Joint Data and Key Distribution of the Linear Cryptanalysis Test Statistic and Its Impact to Data Complexity Estimates of Multiple/Multidimensional Linear and Truncated Differential Attacks

Céline Blondeau and Kaisa Nyberg

Department of Computer Science, Aalto University School of Science, Finland
celine.blondeau@aalto.fi, kaisa.nyberg@aalto.fi
24 September 2015

Abstract. The power of a statistical attack is inversely proportional to the number of plaintexts necessary to recover information on the encryption key. By analyzing the distribution of the random variables involved in the attack, cryptographers aim to provide a good estimate of the data complexity of such an attack. In this paper, we analyze the hypotheses made in simple, multiple, and multidimensional linear attacks that use either non-zero or zero correlations, and provide more accurate estimates of the data complexity of these attacks. This is achieved by taking, for the first time, into consideration the key variance of the statistic for both the right and wrong keys. For the family of linear attacks we differentiate between the attacks which are performed in the known-plaintext and those in the distinct-known-plaintext model. By this differentiation, we improve the data complexity of some attacks by applying the distinct-known-plaintext model. From the analysis provided in this paper, it follows that the number of attacked rounds in the multidimensional linear context is impacted by the fact that the expected capacity of a multidimensional linear approximation for a random permutation is not equal to zero as previously assumed. The impact of the result is relatively important, since it weakens most existing multidimensional linear attacks. From the link between differential and linear cryptanalysis we also derive a new estimate of the data complexity of a truncated differential attack. The theory developed in this paper is backed up by different experiments.
Keywords: multidimensional linear attack, zero-correlation linear attack, key-difference-invariant-bias attack, truncated differential attacks, known plaintext, distinct known plaintext, chosen plaintext, key variance, statistical model.
MSC 2010 codes: 94A60, 11T71, 68P25

1 Introduction

Classical linear [23] and differential [3] cryptanalysis are keystone of most statistical attacks. As generalization of differential attacks, truncated differential

attacks [20] take advantage of simultaneously multiple differential approximations. The question of taking advantage of multiple linear approximations was considered first in [4] for independent linear approximations and then in [18] for linear approximations with input and output masks covering a linear space. More recently zero-correlation linear attacks [9, 11, 13] were introduced. These attacks take advantage of linear approximation with no bias.

To estimate the data complexity of a statistical attack, the distributions of the involved random variables for the right and wrong keys are analyzed. In the following paragraphs we detail the different taken approaches and the improvements considered in this paper.

Distinct-known-plaintext attacks For the recent zero-correlation linear attacks, depending on the number of used approximations and on the relation between the involved linear masks, different statistical models are presented. We first recall the two models given in [9] to compute the data complexity of multiple zero-correlation linear attacks and multidimensional zero-correlation linear attacks. While the statistical model for the multidimensional zero-correlation linear attack assumes that the plaintexts involved in the attacks are distinct, the one for multiple zero-correlation linear attack assumes a normal distribution of the expected capacity for the wrong keys.

In this paper, we develop on distinct-known-plaintext attacks. In particular, we show that avoiding repetition in the plaintexts when the data complexity is close to the full codebook could present some interest not only for multidimensional zero-correlation attacks but also for multiple zero-correlation attacks and more generally for all known-plaintext attacks. In particular using distinct-known-plaintext we improve the data complexity of some multiple zero-correlation linear attacks and key-invariant attacks [8].

Right- and wrong-key randomization hypothesis For most ciphers, we are only able to estimate the expected value of a linear correlation. However, in [16, 17] the authors provide experiments to show that also significant variances occur and present an estimation of the wrong-key variance. In [12], this influence of the wrong-key variance for a simple linear attack is taken into consideration and a better estimate of the data complexity of a linear attack is given. In [19], the distribution of the capacity for the right encryption key is established and it is 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 has been previously taken in [22] in the case of single linear hull.

In this paper, we analyze and combine these different models and go beyond by studying the joint probability distribution of the test statistic as both the data sample and the key are considered as random variables. We present statistical models for both right-key and wrong-key behavior of the test statistic that comprise zero-correlation and ordinary, multiple and multidimensional linear cryptanalysis attacks, in distinct or non-distinct known-plaintext sampling models.

