expected linear potential

IACR Transactions on Symmetric Cryptology ISSN 2519-173X, Vol. 2016, No. 2, pp. 162–191
DOI:10.13154/tosc.v2016.i2.162-191

(ELP) of the linear correlation. In particular, they present an estimate of the variance of the correlation in the wrong-key case. In [BT13], this influence of the wrong-key variance for the classical linear attack was taken into consideration and a better estimate of the data complexity of a linear attack was obtained and demonstrated in experiments. In [HVLN15], the distribution of the capacity for the right encryption key was established and was used to determine weak-key quantiles, that is, lower bounds of capacity that are satisfied by a given proportion, say one half, or 30% of the keys. Such approach was previously taken in [Lea11, CW16] in the case of single linear hull.

In [BN15a] a complete treatment on the statistical distributions of linear attack test statistics, that is, the empirical correlations and capacities, was presented by considering both the data and the key as random variables. In this work, the different sampling models in linear cryptanalysis, that is, the known plaintext (KP) and the distinct known plaintext (DKP) models in linear cryptanalysis were studied for general multiple and multidimensional linear cryptanalysis. The first version of this work, completing [BN15b], was posted in September 2015. While it provided complete statistical models that were shown to comply well with practical examples if real parameter values were used, this version failed to provide accurate methods for computing estimates of the expected value and variance of capacity. Even worse, using the capacity estimate provided by Cho, this model was giving some too groundless doubts about the validity of the multidimensional linear attack of [Cho10] on 26 rounds of PRESENT.

The reason for this failure was that the capacity of the linear approximations is underestimated in the offline analysis, since only the most dominant characteristics and approximations can be taken into account. In a comment on this problem, Bogdanov pointed out that also many weaker linear characteristics contribute to the total correlation at least as much as random noise [Bog16]. While the model of [BN15a] correctly estimates the expected capacity of ℓ linear approximations for random n-bit cipher to be equal to $\ell 2^{-n}$, it fails to consider the corresponding random behavior due to the weak characteristics of the linear approximations. Since the estimated capacity for the right key [Cho10] given in the first version of [BN15a] is then smaller than the one for the wrong keys, the attack on 26 rounds seems to fail. In reality, if the impact of the weak linear characteristics is taken into account, even if not more than random noise for all involved linear approximations, the capacity estimate will never be less than the capacity of random linear approximations.

It is interesting to note that the insufficiency of the single-bit characteristics in PRESENT for providing accurate values of the correlations of linear approximations was previously observed in [AÅBL12] particularly as the number of rounds is increasing. It was concluded that then also characteristics with two- or three-bit masks must be taken into account. An alternative approach taken in this paper is to model the effect of higher-weight characteristics as a linear approximation of a random cipher. This approach is computationally much lighter, and seems to work well for the purposes of linear cryptanalysis.

The methodology for estimating the variance of capacity used in [BN15a] was the same as in [HVLN15]. In the experiments done on SMALLPRESENT it was shown to give an underestimate of the variance, particularly in the case of multidimensional linear cryptanalysis. In the first version of [BN15a] this problem was identified and discussed. The method is based on the assumption that the correlations of all linear approximations involved in the attack are independent and have equal ELP. Since this is quite unrealistic in the multidimensional case, an improved method was briefly sketched. The idea was to separate between the sets of linear approximations used in the offline analysis and in the actual online attack. The main advantage of this approach is that no independence assumption needs to be imposed on the linear approximations used in the multidimensional cryptanalysis. Only a (usually small) subset of linear approximations used in offline analysis, such as a linearly independent set of so-called base approximations, must be

assumed to be statistically independent. This solution is not included in the published version [BN16] of the work [BN15a]. The full description of this method is now part of Section 3 and comparison is provided in Subsection 4.3.

Relation to previous work by Vejre et al. The key-variance of the capacity was first considered in [BLNW12] in the case of attacks with zero correlation. The starting point of the work of Vejre et al. [Bog16,Vej16,BTV16] was to incorporate the variance of correlations to the capacity value and variance estimates and to apply the signal/noise approach, as was also done already in [BT13] for single linear cryptanalysis. The introduction of the noise-based capacity value and variance estimates provided by this paper are due to Vejre et al. They can be considered essentially as a special case of [Vej16] with zero covariances and considering an equal number of approximations in the offline and online analysis.

1.2 Contributions of this Paper

The main goal of this paper is to solve the issues discovered in the treatment of the first version of [BN15a] and left open in [BN16]. Although there are generic approaches how to estimate a correlation of a linear approximation for a given block cipher, the details depend crucially on the structure of the cipher. The same is true even more when the goal is to estimate the expected value or the variance of the capacity. In this paper we present solutions to an iterated key-alternating block cipher. The proofs are given under the assumption of a long-key cipher, that is, a cipher with independent round keys. The results are tested in experiments also for other key-schedules.

To carry out this analysis we need some basic properties of correlations of linear approximations and their distributions. Therefore, we start by presenting a statistical model of the linear key-recovery attack in the case of one linear approximation that has a number of dominant characteristics. When the linear approximation has many dominant trails as described in [BT13], it is often the case that the correlation of the linear approximation is close to zero. In this paper we present, to the best of our knowledge, the first estimate of the data complexity of a simple linear attack when the expected value of the correlation of the linear approximation equals zero. The classical case of a single dominant characteristic was presented in [BN16]. In that case the probability distribution of the right-key correlation is modeled as a union of two normal distributions that are symmetric with respect to zero. As the number of dominant characteristics increases the number of normal distributions increases and their union can be modeled using a single normal distribution with mean close, or equal to zero. By integrating the key as a random variable in both the wrong key and right key case and modeling the effect of weak characteristics as random noise, we accomplish the work done in [BT13] and give the success probability of the key-recovery attack using the hypothesis testing distinguisher. The results are provable for long-key iterated block ciphers. To test our model we have done experiments on 20 rounds of SIMON32/64 and compared it with the previous models [Sel08,BT13].

This case also demonstrates the crucial role of ELP in linear cryptanalysis as stated in [DR06]. Even if the expected correlation is equal to zero, that is, the same as in the random case, distinguishing from random is still possible depending on the ELP (variance) of the correlation. This fact underlines the importance of getting the variance estimates accurately.

We then proceed by presenting an improved capacity estimate of an iterated block cipher in multiple or multidimensional linear cryptanalysis by replacing the effect of missing characteristics by independent noise. We show that the quantity computed in [Cho10] using the matrix method is not a valid capacity estimate in the key-dependent model. By adding the noise factor, the expected capacity for the right key is always larger than the

one for the wrong keys. The validity of the multidimensional linear attack on 26 rounds of PRESENT hence depends on the variance of the capacity.

The open problem from [BN16] of how to properly estimate the variance of capacity is then resumed. As outlined in that preliminary work, the sets of linear approximations used in offline and online analysis typically differ, in particular, when the multidimensional linear attack is concerned. We derive the formula of the estimated variance under the assumption that, over the key, the correlations of the strong linear approximations used in the offline analysis are independent and normally distributed with mean equal to zero. In addition to being conceptually easy to handle in theory, this basic model captures the behavior of the PRESENT cipher quite accurately. It is also computationally feasible in practice. The simplest variance estimate can be computed given the number of the strong linear approximations involved in the offline analysis and the capacity estimate.

Using the new formula of the capacity estimate and of its variance we show that Cho's attack on 26 rounds of PRESENT is still valid and give realistic estimates of its success probability.

The theoretical results are backed up by several experiments. The main new results of this paper are summarized in Theorem 2 where a new estimate of the success probability and data complexity for a linear key-recovery attack is provided, and in Theorem 4 and Theorem 5, where improved estimates of the capacity deviate are provided. In addition, we present an extended comparison with the previous related work. The different experimental results illustrate the improvements in the correlation and capacity deviate estimates. The most visual experimental results are provided in Figure 4 and Figure 5.

Outline. The outline of this paper is as follows. In Section 2 we introduce the necessary notation, determine the data-complexity of a linear attack using several strong linear characteristics and explain how to use noise to estimate the mean and the variance of the correlation in this case. In Section 3 we focus on the multiple and multidimensional linear cryptanalysis. Based on experiments, we show that the new estimate of the key-variance of the capacity is more accurate than the previous ones. In Section 4 we use the new estimate to derive more accurate data complexity estimate for multiple and multidimensional linear cryptanalysis. The theory developed in this paper is backed by experiments in Section 5. Section 6 concludes this paper.

2 Linear Attacks

2.1 Key-Alternating Cipher and Key-Recovery Attack

An iterated key-alternating block cipher with block size of n bits processes plaintext $x \in \{0,1\}^n$ and expanded key $K' = (k_0, \ldots, k_{r'})$ by iterating a round function g to obtain ciphertext y. For simplicity of notation, we restrict to the case where $k_i \in \{0,1\}^n$ as depicted in Figure 1. In some parts of this paper, the proofs are derived for a cipher with independent round keys. We refer to such cipher as a long-key key-alternating cipher [DR07].

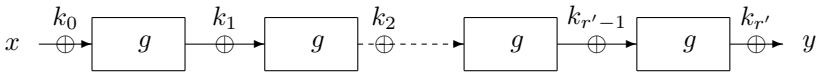

Figure 1: Key-alternating block cipher of r' rounds with round function g and expanded encryption key $(k_0, k_1, \ldots, k_{r'})$

A statistical attack can be performed when one has detected a statistical property that can be observed from some quantity computed from the cipher data. Let us denote by E'_K

this part of the cipher. The cipher E_K is then written as $E_K(x) = (H_K \circ E'_K \circ G_K)(x)$ where G_K and H_K represent respectively the first and last rounds, and E'_K corresponds to $r < r'$ iterations of the round function g.

In the classical linear cryptanalysis, the property in consideration is a biased linear combination of input and output bits over E'_K. Given a vector u in the input space and a vector v in the output space of E'_K, the Boolean function $u \cdot x \oplus v \cdot E'_K(x)$ is called the linear approximation over E'_K with input mask u and output mask v. Its strength is measured by its correlation. In general, we call the quantity

$$\begin{aligned}&\mathrm{cor}(u \cdot x + v \cdot f(x)) = \\ &2^{-n}\Big[\#\left\{x \in \{0,1\}^n | \, u \cdot x + v \cdot f(x) = 0\right\} - \#\left\{x \in \mathbb{F}_2^n | u \cdot x + v \cdot f(x) = 1\right\}\Big].\end{aligned}$$

the correlation of the linear approximation $u \cdot x + v \cdot f(x)$ of a vectorial Boolean function f of n variables. For brevity, we use the following notation

$$c(u, v)(K) = \mathrm{cor}(u \cdot x + v \cdot E'_K(x)).$$

In the offline analysis of the cipher, the attacker selects a linear approximation (u, v). In the classical linear cryptanalysis by Matsui [Mat93] the linear approximation is selected such that $c(u, v)(K)$ is large in absolute value, for all K. This is possible if the linear approximation has a single dominant characteristics. In the general case, it is required that the ELP is large, where $ELP = \mathrm{Exp}_K\left(c(u, v)(K)^2\right)$, see Subsection 2.3.

In the online analysis, we want to extract a part of the encryption key K. Let us denote this part of K by K_0. For this purpose, the attacker has chosen u and v in such a way that there exist some truncation $\widetilde{G_{K_0}}$ and $\widetilde{H^{-1}_{K_0}}$ of the outer round mappings G_K and H_K^{-1}, respectively, such that they depend only on K_0 and that

$$u \cdot \widetilde{G_{K_0}}(x) = u \cdot G_K(x) \text{ and } v \cdot \widetilde{H^{-1}_{K_0}}(y) = v \cdot (E'_K \circ G_K)(x),$$

for all plaintexts x and ciphertexts $y = E_K(x)$.