We show that the data complexity of multiple and multidimensional linear attacks can be computed using essentially the same methods. These attacks offer two different approaches for estimating the variance of the capacity. In the case of the PRESENT cipher [10] we observe experimentally that the standard deviation of capacity is underestimated when using the multidimensional linear approach, while it is overestimated when using the model of multiple independent approximations.

Expected value of the capacity for the wrong keys When modeling the distribution of the test statistic for the wrong keys, it is usually assumed that, for all keys, it behaves as it would have been computed for a single random permutation. In the linear context, this corresponds to the assumption that for each key the expected value of the observed correlation is equal to zero. Similarly, when taking into consideration multiple linear approximations, the test statistic computed from the data samples is assumed to be drawn from a uniform distribution for all wrong key candidates. In other words, the capacity, which corresponds to the sum of squared correlations, has been assumed to be equal to zero. However in this paper, we show that this hypothesis is not adequate and we suggest to take the expected value of the capacity for a wrong key to be equal to $\ell 2^{-n}$ where ℓ is the number of considered linear approximations and n is the encryption block size.

This finding, which has been experimentally verified, has a major impact on existing multidimensional linear attacks. Many such attacks exploited capacity values that are smaller than the expected random capacity. Consequently, we must invalidate the data complexity estimate by Hermelin, et al. [18]. In particular, the attack on 26 rounds of PRESENT [15] seems unrealistic. We show that using the key-recovery attack setting of [15], where the key candidates are used to partially invert one round before and one round after the multidimensional linear distinguisher, only 24 rounds of PRESENT can be attacked. The validity of other multidimensional linear attacks is also discussed in this paper.

Truncated differential attacks In [6], it has been shown that truncated differential attacks and multidimensional linear attacks are strongly related. Both attacks use the same distinguishing property of the cipher but assume that the data samples are provided differently and compute a different test statistic.

Based on the analysis provided in the linear context, we investigate the key variance of the statistics involved in truncated differential attacks, and improve the accuracy of the data complexity estimate of this attack. Then discussion on the validity of the truncated differential attack on 26 rounds of PRESENT [6] and of the known-key distinguisher [7] on the full PRESENT is also presented.

Experiments Our analysis has been backed up using experiments on reduced version of PRESENT but also on other ciphers. Unlike previous experiments we selected ciphers where it is possible to experiment on attacks that require almost the full codebook. Such experiments allowed us to analyze the evolution of the expected value and variance of the random variables involved in the attacks.

Outline The outline of this paper is as follows. The notation are introduced in Section 2. Section 3 focuses on the multiple/multidimensional zero-correlation linear attacks. The data complexity of key-invariant attacks [8] is also discussed in this section. In Section 4 a more accurate statistical model for multiple and multidimensional linear attacks is presented. Based on this model in Section 5, we provide new estimate of the data complexity of a multiple/multidimensional linear attacks. Following the same reasoning in Section 6, we present new models and new estimate of the data complexity for the classical linear attacks as well as for the truncated differential attacks. Section 7 concludes this paper.

2 Preliminaries

2.1 Linear Attacks

While the idea of using distinct-known plaintexts can be extended to any statistical attack, we focus in this paper on the most common known-plaintext statistical attacks which are generalizations of linear cryptanalysis [23].

Given an n-bit permutation F, we denote by $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$, a pair of input and output masks. In linear attacks, we take advantage of linear approximations of the form $u \cdot x \oplus v \cdot F(x) = 0$. The strength of a linear relation is measured by its correlation. The correlation of a Boolean function $f_{u,v}(x) = u \cdot x \oplus v \cdot F(x)$ is defined as

$$\mathrm{cor}(u, v) = 2^{-n}\Big[\#\left\{x \in \mathbb{F}_2^n | f_{u,v}(x) = 0\right\} - \#\left\{x \in \mathbb{F}_2^n | f_{u,v}(x) = 1\right\}\Big].$$

In [4] the statistical model of taking advantage of multiple independent linear approximations was presented. In the more recent multidimensional linear attacks introduced in [18], the attacker takes advantage of all linear approximations with linear masks (u, v) $u \neq 0$ in a linear space.