We denote by D the sample of N plaintexts and by κ the candidate key used in the attack and define the statistic $\hat{c}(D, K, \kappa)$ as follows

$$\begin{aligned}\hat{c}(D, K, \kappa) \;&=\; \frac{1}{N}\Big[\#\left\{x \in D | \, u \cdot \widetilde{G_\kappa}(x) + v \cdot \widetilde{H_\kappa^{-1}}(y) = 0\right\} \\ &-\; \#\left\{x \in D | u \cdot \widetilde{G_\kappa}(x) + v \cdot \widetilde{H_\kappa^{-1}}(y) = 1\right\}\Big].\end{aligned} \tag{1}$$

Further, let us make the following notation

$$\hat{c}(D, K, \kappa) = \begin{cases} \hat{c}_W(D, K, \kappa), & \text{if } \kappa \neq K_0, \\ \hat{c}_R(D, K), & \text{if } \kappa = K_0. \end{cases} \tag{2}$$

Then for the right key, the outer round computations are cancelled and the statistic can be expressed as follows

$$\hat{c}_R(D, K) = \frac{1}{N}\Big[\#\left\{x \in D | \, u \cdot x + v \cdot E'_K(x) = 0\right\} - \#\left\{x \in D | u \cdot x + v \cdot E'_K(x) = 1\right\}\Big].$$

2.2 Distribution of Correlation of Long-Key Cipher

In general, the correlation over the r-round part E'_K of a key-alternating block cipher E_K depicted in Figure 1 can be written as

$$c(u, v)(K) = \mathrm{cor}(u \cdot x + v \cdot E'_K(x)) = \sum_{\substack{\tau \\ \tau_0 = u,\, \tau_r = v}} (-1)^{\tau \cdot K} \prod_{i=1}^{r} \mathrm{cor}(\tau_{i-1} \cdot z + \tau_i \cdot g(z)), \tag{3}$$

where the sum is taken over all r-tuples $\tau = (\tau_0, \tau_1, \ldots, \tau_r)$, where $\tau_0 = u$ and $\tau_r = v$. Such a sequence τ is called a linear characteristic of the linear approximation (u, v) and the quantity

$$\prod_{i=1}^{r} \mathrm{cor}(\tau_{i-1} \cdot z + \tau_i \cdot g(z))$$

is called the correlation of the characteristic τ. A linear approximation is said to have a single dominant characteristic if there is a characteristic $t = (t_0, t_1, \ldots, t_r)$ such that the absolute value of its correlation is large and

$$\Big| \prod_{i=1}^{r} \mathrm{cor}(t_{i-1} \cdot z + t_i \cdot g(z)) \Big| \approx |c(u, v)(K)|,$$

for all K, and all other characteristics $\tau \neq t$ have equally small or zero correlations. Originally Matsui [Mat93] describes linear attacks for linear approximations with single dominant characteristic. This case was revisited and the key variable integrated in the model in [BN15a, BN16].

Nowadays, many ciphers are designed in such a way that all linear approximations comprise several dominant characteristics. As the number of dominant characteristics grows the correlation as expressed in Equation 3 will take several different values, depending of the encryption key, with non-negligible absolute value. As the number of rounds increases it becomes unfeasible since the number of equally dominant characteristics increases. It was shown in [RN13] that it is possible to distinguish between different values of correlations up to seven rounds of PRESENT. In particular, it means that for an increasing number of encryption keys the correlation will be equal, or close, to zero. Still, linear cryptanalysis may be possible.

The goal of this section is to give a statistical model of linear cryptanalysis using such a linear approximations. We follow the theory developed in [DR07, BT13]. The proofs are presented for a long-key cipher. We start by stating the following general property.

Lemma 1. *Suppose that (u, v) is a linear approximation of a long-key block cipher. Then*

$$\mathrm{Exp}_K(\, c(u, v)(K)) = 0 \quad \textit{and} \quad \mathrm{Var}_K(\, c(u, v)(K)) = ELP.$$

Many authors have performed extensive experiments to study the shape of the distribution of the correlation of a linear approximation [DR07, AÅBL12, BT13, RN13]. Most researchers agree that in practical cryptanalysis of most contemporary ciphers it is quite realistic to assume that the shape of the distribution is normal. We also make that assumption throughout this work.

2.3 Data Complexity of the Attack

Although the correlation has an expected value close to or equal to zero, that is, equal to the expected value of a random correlation, it can still be distinguished from random thanks to its larger variance. In this section, we recall the hypothesis testing approach for key recovery by distinguishing distributions, and then apply it to determine the success probability of a key-recovery attack using a linear approximation with several dominant characteristics.

The aim of the classical key-recovery attack is to distinguish a part of the encryption key, which we call the right key, from wrong key candidates as explained in Subsection 2.1. To estimate the data complexity of the attack it is then necessary to know the distribution of the involved random variables. In the classical linear context, the variables $\hat{c}_W(D, K, \kappa)$ and $\hat{c}_R(D, K)$, as defined by Equation 2 for the wrong and right keys, are assumed to

be normal deviates. Under this assumption, a new expression of the parameters of these normal distributions when both the deviation from the data and the key are taken into consideration was derived in [BN15a, BN16]. The estimates were obtained simultaneously for attacks in the known plaintext (KP) and distinct known plaintext (DKP) model. To state the result of [BN16] we introduce a constant B defined as follows

$$B = \begin{cases} 1, & \text{for KP,} \\ \dfrac{2^n - N}{2^n - 1}, & \text{for DKP.} \end{cases} \tag{4}$$

Let us denote by c the expected value of $c(u, v)(K)$ taken over K. Then by Theorem 5 of [BN16] it is known that $\hat{c}_R(D, K)$ has the following mean and variance

$$\mathrm{Exp}_{D,K}(\hat{c}_R(D, K)) = c \quad \text{and} \quad \mathrm{Var}_{D,K}(\hat{c}_R(D, K)) = \frac{B}{N} + ELP - c^2.$$

If moreover the number of dominating characteristics is large then the distribution of $\hat{c}_R(D, K)$ has a normal shape.

In [BT13] (see also [BN16]) it was proved that $\hat{c}_W(D, K, \kappa)$ follows a normal distribution with mean and variance, respectively, as

$$\mu_W = 0 \quad \text{and} \quad \sigma_W^2 = \frac{B}{N} + 2^{-n}.$$

By Lemma 1 we summarize these results for a long-key cipher as follows.

Theorem 1. *Given a linear approximation of a long key-cipher let us assume that its correlation $c(u, v)(K)$ is normally distributed. Then the empirical correlations $\hat{c}_R = \hat{c}_R(D, K)$ and $\hat{c}_W = \hat{c}_W(D, K, \kappa)$ are normal deviates with parameters*

$$\mu_R = 0 \quad \textit{and} \quad \sigma_R^2 = \frac{B}{N} + ELP,$$
$$\mu_W = 0 \quad \textit{and} \quad \sigma_W^2 = \frac{B}{N} + 2^{-n}.$$

Note that in the DKP context, we have $\frac{B}{N} + 2^{-n} \approx \frac{1}{N}$ and the expression of this variance estimate can be simplified accordingly.

In this case μ_R and μ_W are equal as both are equal to zero. Then the derivation of the success probability and data complexity estimate is different than in previous cases [Sel08, BT13, BN16] for a classical linear attack. An example distribution is plotted in Figure 2. Even if $\mu_R = \mu_W = 0$ the difference between the variances makes it possible to distinguish the right key from the wrong ones. On the left side, we illustrate the statistical inference based on the observed correlation $\hat{c}(D, K, \kappa)$. Then if it is smaller than the threshold $-\Theta$, or larger than Θ, the key candidate κ is likelier to be the right key $\kappa = K_0$ than a wrong key. An alternative way of doing this inference is to consider the square correlations. In that case, the observed correlations $\hat{c}_R(D, K)$ in the right-key and $\hat{c}_W(D, K)$ in the wrong-key case when squared and divided by their variances follow a χ^2 distributions with one degree of freedom. It means that $\hat{c}_R^2 = \hat{c}_R(D, K)^2$ and $\hat{c}_W^2 = \hat{c}_W(D, K, \kappa)^2$ follow Gamma distributions and have means and variances as follows

$$\mathrm{Exp}_{D,K}\left(\hat{c}_R^2\right) = \frac{B}{N} + ELP \quad \text{and} \quad \mathrm{Var}_{D,K}\left(\hat{c}_R^2\right) = 2\left(\frac{B}{N} + ELP\right)^2,$$
$$\mathrm{Exp}_{D,(K,\kappa)}\left(\hat{c}_W^2\right) = \frac{B}{N} + 2^{-n} \quad \text{and} \quad \mathrm{Var}_{D,(K,\kappa)}\left(\hat{c}_W^2\right) = 2\left(\frac{B}{N} + 2^{-n}\right)^2.$$

The parameters of the Gamma distributions are $1/2$ and $2\sigma^2$ where σ^2 is equal to σ_R^2 or σ_W^2 as given in Theorem 1 . Key candidates κ with $\hat{c}(D, K, \kappa)^2 > \Theta^2$ are the likeliest candidates for the right key. An example of this case is depicted on the right side of Figure 2.

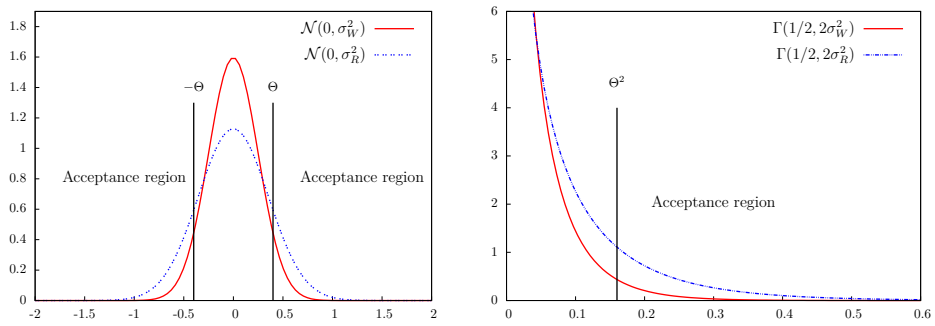

Figure 2: Left: distribution of $\hat{c}_R$ and $\hat{c}_W$. Right: distribution of $\hat{c}_R^2$ and $\hat{c}_W^2$. These are theoretical curves obtained from $\sigma_W^2 = 2^{-4}$ and $\sigma_R^2 = 2^{-3}$.

Using the hypothesis testing approach we obtain the following estimates of the data complexity of a linear attack. The proof provided in Appendix A.1 is based on distinguishing the two normal distributions on the left of Figure 2.

Theorem 2. *Given the advantage a of the key-recovery attack and σ_R and σ_W as in Theorem 1, the success probability of the attack is given as*

$$P_S = 2 - 2\Phi\left(\frac{\sigma_W}{\sigma_R} \cdot \Phi^{-1}(1 - 2^{-a-1})\right), \tag{5}$$

where Φ and Φ^{-1} denote the cumulative distribution function and quantile of the central normal distribution. Equivalently, the data complexity N^{KP} or N^{DKP} of a linear attack using non-distinct or distinct known plaintexts can be estimated as follows:

$$\begin{aligned} N^{\mathrm{KP}} &= \frac{\Phi^{-1}(1-2^{-a-1})^2 - \Phi^{-1}(1-P_S/2)^2}{ELP\,\Phi^{-1}(1-P_S/2)^2 - 2^{-n}\Phi^{-1}(1-2^{-a-1})^2}, \\ N^{\mathrm{DKP}} &\approx \frac{\Phi^{-1}(1-2^{-a-1})^2 - \Phi^{-1}(1-P_S/2)^2}{(ELP - 2^{-n})\Phi^{-1}(1-P_S/2)^2}. \end{aligned}$$

In [CW16] a linear attack on 21 rounds of SIMON32/64 [BSS+13] has been implemented. To check the validity of our results we have performed similar experimental attacks than in [CW16]. The description of the experiments are provided in Appendix B.1 and confirmed (see Table 5) that taking into consideration the key-variance for the right and the wrong keys allows us to provide a relatively good estimate of the success probability of the attack. In the same appendix we recall previous estimates of the success probability of a classical linear attack.