The capacity C defined in [4] and generalized in [18] is a quantity used to collect information of the strength of several linear approximations. Given a set of input and output linear mask pairs (u_i, v_i), $i = 1, \ldots, \ell$, where $v_i \neq 0$, their capacity is defined as the sum of the squared correlations:

$$C = \sum_{i=1}^{\ell} \mathrm{cor}(u_i, v_i)^2.$$

In case the linear approximations (u_i, v_i) form the set of non-zero elements of a linear space $U \times V$ of dimension s, that is, $\ell + 1 = 2^s$, then the capacity can be computed as

$$C = 2^s \sum_{j=0}^{\ell} \left(p_j - \frac{1}{\ell + 1}\right)^2,$$

where p_j is the probability that the value $(x, F(x))$ restricted to $U \times V$ takes on the value $j \in U \times V$. The attack is, in that case, called multidimensional linear attack.

While multiple/multidimensional linear attacks take advantage of a set of linear approximations with large capacity, multiple and multidimensional zero-correlation linear attacks [9, 11, 13] exploit linear approximations with correlation equal to zero. These attacks have been proven efficient on word-oriented structures such as Feistel-type ciphers. When multiple approximations with zero-correlation are used, the capacity C of the set of linear approximations is equal to zero.

In the remainder of this paper, we denote by ℓ the number of linear approximations involved in our attacks. Given s the dimension of the linear space $U \times V$, in (zero-correlation) multidimensional linear attacks we have $\ell = 2^s - 1$. The block cipher size is denoted by n.

2.2 Statistics

The data complexity N of a statistical attack corresponds to the number of plaintexts necessary to perform the attack. In general, we want to find the encryption key also known as right key by differentiating the score of the right key from the one of the wrong keys. In (zero-correlation) multiple/multidimensional linear attacks the test statistic of the scoring function corresponds to the estimated capacity of the multiple/multidimensional linear approximations:

$$T = N \sum_{1=1}^{\ell} \hat{\text{cor}}_i^2, \tag{1}$$

where $\hat{\text{cor}}_i$ is the empirical correlation of the i-th linear approximation (u_i, v_i). In (zero-correlation) multidimensional linear attacks the computation of the statistic T can be simplified and is equivalent to:

$$T = \sum_{j=0}^{\ell} \frac{(V[j] - N/(\ell+1))^2}{N/(\ell+1)}, \tag{2}$$

where $V[j]$ corresponds to the number of occurrences of the j-th element of the multidimensional distribution. In Section 4, we will use this same statistic when drawing a sample over any distribution of values computed from a plaintext.

Following the notation of [28], we denote by P_S the success probability and by a the advantage of the attack where 2^{-a} is the proportion of discarded keys.

Throughout this paper, we denote by Φ the cumulative distribution function of the central normal distribution. To simplify the notation, we also introduce: $\varphi_a = \Phi^{-1}(1 - 2^{-a})$ and $\varphi_{P_S} = \Phi^{-1}(P_S)$. Given $\text{Exp}(T_R)$ and $\text{Var}(T_R)$ (resp. $\text{Exp}(T_W)$ and $\text{Var}(T_W)$), the mean and variance of the normal random variable T_R for the right key (resp. T_W for the wrong keys), we have (see i.e. [28]):

$$P_S \approx \Phi\left(\frac{|\text{Exp}(T_R) - \text{Exp}(T_W)| - \sqrt{\text{Var}(T_W)}\varphi_a}{\sqrt{\text{Var}(T_R)}}\right). \tag{3}$$

2.3 Data Complexity of a Multidimensional Linear Attack

The multidimensional linear cryptanalysis [18] traditionally assumes known plaintext and that the cryptanalyst does not have any means to check for repetitions in the plaintext. Then the statistic T given in Equation (2) computed from the multidimensional distribution follows χ^2 distribution that for larger distributions, say $\ell > 50$ can be accurately approximated using the normal distribution stated as follows.