In Appendix B.2, we also discuss the difference between the distinct plaintext and non-distinct plaintext models, which becomes significant when the sample size is close to the full codebook. With the DKP sampling the success probabilities are higher and achieve the maximum with full codebook. If the KP model is used, then one must go beyond the full codebook to achieve success probabilities comparable to the one achieved using the DKP model and the full codebook of data.

2.4 Estimating ELP and Experiments

The experiments on SIMON32/64 presented in Appendix B.1 were based on an ELP value computed experimentally from the cipher, which is infeasible for ciphers with larger block size. The aim of this section is to present a method for estimating ELP in the offline analysis for an arbitrary key-alternating block cipher. Our theoretical model is

restricted to linear approximations of long-key block ciphers. The model will be tested in experiments also on other types of key-schedules.

Given a correlation of a linear approximation of a key-alternating block cipher as in Equation 3 we denote the correlation of the characteristic τ by ρ_τ. Then

$$c(u,v)(K) = \sum_{\substack{\tau \\ \tau_0=u,\, \tau_r=v}} (-1)^{\tau \cdot K} \rho_\tau. \tag{6}$$

If moreover the cipher is a long-key cipher, the linear hull theorem [Nyb94, DR06] holds, which means that the ELP of the linear approximation can be expressed as follows

$$ELP = \mathrm{Exp}_K\left(c(u,v)(K)^2\right) = \sum_{\substack{\tau \\ \tau_0=u,\, \tau_r=v}} \rho_\tau^2. \tag{7}$$

Now let us assume that the cryptanalyst has found a linear approximation (u,v) such that, in its correlation given as Equation 6, the quantities ρ_τ can be identified and quantified for a significant number of characteristics τ. Let us denote by $\mathcal{S}$ the set of identified characteristics for the linear approximation (u,v). Further, we denote the corresponding part of the total correlation as

$$Q(u,v)(K) = \sum_{\tau \in \mathcal{S}} (-1)^{\tau \cdot K} \rho_\tau, \tag{8}$$

and by $R(K)$ the correlation contribution of the remaining characteristics, that is,

$$R(K) = c(u,v)(K) - Q(u,v)(K). \tag{9}$$

We assume that the offline enumeration of the dominating linear characteristics is exhaustive so that the remainder $R(K)$ behaves like random noise, similarly as in the case of a single dominant characteristic [BT13, BN16]. By [DR07], a correlation of a random linear approximation is normally distributed with expectation zero and variance equal to 2^{-n}. Throughout this paper we model $R(K)$ as the correlation of a random linear approximation.

On the other hand, it can be shown that the variance of $R(K)$ for a long-key cipher is equal to $\sum_{\tau \notin \mathcal{S}} \rho_\tau^2$. Then we get the following theorem.

Theorem 3. *Suppose that a linear approximation over a long-key cipher admits a set $\mathcal{S}$ of dominating characteristics, and suppose that $R(K) = \sum_{\tau \notin \mathcal{S}} (-1)^{\tau \cdot K} \rho_\tau \sim \mathcal{N}(0, 2^{-n})$. Then*

$$\mathrm{Var}_K(\, c(u,v)(K)) = ELP = \sum_{\tau \in \mathcal{S}} \rho_\tau^2 + 2^{-n}.$$

The Sbox used in the block cipher PRESENT [BKL+07] has the particularity of having strong linear approximations with mask of weight one. They can be traced easily over multiple rounds of the cipher. In particular, for this cipher we can use a matrix method to estimate the correlation of linear approximations with input and output masks of weight one. For experimental purposes, we use a scaled version [Lea10] of this cipher called SMALLPRESENT-[4]. One round of this 16-bit cipher is represented in Figure 6 in Appendix C. In Table 6, Appendix C, we recall the strong correlations which are used to estimate the correlation of a linear approximation over multiple rounds of the cipher. The principle of the matrix method to estimate the ELP of a linear approximation is also provided in Appendix C.

In [AÅBL12] it has been experimentally illustrated that the variance of a linear approximation varies depending on the dependency between the round keys. For the purposes of experiments we define three key-schedulings. When the round keys are

independent, the length of the master key of a r-round version of the cipher is $2^{16(r+1)}$ bits. We refer to this key-schedule by *LONGKEY*. Secondly, from a 20-bit master-key we derive 16-bit round keys using a key-schedule called *SCHEDULING* given by the algorithm described in Appendix E. Finally, from a 16-bit master key the key-schedule called *SAME* consists of identical round keys. In the experiments the expected values and variances are computed using a sample of 2^{20} random long keys, and all 2^{20} and all 2^{16} master keys of the key-schedules *SCHEDULING* and *SAME*, respectively.

The results of our experiments are given in Table 1. As explained earlier the set $\mathcal{S}$ taken for experimental purpose consists of the 1-bit linear characteristics of PRESENT. We can see that the noiseless estimate $\sum_{\tau\in S}\rho_\tau^2$ of the ELPs of the linear approximations used in [Cho10] is far from accurate. When taking the noise into consideration the estimate of the variance is significantly improved particularly for the *LONGKEY* scheduling when the round keys are independent.

Table 1: Variance of the correlation of the linear trail with $u = v =$ 0x0020

r	$\sum_{\tau\in\mathcal{S}}\rho_\tau^2$	$\sum_{\tau\in\mathcal{S}}\rho_\tau^2 + 2^{-n}$	$\mathrm{Var}_K(c(u,v)(K))$ *LONGKEY*	$\mathrm{Var}_K(c(u,v)(K))$ *SCHEDULING*	$\mathrm{Var}_K(c(u,v)(K))$ *SAME*
3	$2^{-10.42}$	$2^{-10.39}$	$2^{-10.30}$	$2^{-9.98}$	$2^{-10.83}$
4	$2^{-12.83}$	$2^{-12.68}$	$2^{-12.35}$	$2^{-12.15}$	$2^{-11.90}$
5	$2^{-15.42}$	$2^{-14.68}$	$2^{-14.16}$	$2^{-14.11}$	$2^{-14.01}$
6	2^{-18}	$2^{-15.68}$	$2^{-15.36}$	$2^{-15.36}$	$2^{-15.04}$

3 Multiple and Multidimensional Linear Attacks

3.1 Preliminaries

The goal of this section is to extend the statistical model of key-recovery attack to generalizations of linear attacks of iterated block ciphers. As depicted in Figure 2 the Gamma distributions related to the squared correlation have different means in the right and wrong key case for certain linear approximations. The idea of using multiple linear approximations simultaneously is to amplify this effect by combining such Gamma distributed variables. When applying these attacks in practice, sufficiently accurate estimates of the parameters of the involved distributions is needed. The accuracy of the parameter estimates depends on the amount and quality of information obtained from the cipher.

To collect information of the correlations of all the linear approximations over E'_K used in the attack the notion of capacity was introduced in [BCQ04] and generalized in [HCN09]. Given a set of linear approximations with input and output mask pairs (u_j, v_j), $j = 1, \ldots, \ell$, where $(u_j, v_j) \neq 0$, their capacity is defined as the sum of the squared correlations:

$$C(K) = \sum_{j=1}^{\ell} c(u_j, v_j)(K)^2.$$

The expected value of the capacity is denoted by C. Then

$$C = \mathrm{Exp}_K(C(K)) = \sum_{j=1}^{\ell} \mathrm{Exp}_K(c(u_j, v_j)(K)^2),$$

that is, the sum of the ELP values of the involved linear approximations. Estimating the capacity is essential for providing estimates of the strength of the attack. Given estimates of the ELP values we obtain by summing them up an estimate of the capacity. There exist also algorithms that compute the capacity estimate directly.

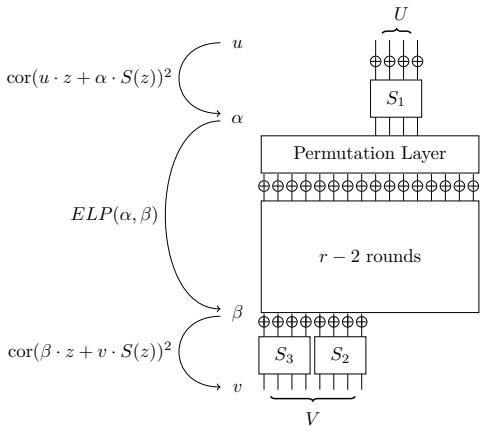

Figure 3: Estimating the capacity of a multidimensional linear approximation.

3.2 A Setting of Estimating Capacity for Iterated Ciphers

It is quite common in multidimensional linear cryptanalysis that the linear approximations used in the attack are different from those in the offline analysis when estimating the capacity. In Figure 3 we present an example where the linear approximations $(u, v) \in U \times V$ over r rounds of the cipher are used in the online attack while the estimation of the capacity C can be done using the linear approximations (α, β) that span over $r-2$ rounds only. The idea is to exploit the fact that a probability distribution is preserved under a bijective mapping. In the example situation depicted in Figure 3, the probability distribution of three 4-bit data values (z_1, z_2, z_3) observed outside the Sboxes is identical to the probability distribution of the data values $(S_1(z_1), S_2^{-1}(z_2), S_3^{-1}(z_3))$ looked from the inside of the cipher before the Sboxes.

Let us assume that the cipher is an SPN cipher and denote by S the Sbox layer. Then the round function g of the iterated block cipher is affinely equivalent to S. It suffices to show that the expected capacity value of the multidimensional linear approximation over r rounds determined by $(u, v) \in U \times V$ is equal to the capacity determined by linear approximations $(\alpha, \beta) \in S(U) \times S^{-1}(V)$ over $r-2$ rounds.

In addition to reducing the number of nonlinear rounds, this approach is advantageous if the linear approximations (α, β) are easier to analyze. For example, it may be the case that only a subset of them have large ELP and their independence can be justified. For example, the key bits that control the encryption function are different for different (α, β) in this subset.