Lemma 1. *[18] In the known-plaintext model, the statistic T_R involved in a multiple/multidimensional linear attack for the right key follows approximately a normal distribution with parameters:*

$$\begin{aligned} \mathrm{Exp}(T_R) &\approx \ell + N \cdot C \text{ and} \\ \mathrm{Var}(T_R) &\approx 2(\ell + 2 \cdot N \cdot C). \end{aligned} \tag{4}$$

When distinguishing the cipher distribution from random, the alternative distribution was in [18] assumed to be given by a statistic T_W that, if computed over sufficiently large ℓ, follows the normal distribution with parameters $\mathrm{Exp}(T_W) = \ell$ and $\mathrm{Var}(T_W) = 2\ell$. Then the data complexity of a known-plaintext multidimensional linear attack was computed from these distributions as

$$N \approx \frac{\sqrt{4a\ell} + 4\Phi^{-1}(2P_S - 1)^2}{C}. \tag{5}$$

This approach assumes that the right key is fixed and that the capacity of the cipher data distribution with this key is equal to C. In practice, the same value C is used for all encryption keys. An estimate of C is obtained using offline analysis of the cipher. It is usually a lower bound of the average capacity over the keys and a positive value. Similarly for all of the wrong keys, the same uniform distribution of T_W is used as explained above. In [12, 24] this simple approach has been criticized and shown to produce too optimistic (for the attacker) results in practice.

In Section 4, we study the statistical distributions of multiple/multidimensional linear cryptanalysis as the encryption key and the wrong key candidates vary, and provide a more accurate estimate of the data complexity. We first recall some results on zero-correlation linear attack which in part motivated our work on distinct-known-plaintext attacks as well as on the analysis of key-variance for the right and wrong keys.

3 Zero-Correlation Linear Cryptanalysis

3.1 Multiple and Multidimensional Zero-Correlation Linear Attacks

In [9] we have the following two estimates of the data complexity of a multiple and multidimensional zero-correlation linear attacks derived from [11, 13].

Lemma 2. *[13] The number N of known plaintexts required in a multiple zero-correlation linear cryptanalysis is:*

$$N \approx \frac{2^n(\varphi_{PS} + \varphi_a)}{\sqrt{\ell/2} - \varphi_a}. \tag{6}$$

The proof [13] follows from Equation (3) using the fact that the distribution of T_R (resp T_W) can be estimated by a normal distribution with parameters $\mathrm{Exp}(T_R) = \ell$ and $\mathrm{Var}(T_R) = 2\ell$ (resp. $\mathrm{Exp}(T_W) = \ell(1 + \frac{N}{2^n})$ and $\mathrm{Var}(T_W) = 2\ell(1 + \frac{N}{2^n})^2$).

Lemma 3. *[9, 11][1] The number N of distinct-known plaintexts required in a multidimensional zero-correlation linear cryptanalysis is:*

$$N \approx \frac{2^n(\varphi_{PS} + \varphi_a)}{\sqrt{\ell/2} + \varphi_{PS}}. \tag{7}$$

The proof [9, 11] follows from the use of the hypergeometric distribution as it will be given in a more general case in Theorem 1.

Assuming as in the proof of Lemma 2 that the correlation of the involved linear approximations are independent, we can adapt this result to the context of multiple zero-correlation linear cryptanalysis. In practice, we observed, see Section 3.2, that the data complexity of a multiple zero-correlation linear attack can be estimated by Equation (7) when assuming distinct-known plaintexts. This result will be confirmed by the theory developed in Section 4.

Corollary 1. *The data complexity of a known-plaintext multiple/multidimensional zero-correlation linear attack using ℓ linear approximations is given by Equation (6). If we consider distinct-known plaintexts, the data complexity is given by Equation (7).*

Since for most attacks $0.5 \leq P_S \leq 0.99$, meaning that $0 \leq \varphi_{P_S} \leq 2.4$, the difference between Equation (7) and Equation (6) is particularly noticeable when $\sqrt{\ell/2}$ and φ_a are in the same order of magnitude. From Equation (7) and Equation (6) we deduce that the success probability of a known-plaintext zero-correlation linear attack is:

$$P_S \approx \Phi\left(\frac{N}{2^n}\sqrt{\ell/2} - \varphi_a\left(\frac{N + 2^n}{2^n}\right)\right), \tag{8}$$

and the one of a distinct-known-plaintext zero-correlation linear attack is:

$$P_S \approx \Phi\left(\frac{N\sqrt{\ell/2}}{2^n - N} - \varphi_a\frac{2^n}{2^n - N}\right). \tag{9}$$

[1] The distribution of the random variables has been derived in [11], the correct estimate of the data complexity appears in [9].