We denote the expected linear potential of a linear approximation (a, b) by $ELP(a, b)$. By Equation 7 we then have

$$ELP(u,v) = \sum_{\tau} \rho_{\tau}^2 = \sum_{\tau_1, \tau_{r-1}} \mathrm{cor}(u \cdot z + \tau_1 \cdot g(z))^2 ELP(\tau_1, \tau_{r-1}) \mathrm{cor}(\tau_{r-1} \cdot z + v \cdot g(z))^2.$$

Since S is the only nonlinear function of the round function g, it follows that for each τ_1 there is a unique α, a linear mask after the first Sbox layer, and also for each τ_{r-1} there is a unique β, a linear mask before the last Sbox layer, such that

$$\begin{aligned} &\sum_{\tau_1, \tau_{r-1}} \mathrm{cor}(u \cdot z + \tau_1 \cdot g(z))^2 ELP(\tau_1, \tau_{r-1}) \mathrm{cor}(\tau_{r-1} \cdot z + v \cdot g(z))^2 \\ &= \sum_{\alpha, \beta} \mathrm{cor}(u \cdot z + \alpha \cdot S(z))^2 ELP(\alpha, \beta) \mathrm{cor}(\beta \cdot z + v \cdot S(z))^2. \end{aligned}$$

Due to the properties of the Sbox layer, it holds for all $u \in U$ and $v \in V$ that

$$\mathrm{cor}(u \cdot z + \alpha \cdot S(z)) = 0, \text{ if } \alpha \notin S(U), \text{ and } \mathrm{cor}(\beta \cdot z + v \cdot S(z)) = 0, \text{ if } \beta \notin S^{-1}(V).$$

Then we obtain

$$\begin{aligned} C &= \sum_{\substack{(u,v)\in U\times V\\(u,v)\neq 0}} ELP(u,v) = \sum_{(u,v)\in U\times V} ELP(u,v) - 1 \\ &= \sum_{(u,v)\in U\times V} \sum_{\alpha}\sum_{\beta} \mathrm{cor}(u\cdot z+\alpha\cdot S(z))^2 ELP(\alpha,\beta)\mathrm{cor}(\beta\cdot z+v\cdot S(z))^2 - 1 \\ &= \sum_{\alpha\in S(U)}\sum_{\beta\in S^{-1}(V)} ELP(\alpha,\beta) \sum_{u\in U}\mathrm{cor}(u\cdot z+\alpha\cdot S(z))^2 \sum_{v\in V}\mathrm{cor}(\beta\cdot z+v\cdot S(z))^2 - 1 \\ &= \sum_{\alpha\in S(U)}\sum_{\beta\in S^{-1}(V)} ELP(\alpha,\beta) - 1 = \sum_{\substack{(\alpha,\beta)\in S(U)\times S^{-1}(V)\\(\alpha,\beta)\neq 0}} ELP(\alpha,\beta), \end{aligned}$$

where the first equality on the last line follows from Parseval's theorem. Hence we have shown that the capacity determined by the linear approximations $(u, v) \in U \times V$ can be computed using the linear approximations $(\alpha, \beta) \in S(U) \times S^{-1}(V)$.

3.3 Estimating Expected Value of Capacity

Next we show how to derive a capacity value estimate by restricting to a subset of all linear approximations involved in the computation of the capacity and using sufficiently many enumerated strong characteristics for each linear approximation. Let us denote by ELP_j the expected linear potential of $c(u_j, v_j)(K)$. By Equation 7 we have

$$ELP_j = \mathrm{Exp}_K\left(c(u_j,v_j)(K)^2\right),$$

for $j = 1, \ldots, \ell$, and for the capacity,

$$C = \mathrm{Exp}_K(C(K)) = \sum_{j=1}^{\ell} \mathrm{Exp}_K(c(u_j,v_j)(K)^2) = \sum_{j=1}^{\ell} ELP_j$$

holds. Then we focus on a subset of M linear approximations, which we number from 1 to M. Under the assumption of a long-key cipher, one can select, for each dominant linear approximation (u_j, v_j), $j = 1, \ldots, M$, an enumerated part $Q(u_j, v_j)(K)$ as defined by Equation 8 and use them to compute a capacity estimate

$$C_* = \mathrm{Exp}_K\left(\sum_{j=1}^{M} Q(u_j,v_j)(K)^2\right) = \sum_{j=1}^{M}\sum_{\tau\in\mathcal{S}_j} \rho_\tau^2, \tag{10}$$

where we denote by $\mathcal{S}_j$ the set of significant characteristics for (u_j, v_j). For a practical example, how to compute such an estimate as a product of squared correlation matrices see Appendix C or [Cho10]. In this manner, one gets a lower bound of the average value of the capacity over the keys. For all involved linear approximations the effect of missing characteristics is modeled as the correlation of a linear approximation of a random cipher as presented in Subsection 2.4. Consequently, we get the following capacity estimate.

$$C = \sum_{j=1}^{\ell} ELP_j = \sum_{j=1}^{M}\left(\sum_{\tau\in\mathcal{S}_j}\rho_\tau^2 + 2^{-n}\right) + \sum_{j=M+1}^{\ell} 2^{-n} = C_* + \ell 2^{-n}. \tag{11}$$

3.4 Estimating Capacity Variance When ELP Estimates Are Known

Similarly as in the previous subsection we assume that a subset of linear approximations has been identified to have large (squared) correlations and express the capacity as

$$C(K) = \sum_{j=1}^{\ell} c(u_j, v_j)(K)^2 = \sum_{j=1}^{M} c(u_j, v_j)(K)^2 + \sum_{j=M+1}^{\ell} c(u_j, v_j)(K)^2.$$

In the second sum we collected squared correlations of linear approximations which are assumed to behave as random. Then it remains to assume that the correlations of M linear approximations with significant ELP are independent to have a set of ℓ independent and normally distributed random variables $c(u_j, v_j)(K)$ such that the means are equal to zero and

$$\mathrm{Var}_K(c(u_j, v_j)(K)) = \begin{cases} ELP_j, & \text{for } j = 1, 2, \ldots, M, \text{ and} \\ 2^{-n}, & \text{for } j = M+1, 2, \ldots, \ell, \end{cases}$$

by Lemma 1 assuming that the cipher is a long-key cipher. It follows that the squares of the correlations divided by the variance of the correlation are independent random variables and follow a χ^2 distribution with one degree of freedom. From the parameters of the χ^2 distribution we obtain that

$$\mathrm{Var}_K(c(u_j, v_j)(K)^2) = \begin{cases} 2ELP_j^2, & \text{for } j = 1, 2, \ldots, M, \text{ and} \\ 2^{1-2n}, & \text{for } j = M+1, 2, \ldots, \ell. \end{cases}$$

By independency, the variance of the capacity is now obtained as a sum of all these variances and we can state the following result.

Theorem 4. *For a long-key key-alternating cipher, given a set of ℓ linear approximations where M have ELP estimates, we assume that their correlations are independent random variables with normal distribution with variance as given by Theorem 3. Moreover, it is assumed that the remaining $\ell - M$ linear approximations behave like random linear approximations. Then the variance $\mathrm{Var}_K(C(K))$ is given by*

$$\mathrm{Var}_K(C(K)) = \sum_{j=1}^{M} 2\,ELP_j^2 + (\ell - M)2^{1-2n} = 2\sum_{j=1}^{M}\left(\sum_{\tau \in \mathcal{S}_j} \rho_\tau^2\right)^2 + C_* 2^{2-n} + \ell 2^{1-2n}, \quad (12)$$

where C^* is as defined by Equation 10.

Parallel to our work, Vejre has developed a method for computing the capacity variance in the case of dependent correlations by taking into consideration the covariances of the correlations [Vej16]. In the case where $M = \ell$, our estimate given in Equation 12 is a special case of Vejre's method, and is obtained from it by setting the covariances and the expected values of the correlations equal to zero as shown in Subsubsection 4.3.3.

3.5 Estimating Capacity Variance When Only Capacity Estimate Is Known

Given only an estimate of the capacity C, further assumptions are needed to obtain an estimate of the capacity variance. The simplest approach is to assume that all ELP_j, $j = 1, \ldots, M$, are equal, in which case we can state the following result.

Theorem 5. *In the context of Theorem 4, let us suppose that all the ELP estimates are equal for all $j = 1, \ldots, M$. Given the capacity value C the capacity variance is given by*

$$\mathrm{Var}_K(C(K)) = \frac{2}{M}C^2 - \frac{\ell - M}{M}C2^{2-n} + \frac{\ell - M}{M}\ell 2^{1-2n} = \frac{2}{M}C_*^2 + C_* 2^{2-n} + \ell 2^{1-2n}.$$

Proof. If all the ELP_j estimates are equal, then

$$ELP_j = \frac{1}{M}(C - (\ell - M)2^{-n}) \text{ and } \sum_{\tau \in \mathcal{S}_j} \rho_\tau^2 = \frac{1}{M}C^*, \text{ for all } j = 1, \ldots, M.$$

We get the claimed result by substituting these expressions to Equation 12. □

In this paper we show results of experiments where the capacity estimate is given and the variance estimate is obtained by Theorem 5.

3.6 Experiments

The different steps of our experiments on SMALLPRESENT-[4] are described below. We selected a multidimensional linear space of size $\ell = 2^8 - 1$, involving bits $8, 9, 10, 11$ at the input and bits $4, 5, 6, 7$ after r rounds as described in blue in Figure 7 given in Appendix D. For this multidimensional linear space, we can estimate the capacity of the multidimensional linear approximation using the matrix method over $r - 2$ rounds. In Subsection 3.2 we explained how to estimate the capacity for such multidimensional linear space. Note that the technique is similar to the one used in [Cho10] to estimate the capacity of the multidimensional linear space involved in the attack on 26 rounds of PRESENT. For this reduced cipher we have $M = 9$.

The value of $C_* = \sum_{j=1}^{M} \sum_{\tau \in \mathcal{S}_j} \rho_\tau^2$ is given in Table 2 as well as the estimate of the capacity using Equation 11. In the same table, we provide the expected value of the capacity for the three different key-schedules introduced in Subsection 2.4.

Table 2: The expected value of the capacity

r	C_*	C	$\mathrm{Exp}_K(C(K))$ *LONGKEY*	$\mathrm{Exp}_K(C(K))$ *SCHEDULING*	$\mathrm{Exp}_K(C(K))$ *SAME*	$\mathrm{Exp}_K(C(K)) - C_*$ *LONGKEY*
5	$2^{-7.41}$	$2^{-6.68}$	$2^{-6.600}$	$2^{-6.596}$	$2^{-6.598}$	$2^{-7.82}$
6	$2^{-10.02}$	$2^{-7.68}$	$2^{-7.42}$	$2^{-7.404}$	$2^{-7.401}$	$2^{-7.68}$
7	$2^{-12.61}$	$2^{-7.94}$	$2^{-7.95}$	$2^{-7.940}$	$2^{-7.950}$	$2^{-8.01}$

In the last column of Table 2 we compare the difference between the expected value of the capacity and C_* computed in the offline analysis, and demonstrate that the noise is close to $\ell 2^{-n} = 2^{-8}$ in the setting of the presented experiments. The noise-based modeling of estimated capacity has also been experimentally verified in [Vej16], Fig. 5.1, see also [BTV16], Fig. 3.

Next, we compare in Table 3 the estimates $\frac{2}{\ell}C_*^2$ and $\frac{2}{\ell}C^2$, which correspond to the estimates derived in [BN16], and the estimate provided in Theorem 5 with the experimental variances for the different key-schedules defined in Subsection 2.4.

Table 3: Comparison of between different theoretical and experimental capacity variances

r	$\frac{2}{\ell}C_*^2$	$\frac{2}{\ell}C^2$	$\frac{2}{M}C_*^2 + 2^{2-n}C_* + 2^{1-2n}\ell$ Theorem 5	$\mathrm{Var}_K(C(K))$ *LONGKEY*	$\mathrm{Var}_K(C(K))$ *SCHEDULING*	$\mathrm{Var}_K(C(K))$ *SAME*
5	$2^{-21.82}$	$2^{-20.36}$	$2^{-16.91}$	$2^{-17.39}$	$2^{-17.83}$	$2^{-16.96}$
6	$2^{-27.04}$	$2^{-22.37}$	$2^{-21.31}$	$2^{-20.94}$	$2^{-20.71}$	$2^{-20.85}$
7	$2^{-32.21}$	$2^{-22.89}$	$2^{-22.82}$	$2^{-22.51}$	$2^{-22.40}$	$2^{-22.34}$

These experimental results illustrate that for a long-key key-alternating cipher the variance estimate provided in Theorem 5 is much closer to the experimental one. The implication of this result to the success of the attack is provided in the next section.

Note that while we observe a difference in the capacity variance depending of the used key-schedule, this difference becomes marginal as the number of rounds increases and the theory developed in this paper for a long-key cipher is also applicable on ciphers with different key-schedules.

In previous publications [Cho10, Lea11], the experiments were performed on a reduced number of rounds of the 64-bit PRESENT. The influence of the noise was then not detected since C_* was too large in comparison to the noise $\ell 2^{-n}$. Experiments on a scaled (here 16-bit) version of the cipher may be helpful for detecting the influence of the weak linear characteristics and approximations.

4 Impact on Multidimensional Linear Attacks

4.1 Statistic for Right Key

In practice when an attack is performed only part of the data is considered. In the multiple/multidimensional linear context the statistic $T(D, K, \kappa)$ is computed during the online part of the attack

$$T = T(D, K, \kappa) = N \sum_{j=1}^{\ell} \hat{c}_j(D, K, \kappa)^2, \tag{13}$$

where $\hat{c}_j(D, K, \kappa)$ is the empirical correlation of the j-th linear approximation as defined by Equation 1 in the classical linear context.

In multidimensional linear key-recovery attacks, the online test statistic is computed over all non-zero linear approximations in space $U \times V$, in which case, instead of the individual empirical correlations, cryptanalyst may compute the test statistic over the observed data $(\widetilde{G_\kappa}(x), \widetilde{H_\kappa^{-1}}(y))$ with $\widetilde{G_\kappa}(x) \in U$ and $\widetilde{H_\kappa^{-1}}(y) \in V$, also as follows

$$T = T(D, K, \kappa) = \sum_{\eta=0}^{\ell} \frac{(V[\eta] - N2^{-s})^2}{N2^{-s}}, \tag{14}$$

where $V[\eta]$ corresponds to the number of times the value $\eta \in U \times V$ occurs for the observed data $(\widetilde{G_\kappa}(x), \widetilde{H_\kappa^{-1}}(y))$ in the sample D. In the offline analysis, only a subset of all linear approximations are taken into consideration when the capacity estimate is computed over the linear space $U \times V$ or an equivalent space as explained in Subsection 3.2.

To perform an attack, the statistical model for both the wrong and right keys have to be considered. Let us make the following notations

$$\begin{aligned} T_R(D, K) &= T(D, K, \kappa), \text{ for } \kappa = K_0, \\ T_W(D, K, \kappa) &= T(D, K, \kappa), \text{ for } \kappa \neq K_0. \end{aligned}$$

Theorem 6. *The statistic $T_R(D, K)$ computed either as in Equation 14 (only in multidimensional linear attack) or as in Equation 13 has the following mean and variance*

$$\begin{aligned} \mu_R &= \mathrm{Exp}_{D,K}\left(T_R(D, K)\right) = B\ell + N \cdot \mathrm{Exp}_K(C(K)) \text{ and} \\ \sigma_R^2 &= \mathrm{Var}_{D,K}\left(T_R(D, K)\right) = 2B^2\ell + 4BN \cdot \mathrm{Exp}_K(C(K)) + N^2 \cdot \mathrm{Var}_K(C(K)), \end{aligned} \tag{15}$$

where B is as defined in Equation 4 for a KP or DKP attack.

Proof. From [HCN09] for the KP model and from [BN15b] for the DKP we have that for a fixed key a constant multiple of $T_R(D, K)$ follows a non-central χ^2 distribution. The parameters are the following

$$\mathrm{Exp}_D\left(T_R(D, K)\right) = B\ell + NC(K) \text{ and } \mathrm{Var}_D\left(T_R(D, K)\right) = 2B^2\ell + 4BNC(K).$$

From the following formulas

$$\begin{aligned}\mathrm{Exp}_{D,K}\left(T_R(D,K)\right) &= \mathrm{Exp}_K\left(\mathrm{Exp}_D(T_R(D,K))\right),\\ \mathrm{Var}_{D,K}\left(T_R(D,K)\right) &= \mathrm{Exp}_K\left(\mathrm{Var}_D(T_R(D,K))\right)+\mathrm{Var}_K\left(\mathrm{Exp}_D(T_R(D,K))\right),\end{aligned}$$

we derive the result. □

Using the results from Subsection 2.2 and the estimate given in Theorem 5, we obtain the following estimates of the expected value and variance of the statistic $T_R(D,K)$.

Corollary 1. *Given B defined by Equation 4 let us suppose that $C = \mathrm{Exp}_K(C(K))$ is equal to $C_* + \ell 2^{-n} = \sum_{j=1}^{M}\sum_{\tau\in\mathcal{S}_j}\rho_\tau^2 + \ell 2^{-n}$ as given in Equation 11. Assuming the estimate of the capacity variance given in Theorem 5, we have*

$$\begin{aligned}\mathrm{Exp}_{D,K}(T_R(D,K)) &= B\ell + NC, \text{ and}\\ \mathrm{Var}_{D,K}(T_R(D,K)) &= 2B^2\ell + 4BNC + N^2\left(\frac{2}{M}C_*^2 + 2^{2-n}C_* + \ell\cdot 2^{1-2n}\right).\end{aligned}$$

Or equivalently in the KP setting ($B = 1$)

$$\mathrm{Var}_{D,K}(T_R(D,K)) = 2\ell\left(1+\frac{N^2}{2^{2n}}+\frac{2N}{2^n}\right)+4NC_*\left(1+\frac{NC_*}{2M}+\frac{N}{2^n}\right),$$

and in the DKP setting

$$\mathrm{Var}_{D,K}(T_R(D,K)) \approx 2\ell + 4NC_*\left(1+\frac{NC_*}{2M}\right).$$

4.2 Statistic for Wrong Key

Let us denote by C_W the expected capacity in the wrong key case. Then

$$C_W = \sum_j \mathrm{Exp}_{D,(K,\kappa)}\left(\hat{c}_j(D,K,\kappa)^2\right),\ \kappa\neq K_0.$$

In [HCN09, Cho10] the value $C_W = 0$ was used. Now that we take the noise introduced by the key variable into account, we take this estimate to be equal to $C_W = 2^{-n}\ell$ as in [BN16]. Then the behavior of the test statistic for the wrong key can be stated as follows.

Theorem 7. *[BN16] Assuming that $\ell > 50$ and a normal approximation of the χ^2 distribution, the statistic $T_W(D,K,\kappa)$ for $\kappa\neq K_0$ follows a normal distribution with mean μ_W and variance σ_W^2 defined as follows*

$$\mu_W = B\ell + N2^{-n}\ell \text{ and } \sigma_W^2 = \frac{2}{\ell}\left(B\ell + N2^{-n}\ell\right)^2,$$

where B is given as in Equation 4.

4.3 Previous Models for Right Key

4.3.1 The model of [HCN09, Cho10]

In [Cho10] a multidimensional linear attack on 26 rounds of the block cipher PRESENT is presented. The success probability estimate was based on the statistical model developed in [HCN09]. In this model it was assumed that the statistic T_W for the wrong keys follows a normal distribution with mean ℓ and variance 2ℓ. For the purpose of clarity, we denote these previous estimates by $\tilde{\mu}_W = \ell$ and $\tilde{\sigma}_W^2 = 2\ell$. Recently, in [BN15a], new estimates of μ_W and σ_W have been provided. These estimates are recalled in Theorem 7 and are based

on the estimate $C_W = \ell 2^{-n}$. For the right key, in [HCN09], the mean $\tilde{\mu}_R$ and the variance of $\tilde{\sigma}_R^2$ were estimated to

$$\tilde{\mu}_R = \ell + NC_*, \text{ and } \tilde{\sigma}_R^2 = 2(\ell + 2NC_*).$$

In [Cho10] the capacity was computed using the matrix method as described in Subsection 2.4 and Subsection 3.6. In particular C was estimated to be close to $C_* = \sum_{j=1}^{M} \sum_{\tau \in \mathcal{S}_j} \rho_\tau^2$ meaning that the mean and the variance of T_R were estimated to

$$\tilde{\mu}_R = \ell + NC_*, \text{ and } \tilde{\sigma}_R^2 = 2(\ell + 2NC_*).$$

In this paper we showed the difference between C_* and C which is particularly important when C is close to $2^{-n}\ell$ (see example in Table 2) and provide a new estimate of the expected value μ_R of T_R. The difference between the means in the right-key and wrong-key case is always positive and the same as estimated in [Cho10], meaning that $\tilde{\mu}_R - \tilde{\mu}_W = \mu_R - \mu_W = NC_*$. The success probability (see Equation 17) of the attack is then not influenced by these new mean estimates obtained for the wrong keys in [BN15a] and for the right keys in Subsection 4.1. Using the result of [BN16] for a fixed success probability using the new variance estimate we obtain a better estimate of the data complexity of the attack.

4.3.2 The model of [BN15a, BN16]

Assuming, as it is possible for SIMON32/64 a good estimate of the ELP of each linear approximation, in [BN16] the following result is derived

Theorem 8. *[BN16] Assuming that all linear approximations have equal ELP and given* $C = \sum_{j=1}^{\ell} \mathrm{Exp}_K(c(u_j, v_j)(K)^2)$ *and* $C_0 = \sum_{j=1}^{\ell} \mathrm{Exp}_K(c(u_j, v_j)(K))^2$, *we have*

$$\mathrm{Exp}_{D,K}(T_R(D,K)) = B\ell + NC, \text{ and } \mathrm{Var}_{D,K}(T_R(D,K)) = \frac{2}{\ell}((B\ell + NC)^2 - (NC_0)^2)$$

The form of the distribution of T_R *can be determined in two cases:*

1. $\ell > 50$, *in which case normal approximation can be used, or*
2. $C_0 = 0$, *in which case* T_R *follows a Gamma distribution with variance*

$$\frac{2}{\ell}((B\ell + NC)^2) = 2B^2\ell + 4BNC + N^2\left(\frac{2}{\ell}C_*^2 + 2^{2-n}C_* + \ell \cdot 2^{1-n}\right) \tag{16}$$

The variance estimates provided in Corollary 1 and in Equation 16 are similar. The difference is only in the multiplier of C_*^2. The previous estimate from Equation 16 has multiplier $\frac{2N^2}{\ell}$ and it was experimentally observed in [BN15a] to give an underestimate for the variance of $T_R(D,K)$. In the formula given in Corollary 1 this multiplier is equal to $\frac{2N^2}{M}$ where $M \leq \ell$ corresponds to the number of dominant linear approximations. The experimental comparison between these estimates is given in Subsection 5.1.

4.3.3 The model of [Vej16, BTV16]

In this section we recall the result of [Vej16, BTV16], in the particular case where we assume that covariances of the linear approximations are equal to 0.

Theorem 9. *Corollary 2 of [Vej16]. Given* ℓ *linear approximations* (u_j, v_j), *let us denote by* $C_*^{(\ell)} = \sum_{j=1}^{\ell} \sum_{\tau \in \mathcal{S}_j} \rho_\tau^2$ *and* $C = C_*^{(\ell)} + \ell 2^{-n}$. *Assuming that the correlations of these*

linear approximations are statistically independent, we have

$$\begin{aligned}\mathrm{Exp}_{D,K}(T_R(D,K)) &= B\ell + N(C_*^{(\ell)} + \ell 2^{-n}) = B\ell + NC\\ \mathrm{Var}_{D,K}(T_R(D,K)) &= 2B^2\ell + 4BNC + 2N^2(2^{-n+1}C_*^{(\ell)} + \ell\cdot 2^{-2n})\\ &+ 2N^2\sum_{j=1}^{\ell}\left[\left(\mathrm{Exp}_K(Q(u_j,v_j)(K)^2)\right)^2 - \left(\mathrm{Exp}_K(Q(u_j,v_j)(K))\right)^4\right].\end{aligned}$$

In the special case, when $\mathrm{Exp}_K(Q(u_j,v_j)(K)) = 0$ *as in Section 2, we obtain*

$$\mathrm{Var}_{D,K}(T_R(D,K)) = 2B^2\ell + 4BNC + N^2\Big(2\sum_{j=1}^{\ell}\left(\sum_{\tau\in\mathcal{S}_j}\rho_\tau^2\right)^2 + 2^{2-n}C_*^{(\ell)} + \ell 2^{1-2n}\Big).$$

The last expression is equal to the one we obtain by combining Equation 12 and Equation 15 and by setting $M = \ell$.