3.2 Experimental Results

We have implemented experiments on a Feistel-type cipher which is depicted in Figure 1 and could correspond to scaled versions of CLEFIA [29] (a 16-bit type-II GFN with 4 branches) .

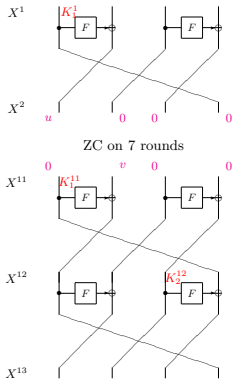


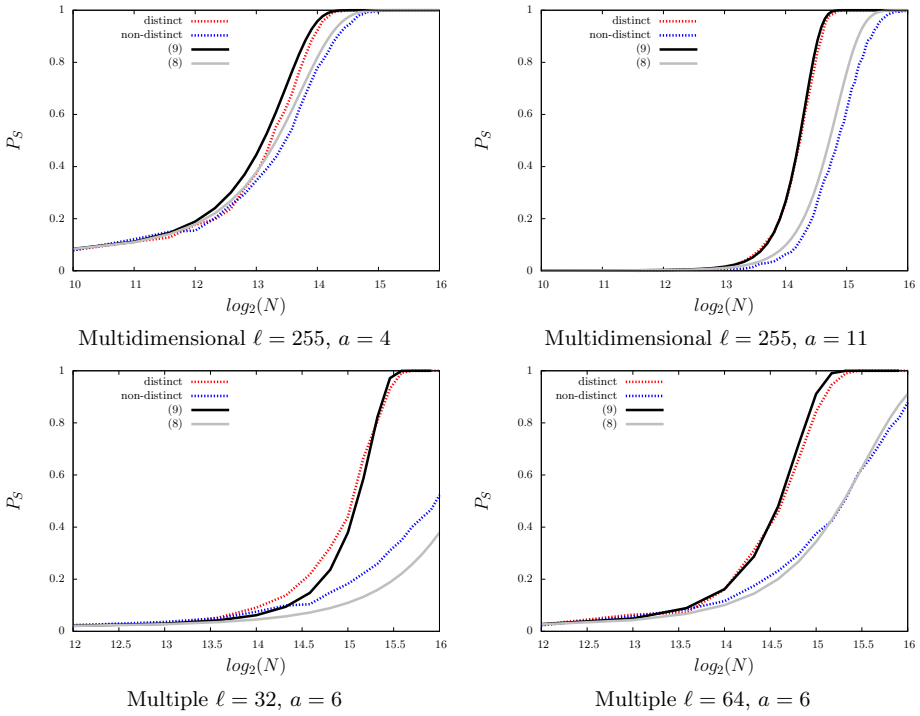
Fig. 1: Description of the key-recovery attack done on a Type-II GFN.

While in [30] experiments showing the distribution of $\mathrm{Exp}(T_R)$ and $\mathrm{Exp}(T_W)$ have been presented, there is, to the best of our knowledge, no previous mentioning of experimental zero-correlation linear attacks in the literature.

The results of our experimental attacks averaged over 1000 keys are provided in Figure 2. In these graphics we compare the success probability of multidimensional and multiple zero-correlation linear attacks with the theoretical ones given by Equation (9) for distinct plaintexts and by Equation (8) for non-distinct plaintexts. These experiments support the theory given in Section 3.1 showing that the same formula can be used to compute the complexity of multiple zero-correlation and multidimensional zero-correlation linear attacks. The difference lies only in the way of sampling, whether distinct or non-distinct known plaintexts are used in the attack.

3.3 Applications

Multiple Zero-Correlation Linear Attacks As explained in detail later in this paper, by considering distinct-known plaintexts we can use Equation (7) to compute the data complexity of a multiple zero-correlation linear attack. As the data complexity of multidimensional linear attacks has already been computed under this setting, and because other comparable (in number of attacked rounds) attacks have been performed in the chosen-plaintext model, this should give us a better comparison factor. The result of our computation and a comparison with the best attacks on the block cipher Camellia [1] are provided in Table 1. The attack is from [9]. The data complexity has been computed using Equation (7) instead of using Equation (6) with the parameters of the attack chosen as $P_S =$



Multidimensional $\ell = 255$, $a = 4$ | Multidimensional $\ell = 255$, $a = 11$

Multiple $\ell = 32$, $a = 6$ | Multiple $\ell = 64$, $a = 6$

Fig. 2: Attacks on a type-II-GFN cipher. Top: multidimensional zero-correlation linear attacks, bottom: multiple zero-correlation linear attacks.