5 Experiments

5.1 Experiments on SMALLPRESENT-[4]

In Figure 4 and Figure 5 the distribution of $T_R(D,K)$ is experimentally computed, for the long key version of SMALLPRESENT-[4]. The experiments are performed over 5 rounds of the cipher with the multidimensional linear space as in Subsection 3.6. We use the normal distribution to estimate the distribution of $T_R(D,K)$. The theoretical expected value and variance are taken from Corollary 1. In these graphics we observe that the new variance estimate is more accurate than the one given in [BN16]. The theoretical results have been computed with the estimate of the expected capacity $C = C_* + \ell 2^{-n}$. In Figure 5, the experiments are performed using known plaintexts and a comparison with the model of [HCN09] is also provided. Similar experiments over 6 and 7 rounds are presented in Appendix F.

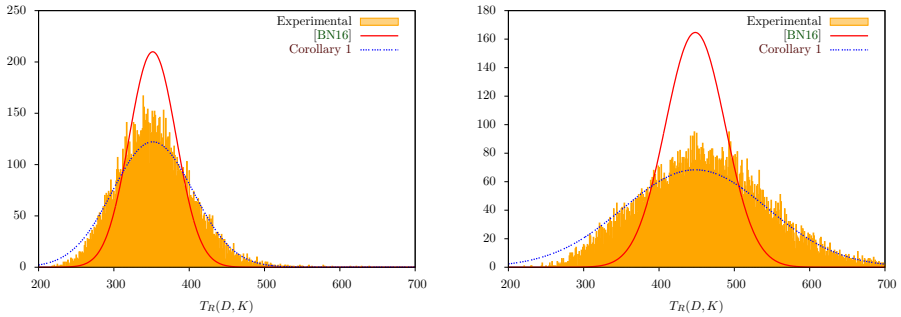

Figure 4: Comparison between the experimental distribution of $T(D,K)$ and normal distributions with mean $B\ell + NC$ and different variances recalled in this paper. Left with $N = 2^{14}$. Right with $N = 2^{15}$. Experiments in the DKP setting.

The distribution of $T_R(D,K)$. At the contrary of [BN16], the study of the statistic $T_R(D,K)$ presented in this paper does not directly give us the distribution of $T_R(D,K)$. As recalled in Theorem 8, in [BN16], it is shown that the distribution of $T_R(D,K)$ can be approached by a normal distribution if the number of linear approximations is large.

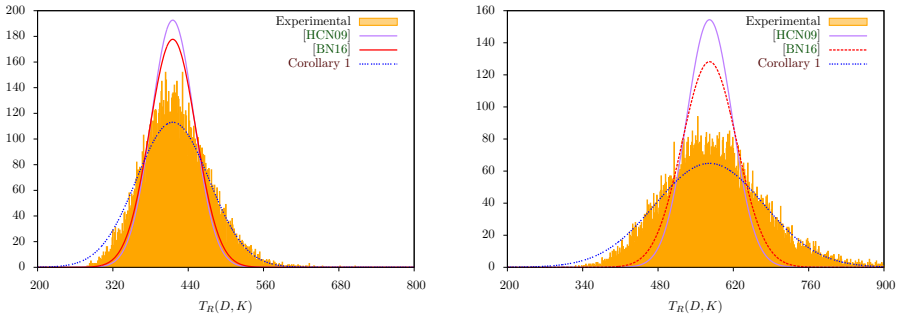

Figure 5: Comparison between the experimental distribution of $T(D,K)$ and normal distributions with mean $B\ell + NC$ and different variances recalled in this paper. Left with $N = 2^{14}$. Right with $N = 2^{15}$. Experiments in the KP setting.

The use of the normal distribution to approximate the distribution of $T_R(D,K)$ is also confirmed by our experiments. Therefore, to analyze the success of the attack using classical tools, we make the following assumption.

Assumption 1. *For $\ell > 50$, the statistic $T_R(D,K)$ as defined in Subsection 4.1 follows a normal distribution with mean μ_R and variance σ_R^2 as given in Corollary 1.*

An estimate of success probability. In practice, we know that it is hard to get a correct estimate of the mean and standard deviates of the variables in a statistical attack. In Figure 4 and Figure 5, it is illustrated that the theoretical and experimental variances slightly differ from the experimental ones. In our experiments on 5 rounds of SMALLPRESENT-[4] the variance estimate of $T_R(D,K)$ is larger than the one obtained in practice. When the distributions are normal and $\mu_R > \mu_W$, we use the following estimate of the success probability

$$P_S = 1 - \alpha = \Phi\left(\frac{\mu_R - \mu_W - \sigma_W \Phi^{-1}(1-2^{-a})}{\sigma_R}\right), \tag{17}$$

where a is called the advantage of the attack and corresponds to the number of gained bits during the attack. For details, see Appendix A.2.

From Equation 17 we can conclude that if the estimate of the mean is smaller than one obtained in practice and if the variance estimate of $T_R(D,K)$ is larger than the one obtained in practice and the experimental and theoretical means and variances for the wrong keys are equal, then we obtain an underestimate of the success probability or equivalently an overestimate of the data complexity. The experimental results illustrate that this was not the case with the previous estimates derived in [HCN09, HVLN15, BN16].

5.2 The Multidimensional Linear Attack on PRESENT

From Theorem 7 and Corollary 1 and under Assumption 1, we can estimate the success probability of a multiple/multidimensional linear attack using Equation 17. In particular in this section we apply our result to the multidimensional linear attack on PRESENT [Cho10].

In [Cho10] the attack takes advantage of 9 multidimensional linear space involving in total $\ell = 9 \cdot (2^8 - 1)$ linear approximations. For this $n = 64$-bit block cipher we then obtain $C_W = 2^{-52.83}$ (see Subsection 4.2).

In Table 4 we compare the previous estimate of the success probability using the setting of [Cho10] with the one of this paper. The success probability estimate obtained in [Cho10] does not take into consideration the variance of the capacity for the right and wrong keys.

The new success probability estimate has been computed for an advantage of 8-bits. While in [Cho10] the attack is performed in the KP model, we illustrate that we can

Table 4: Multidimensional linear attacks on PRESENT. Computation of the success probability for an advantage a of 8 bits.

attacked rounds	C_* (over $r-2$ rounds)	C	N	Success Probability [Cho10]	Success Probability This paper DKP	Success Probability This paper KP
24	$2^{-50.16}$ (22 rounds)	$2^{-49.95}$	$2^{58.5}$	97%	87%	86%
25	$2^{-52.77}$ (23 rounds)	$2^{-51.80}$	2^{61}	94%	84%	74%
26	$2^{-55.38}$ (24 rounds)	$2^{-52.60}$	$2^{63.8}$	98%	90%	51%

also assume distinct plaintexts. It is important to notice that the attack on 26 rounds of PRESENT as presented in [Cho10] is not threatened by the more accurate statistical model derived in this paper. For instance with a data complexity of $2^{63.5}$ distinct plaintexts and an advantage of 8-bit, the attack will succeed in 81% of the cases. In [BTV16] a multiple linear attack on 27 rounds of PRESENT is presented, the attack used a multiple linear distinguisher over 23 rounds derived from 189 linear approximations.

6 Conclusion

In this paper, we derive a method for estimating the variance of the correlation of a linear approximation that comprises a number of strong characteristics. Our method does not require any heavier computation that is needed to compute an estimate of the ELP for the linear approximation. We also showed how to use this estimate to derive the success probability of the online linear attack. This method is then extended to multiple and multidimensional linear cryptanalysis to provide an improved estimate of the expected value and the variance of the capacity. The results of this paper are compared with previous results in the simple, multiple and multidimensional linear contexts and are heavily backed up by experiments. Finally from the new developed theory we provide a new estimate of the success of a multiple and multidimensional linear attack. Simultaneously to our work, Vejre et al developed an extension to [BN15a] using which the variance of the capacity can be estimated also in the case when the linear approximations involved in the offline analysis have statistically dependent correlations.

When using multiple linear approximations, the question about their independence is often an issue. In the course of this work, one of the main lessons learnt has been that the correlations of linear approximations occur in two completely different types of random variables:

1. the empirical correlations computed for a fixed key are random variables as function of the random data sample, and
2. the correlations of linear approximations are random variables as function of the random key.

It follows that in this model, which integrates both the data and the key as random variables, we have two unrelated concepts of independence of linear approximations. Moreover, the two types of random variables are also separated by their different usage: the type (1) random variables are used in online analysis while the type (2) variables occur only in offline analysis when estimating parameters of the distributions of type (1) variables. In particular, it means that assuming independence of type (2) variables does not imply independence, or any other restriction, for type (1) variables. The main advantage of the multidimensional linear cryptanalysis method that it does not need any assumption about the statistical independence of the empirical correlations of the linear approximations. This advantage is not lost if the independence of the correlations over the key is assumed in the offline analysis for the purposes of parameter estimation as done in this paper.

Acknowledgements

We wish to thank the anonymous reviewers for useful comments that helped us to improve this paper. We wish to acknowledge the assistance of Elmar Tischhauser in formulations concerning relations to previous work. We also acknowledge the Dagstuhl seminar on Symmetric Cryptography for facilitating exchange of ideas between researchers.

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.

[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.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *CHES*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, 2007.

[BLNW12] Andrey Bogdanov, Gregor Leander, Kaisa Nyberg, and Meiqin Wang. Integral and Multidimensional Linear Distinguishers with Correlation Zero. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT*, volume 7658 of *Lecture Notes in Computer Science*, pages 244–261. Springer, 2012.

[BN15a] Céline Blondeau and Kaisa Nyberg. Joint Data and Key Distribution of Simple, Multiple, and Multidimensional Linear Cryptanalysis Test Statistic and Its Impact to Data Complexity. *IACR Cryptology ePrint Archive*, 2015:935, 2015. First online in September 2015, revised in May 2016. http://eprint.iacr.org/2015/935.pdf.

[BN15b] Céline Blondeau and Kaisa Nyberg. On Distinct Known Plaintext Attacks. In Jean-Pierre Tillich Pascale Charpin, Nicolas Sendrier, editor, *WCC2015 - 9th International Workshop on Coding and Cryptography 2015*, Proceedings of the 9th International Workshop on Coding and Cryptography 2015 WCC2015, Paris, France, April 2015.

[BN16] Céline Blondeau and Kaisa Nyberg. Joint Data and Key Distribution of Simple, Multiple, and Multidimensional Linear Cryptanalysis Test Statistic and Its Impact to Data Complexity. *Design Codes and Cryptography*, pages 1–31, 2016. Online First 17 August 2016.

[Bog16] Andrey Bogdanov. Private communication. Dagstuhl seminar 16021“Symmetric Cryptography”, 2016.

[BSS+13] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK Families of Lightweight

Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/404.

[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.

[BTV16] Andrey Bogdanov, Elmar Tischhauser, and Philip S. Vejre. Multivariate Linear Cryptanalysis: The Past and Future of PRESENT. *IACR Cryptology ePrint Archive*, 2016:667, June 2016.

[BW12] Andrey Bogdanov and Meiqin Wang. Zero Correlation Linear Cryptanalysis with Reduced Data Complexity. In Anne Canteaut, editor, *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, volume 7549 of *Lecture Notes in Computer Science*, pages 29–48. Springer, 2012.

[Cho10] Joo Yeon Cho. Linear Cryptanalysis of Reduced-Round PRESENT. In Josef Pieprzyk, editor, *Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings*, volume 5985 of *Lecture Notes in Computer Science*, pages 302–317. Springer, 2010.

[CW16] Huaifeng Chen and Xiaoyun Wang. Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-Guessing Techniques. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 428–449. Springer, 2016.

[DR06] Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *IACR Cryptology ePrint Archive*, 2005:212, 2006.

[DR07] Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *J. Mathematical Cryptology*, 1(3):221–242, 2007.

[HCN09] Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Multidimensional Extension of Matsui's Algorithm 2. In Orr Dunkelman, editor, *Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers*, volume 5665 of *Lecture Notes in Computer Science*, pages 209–227. Springer, 2009.

[HVLN15] Jialin Huang, Serge Vaudenay, Xuejia Lai, and Kaisa Nyberg. Capacity and data complexity in multidimensional linear attack. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 141–160. Springer, 2015.

[Jun04] Pascal Junod. Statistical Cryptanalysis of Block Ciphers, 2004. PhD thesis.

[Lea10] Gregor Leander. Small scale variants of the block cipher PRESENT. *IACR Cryptology ePrint Archive*, 2010:143, 2010.

[Lea11] Gregor Leander. On Linear Hulls, Statistical Saturation Attacks, PRESENT and a Cryptanalysis of PUFFIN. In K. G. Paterson, editor, *EUROCRYPT*, volume 6632 of *Lecture Notes in Computer Science*, pages 303–322. Springer, 2011.

[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.

[Mat94] Mitsuru Matsui. The First Experimental Cryptanalysis of the Data Encryption Standard. 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 1–11. Springer, 1994.

[Nyb94] Kaisa Nyberg. Linear Approximation of Block Ciphers. In 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*, pages 439–444. Springer, 1994.

[RN13] Andrea Röck and Kaisa Nyberg. Generalization of Matsui's Algorithm 1 to linear hull for key-alternating block ciphers. *Des. Codes Cryptography*, 66(1-3):175–193, 2013.

[Sel08] Ali Aydin Selçuk. On Probability of Success in Linear and Differential Cryptanalysis. *J. Cryptology*, 21(1):131–147, 2008.

[Vej16] Philip Vejre. The Past and Future of PRESENT: Establishing Multivariate Linear Cryptanalysis, January 2016. Master's thesis.

A Success Probability

A.1 Proof of Theorem 2

In this section we prove Theorem 2 given in Section 2 and restated below

Theorem 2. *Given the advantage a of the key-recovery attack and σ_R and σ_W as in Theorem 1, the success probability of the attack is given as*

$$P_S = 2 - 2\Phi\left(\frac{\sigma_W}{\sigma_R} \cdot \Phi^{-1}(1 - 2^{-a-1})\right), \tag{5}$$

where Φ and Φ^{-1} denote the cumulative distribution function and quantile of the central normal distribution. Equivalently, the data complexity N^{KP} or N^{DKP} of a linear attack using non-distinct or distinct known plaintexts can be estimated as follows:

$$\begin{aligned} N^{\mathrm{KP}} &= \frac{\Phi^{-1}(1-2^{-a-1})^2 - \Phi^{-1}(1-P_S/2)^2}{ELP\,\Phi^{-1}(1-P_S/2)^2 - 2^{-n}\Phi^{-1}(1-2^{-a-1})^2}, \\ N^{\mathrm{DKP}} &\approx \frac{\Phi^{-1}(1-2^{-a-1})^2 - \Phi^{-1}(1-P_S/2)^2}{(ELP-2^{-n})\Phi^{-1}(1-P_S/2)^2}. \end{aligned}$$

Proof. For the purpose of this proof we denote by CDF_R and CDF_W the cumulative distribution functions of the normal distributions $\mathcal{N}(0,\sigma_R^2)$ and $\mathcal{N}(0,\sigma_W^2)$ with $\sigma_R^2 = \frac{B}{N} + ELP$ and $\sigma_W^2 = \frac{B}{N} + 2^{-n}$ as in Section 2. The probability density functions of these distributions are illustrated in Figure 2.

Given an acceptance threshold Θ, the non detection error probability $1-P_S$ corresponds to the case where $-\Theta < \hat{c}_R < \Theta$ (see Figure 2). Meaning that $1 - P_S = CDF_R(\Theta) - CDF_R(-\Theta)$. Similarly the false alarm error probability 2^{-a} corresponds to the case where $\hat{c}_W \le -\Theta$ or $\hat{c}_W \ge \Theta$. We obtain that $1 - P_S = 2\Phi(\Theta/\sigma_R) - 1$ and $2^{-a} = 2\Phi(-\Theta/\sigma_W)$, where Φ is the cumulative distribution function of the central normal distribution.

For correctly selected parameters we can find Θ such that

$$\Theta = \sigma_R\Phi^{-1}(1 - P_S/2) = \sigma_W\Phi^{-1}(1 - 2^{-a-1}). \tag{18}$$

The success probability is then

$$P_S = 2 - 2\Phi\left(\frac{\sigma_W}{\sigma_R} \cdot \Phi^{-1}(1 - 2^{-a-1})\right).$$

To estimate the data complexity we first consider the KP case and take $B = 1$. From Equation 18 we obtain the equality

$$\frac{1}{N}\left(\Phi^{-2}(1 - P_S/2) - \Phi^{-2}(1 - 2^{-a-1})\right) = 2^{-n}\Phi^{-2}(1 - 2^{-a-1}) - ELP \cdot \Phi^{-2}(1 - P_S/2)$$

and consequently

$$N^{\mathrm{KP}} = \frac{\Phi^{-1}(1-2^{-a-1})^2 - \Phi^{-1}(1-P_S/2)^2}{ELP\Phi^{-1}(1-P_S/2)^2 - 2^{-n}\Phi^{-1}(1-2^{-a-1})^2}.$$

Now to consider the DKP case, we assume that $B \approx 1 - N/2^n$ and set

$$(1/N - 2^{-n} + ELP) \cdot \Phi^{-1}(1 - P_S/2)^2 - \frac{1}{N} \cdot \Phi^{-1}(1 - 2^{-a-1})^2 \approx 0$$

from where

$$N^{\mathrm{DKP}} \approx \frac{\Phi^{-1}(1-2^{-a-1})^2 - \Phi^{-1}(1-P_S/2)^2}{(ELP-2^{-n})\Phi^{-1}(1-P_S/2)^2}.$$

□

A.2 The Case With Different Means

Assuming that the statistic modeling the behavior of the scoring value for the wrong and the right keys follow normal distributions, we can use classical statistical methods [Sel08,BW12] to determine the success of the attack. The general idea is the following. Given two statistics T_R and T_W following normal distributions with respective parameters (μ_R, σ_R^2) and (μ_W, σ_W^2) and assume w.l.o.g. that $\mu_W < \mu_R$. Given the error probabilities, β and $\alpha = 1 - P_S$, let us denote by φ_β and φ_α the quantiles of the standard normal distribution corresponding to the probabilities $1-\beta$ and $1-\alpha$. It means that $\Phi(\varphi_\beta) = 1-\beta$ and $\Phi(\varphi_\alpha) = 1-\alpha$, where we have denoted by Φ the cumulative distribution function of the standard normal distribution. If it holds

$$\mu_W + \sigma_W \varphi_\beta \leq \mu_R - \sigma_R \varphi_\alpha, \tag{19}$$

we can select a threshold Θ such that

$$\mu_W + \sigma_W \varphi_\beta \leq \Theta \leq \mu_R - \sigma_R \varphi_\alpha,$$

Observing a value $T < \Theta$ the cryptanalyst decides that T is drawn from the distribution of T_W. Then the probability that this decision is wrong is equal to

$$\begin{aligned}
&\Pr(T_R < \Theta) = \Pr(\frac{T_R - \mu_R}{\sigma_R} < \frac{\Theta - \mu_R}{\sigma_R}) \\
&\leq \Pr(\frac{T_R - \mu_R}{\sigma_R} < -\varphi_\alpha) = \Pr(\zeta < -\varphi_\alpha) = 1 - \Pr(\zeta < \varphi_\alpha) = \alpha,
\end{aligned}$$

where we have denoted by ζ a random variable following a standard normal distribution. Similarly, we can verify that with this threshold value the probability that an observed value $T > \Theta$ is drawn from distribution of T_W is equal to β. In particular, if equality holds in Equation 19, we obtain the following success probability P_S

$$P_S = 1 - \alpha = \Phi\left(\frac{\mu_R - \mu_W - \sigma_W \Phi^{-1}(1-\beta)}{\sigma_R}\right).$$

Usually as the parameters of the normal distributions $\mathcal{N}(\mu_W, \sigma_W)$ and $\mathcal{N}(\mu_R, \sigma_R)$ depend on data, the data complexity of the attack is derived from this formula. The false alarm error probability β corresponds to the ratio of wrong keys which are accepted as potential key candidate. In [Sel08] and in recent research publications this one is expressed as $\beta = 2^{-a}$ where a is called the advantage of the attack and corresponds to the number of gained bits during the attack.

B Experiments on SIMON

B.1 Experimental Results

For experimental purpose, we use the implementation of [CW16] to attack 20 rounds of SIMON32/64. For this attack we take advantage of a distinguisher on 13 rounds with ELP estimated experimentally to $ELP = 2^{-28.19}$. The result of our experiments for $2^{31.5}$ and 2^{32} distinct plaintexts as well as for 2^{33} and 2^{35} non-distinct plaintexts are provided in Table 5. In the following we describe the different quantities given in this table.

- The first column of Table 5 indicates the sampling method.
- The second one corresponds to the data complexity N.
- We computed the success probability $P_S^{(exp)}$ of 1000 attacks for an advantage of 8 and of 3 bits and compared it to different theoretical success probabilities.

Table 5: Results of our experimental linear attacks on 20 rounds SIMON32/64. The different notations are defined in Appendix B.1. Values in brackets have been computed assuming that $N^{\mathrm{DKP}} = N^{\mathrm{KP}}$ since the corresponding models do not make distinction between DKP and KP sampling, that is, the estimates of the success probability are derived using binomial distributions.

Experiments	N	a	$P_S^{(exp)}$	$\mathbf{P_S^{(our)}}$	$P_S^{(bt)}$	$P_S^{(selcuk)}$	$P_S^{(min)}$	$P_S^{(max)}$
DKP	$2^{31.5}$	8	32.2%	**36.6**%	(26.7%)	(60.4%)	(23.5%)	(35.6%)
DKP	2^{32}	8	38.4%	**44.1**%	(36.8%)	(80.5%)	(24.9%)	(38.9%)
KP	2^{33}	8	30.6%	**35.3**%	61.7%	99.2%	26.1%	42.7%
KP	2^{35}	8	35.5%	**41.4**%	97.3%	100%	26.4%	43.7%
DKP	$2^{31.5}$	3	58.4%	**63**%	(87.4%)	(94.7%)	(25.9%)	(42.0%)
DKP	2^{32}	3	64.1%	**68.1**%	(94.2%)	(98.6%)	(26.2%)	(42.9%)
KP	2^{33}	3	60.5%	**62.2**%	99.5%	100%	26.4%	43.7%
KP	2^{35}	3	59.6%	**66.3**%	100%	100%	26.4%	43.7%

- $P_S^{(our)}$ corresponds to the estimate given in Equation 5 of this paper.
- $P_S^{(selcuk)}$ corresponds to the estimate given in [Sel08] and recalled below:

$$P_S^{(selcuk)} = \Phi\left(\sqrt{N \cdot ELP} - \Phi^{-1}(1 - 2^{-a-1})\right). \tag{20}$$

  This estimate does not take into consideration the key deviation and does not assume distinct plaintexts.

- As observed in [CW16], because of the key deviation of the correlation, the success probability of Selçuk (Equation 20) is very optimistic. As for SIMON32/64 it is possible to estimate the portion of keys with a given capacity, the authors of [CW16] suggested to use this knowledge to provide lower $P_S^{(min)}$ and upper $P_S^{(max)}$ bounds of the success probability. For a complete description we refer to [CW16]. These bounds seems to be accurate for an advantage of 8 bits but not for an advantage of 3 bits. The difference could be explained by the fact that they do not take into consideration the key deviation for the wrong keys.

- To complete the comparison we added the estimate of the success probability $P_S^{(bt)}$ of the attack given in [BT13] taking into consideration the key deviation only for the wrong keys.

$$P_S^{(bt)} = \Phi\left(\sqrt{N \cdot ELP} - \sqrt{1 + \frac{N}{2^n}}\Phi^{-1}(1 - 2^{-a-1})\right).$$

  Note that this estimate which does not take into consideration the key-deviation of the right key remain far from accurate.

These results validate the estimate of the data complexity and success probability of a linear attack given in Theorem 2

B.2 Distinct Known Plaintexts or Known Plaintexts

The surprising fact about the experiments of [CW16] is the experimental use of distinct plaintexts while the theoretical expression of the success probability is extracted from the binomial distribution. Thanks to the recently developed theory we know that this theoretical expression should correspond to the non-distinct plaintext case. The same observation could be done about the experimental linear attacks on the DES performed

in [Mat94, Jun04] however the data complexity was far enough from the full codebook for being observed in practice.

The following lemma provides the relation between distinct and non-distinct plaintexts.

Lemma 2. *Given a set of 2^n elements and taking randomly N elements in this set we expect to have $N_{\neq}$ different elements with*

$$N_{\neq} = 2^n \left(1 - (1 - 2^{-n})^N\right).$$

As a consequence in the cryptographic context for a data complexity N and a block cipher of size n bits the number of distincts elements is

$$N_{\neq} \approx 2^n[1 - \exp(-N2^{-n})].$$

For instance when $N = 2^{35}$ and $2^n = 2^{32}$ we have $N_{\neq} \approx 2^{31.99} \approx 2^{32}$ and as illustrated in Table 5 the success probabilities are of similar order of magnitude. In practice the maximal success probability could be reached using the full codebook in the distinct plaintext context. This observation is valid for all statistical attacks.

C The Matrix Method to Estimate the ELP of a Linear Characteristic

One round of SMALLPRESENT-[4] is represented in Figure 6.

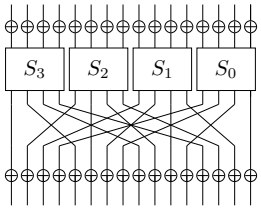

Figure 6: 1 round of SMALLPRESENT-[4]

In [Cho10] the matrix method has been used to estimate the ELP of linear approximations. In this section, we describe how this method is implemented and provide related matrices for SMALLPRESENT-[4]. The matrix method is particularly efficient for this cipher with strong 1-bit linear characteristics which propagate easily thought the different rounds. This property is derived from the correlation of the 1-bit linear approximations of the Sbox of PRESENT. The correlation values of these 1-bit masks are resumed in Table 6.

Table 6: Correlation $c(u, v)$ of the Sbox of PRESENT when u and v are 1-bit linear masks.

u/v	0x1	0x2	0x4	0x8
0x1	0	0	0	0
0x2	0	2^{-2}	-2^{-2}	2^{-2}
0x4	0	-2^{-2}	2^{-2}	-2^{-2}
0x8	0	2^{-2}	0	-2^{-2}

As the permutation of PRESENT is a bit permutation, these strong 1-bit linear approximations can be traced thought the cipher. The matrix $\mathcal{M}$ provided below corresponds to

the square correlations of all 1-bit linear characteristics over one round, non-linear and linear layer, of SMALLPRESENT-[4] (see Figure 6). For instance in column 6 row 6 we can read that the square correlation of the linear approximation $(\texttt{0x20}, \texttt{0x20})$ is 2^{-4}.

$$\mathcal{M} = \begin{pmatrix}
0&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0&0\\
0&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0&0\\
0&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0&0\\
0&0&0&0&2^{-4}&0&0&0&0&0&0&0&2^{-4}&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0\\
0&0&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0\\
0&0&0&0&0&2^{-4}&0&0&0&0&0&0&0&2^{-4}&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0&0&2^{-4}&0\\
0&0&0&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0&0&2^{-4}&0\\
0&0&0&0&0&0&2^{-4}&0&0&0&0&0&0&0&2^{-4}&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0&0&2^{-4}\\
0&0&0&0&0&0&0&2^{-4}&0&0&0&2^{-4}&0&0&0&2^{-4}\\
0&0&0&0&0&0&0&2^{-4}&0&0&0&0&0&0&0&2^{-4}
\end{pmatrix}$$

Observing that for the PRESENT's Sbox S, $c_S(u, v) = 0$ if $v = \texttt{0x2}, \texttt{0x4}, \texttt{0x8}$ and $u = \texttt{0x1}$ or if $u = \texttt{0x2}, \texttt{0x4}, \texttt{0x8}$ and $v = \texttt{0x1}$, some lines and columns of $\mathcal{M}$ can be removed in the computation. For SMALLPRESENT-[4], $\mathcal{M}$ can be reduced to a 9×9 matrix (values in black). For the 64-bit PRESENT the 64×64 matrix can be reduced to a 21×21 matrix.

To obtain the value of $\text{Exp}_K(Q(u, v)(K)^2) = \sum_{\tau \in \mathcal{S}} \rho_\tau^2$ of a 1-bit linear approximation where the set $\mathcal{S}$ corresponds to the strong 1-bit linear approximations, we just multiply the matrix $\mathcal{M}$ by itself. Below $\mathcal{M}^4$ is the result for 4 rounds of SMALLPRESENT-[4]. On this matrix we can read that the ELP of the linear approximation $(\texttt{0x20}, \texttt{0x20})$ over 4 rounds is $2^{-12.83}$. This quantity has been taken into consideration for the experiments of Subsection 2.4. If the last permutation is omitted, a linear permutation of $\mathcal{M}^4$ should be performed.

$$\mathcal{M}^4 = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&2^{-12.83}&2^{-13.42}&2^{-12.83}&0&2^{-13.42}&2^{-14.00}&2^{-13.42}&0&2^{-12.83}&2^{-13.42}&2^{-12.83}\\
0&0&0&0&0&2^{-12.83}&2^{-13.42}&2^{-12.83}&0&2^{-13.42}&2^{-14.00}&2^{-13.42}&0&2^{-12.83}&2^{-13.42}&2^{-12.83}\\
0&0&0&0&0&2^{-13.42}&2^{-14.42}&2^{-13.42}&0&2^{-14.00}&2^{-15.00}&2^{-14.00}&0&2^{-13.42}&2^{-14.42}&2^{-13.42}\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&2^{-12.83}&2^{-13.42}&2^{-12.83}&0&2^{-13.42}&2^{-14.00}&2^{-13.42}&0&2^{-12.83}&2^{-13.42}&2^{-12.83}\\
0&0&0&0&0&2^{-12.83}&2^{-13.42}&2^{-12.83}&0&2^{-13.42}&2^{-14.00}&2^{-13.42}&0&2^{-12.83}&2^{-13.42}&2^{-12.83}\\
0&0&0&0&0&2^{-13.42}&2^{-14.42}&2^{-13.42}&0&2^{-14.00}&2^{-15.00}&2^{-14.00}&0&2^{-13.42}&2^{-14.42}&2^{-13.42}\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&2^{-13.42}&2^{-14.00}&2^{-13.42}&0&2^{-14.42}&2^{-15.00}&2^{-14.42}&0&2^{-13.42}&2^{-14.00}&2^{-13.42}\\
0&0&0&0&0&2^{-13.42}&2^{-14.00}&2^{-13.42}&0&2^{-14.42}&2^{-15.00}&2^{-14.42}&0&2^{-13.42}&2^{-14.00}&2^{-13.42}\\
0&0&0&0&0&2^{-14.00}&2^{-15.00}&2^{-14.00}&0&2^{-15.00}&2^{-16.00}&2^{-15.00}&0&2^{-14.00}&2^{-15.00}&2^{-14.00}
\end{pmatrix}$$

D The Multidimensional Linear Space Used in our Experiments

The multidimensional linear space used in our experiments is represented in Figure 7. The multidimensional linear space is defined by the set of linear approximations $\{(u, v) \neq (0, 0) | u = (0 * 00) \text{ and } v = (00 * 0)\}$, where each symbol represents a nibble. This multidimensional linear space involving $\ell = 255$ linear approximations activate S_2 at the input and S_1 at the output.

E The 20-bit Key-Schedule

Let K be the 20-bit master key. The rounds keys are derived from the following rules:

- Left rotate K by 5 bits
- Apply the PRESENT Sbox to the 4 most significant bits of K

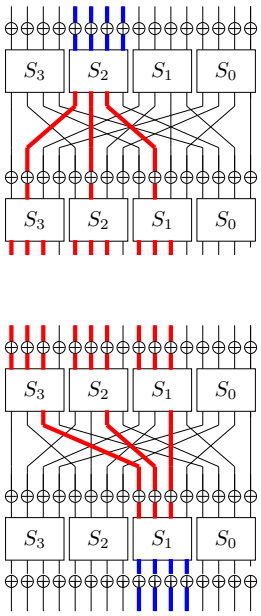

Figure 7: SMALLPRESENT and the one bit linear trails used for estimating the capacity

- Add a round counter to the least significant bits of K
- The round key corresponds to the 16 least significant bits of K

F Experiments over 6 and 7 Rounds

Experiments similar to the ones of Subsection 5.1 over 6 and 7 rounds of SMALLPRESENT-[4] are provided in Figure 8. These experiments have been performed in the DKP setting using 2^{15} plaintexts. On the left graphic, the slight underestimate of the capacity value (see Table 2) can be observed by the slight shift between the theoretical and experimental curves. This result could be explained by the use of the 1-bit linear trails to estimate the capacity of the linear approximation even if as resumed in Table 2 the difference between both expected values remain small. However we observe that the new variance estimate is better than the previous estimate.

In the right graphic we illustrate that when the capacity of the multidimensional linear approximation is close to the uniform one the capacity and its variance are correctly estimated. In this graphic previous and new estimates are similar.

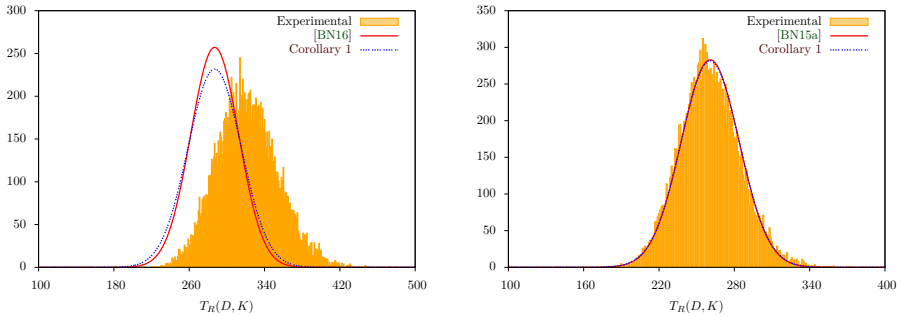

Figure 8: Comparison between the experimental distribution of $T_R(D, K)$ and normal distributions with different variances. Both figures are for 2^{15} plaintexts. Left: over 6 rounds. Right: over 7 rounds.

In these different experiments, we illustrate that when the expected capacity is correctly estimated then the new estimate of the variance provided in Corollary 1 is relatively accurate.