0.85 and $a = 96$ or $a = 160$. The time complexity has been computed according to the description given in [9]. We use the abbreviations KP, DKP and CP for known plaintext, distinct-known plaintext and chosen plaintext, respectively.

Version	#R	Type	ℓ	a	P_S	N	Time	Mem.	Ref.
128	11	ID	-	-	-	$2^{118.4}$ CP	$2^{118.43}$	$2^{96.4}$	[14]
128	11	ZC	2^{14}	96	85%	$2^{125.3}$ KP	$2^{125.8}$	2^{112}	[9]
128	11	ZC	2^{14}	96	85%	$\mathbf{2^{125.1}}$ **DKP**	$2^{125.8}$	2^{112}	This paper
192	12	ID	-	-	-	$2^{119.7}$ CP	$2^{161.06}$	$2^{147.7}$	[14]
192	12	ZC	2^{14}	160	85%	$2^{125.7}$ KP	$2^{125.8}$	2^{112}	[9]
192	12	ZC	2^{14}	160	85%	$\mathbf{2^{125.46}}$ **DKP**	$2^{125.8}$	2^{112}	This paper

Table 1: Best key-recovery attacks on Camellia-128 and Camellia-192 (attacks starting from the first round). The memory is expressed in number of bytes. #R denotes the number of attacked rounds. ID stands for impossible differential, ZC for zero-correlation.

Similarly we can improve the data complexity of the multiple zero-correlation linear attack on CAST-128 [31]. The parameters of the attack being $n = 128$, $\ell = 64770$, $a = 50$ and $P_S = 0.85$, the data complexity of the attack using known plaintexts[2] is $N = 2^{123.73}$ and the data complexity of the attack using distinct-known plaintexts is $N = 2^{123.67}$.

Key-Difference-Invariant-Bias Attacks To the best of our knowledge, the only paper presenting attacks in this context is the seminal paper [8]. For these attacks, the statistical analysis is similar to the one done for zero-correlation linear attacks. In Table 2 we summarize the complexity of the best related key-attacks on LBlock [33] and show that by assuming distinct-known plaintexts the data and time complexity of the attack can be improved. Similar improvement can be obtained for the related-key attack on TWINE presented in [8]. The two-letter abbreviation RK refers to related-key attack throughout the table.

4 Statistical Attacks and Key Variance of Capacity

In the previous section we showed that the data complexity of zero-correlation linear attacks is reduced once we consider distinct-known plaintexts. The goal of this section is to examine if using distinct plaintext gives any advantage in other types of statistical attacks that analyze distributions of cipher data with non-zero capacity. Contrary to the zero-correlation property, which is the same for all encryption keys and hence has no variance due to the key, the non-zero capacities

[2] With these parameters, the data complexity can not be equal to $2^{123.2}$ as given in [31].

#R	Type	#Keys	ℓ	a	P_S	N	Time	Mem.	Ref.
23	RKID	4	-	-	-	$2^{61.4}$ RKCP	$2^{78.3}$	$2^{61.4}$	[32]
24	KIB	32	$2^{7.81}$	4.5	85%	$2^{62.29}$ RKKP	$2^{74.59}$	2^{61}	[8]
24	KIB	32	$2^{7.81}$	8.5	85%	$2^{62.95}$ RKKP	$2^{70.67}$	2^{61}	[8]
24	KIB	32	$2^{7.81}$	8.5	85%	$\mathbf{2^{62.38}}$ **RKDKP**	$2^{70.67}$	2^{61}	This paper
24	KIB	32	$2^{7.81}$	**16**	85%	$\mathbf{2^{62.84}}$ **RKDKP**	$\mathbf{2^{66.57}}$	2^{61}	This paper*

Table 2: Best related-key attacks on LBlock. *: Computation of the time complexity according to the description given in Section 5.3 of [8]. RKID stands for related-key impossible differential, KIB for key-invariant bias.

may vary with the key. We build a comprehensive model that takes also the key variance into account. In addition to the behavior of correct keys, the model is general enough so that it can be applied also for the modeling of the behavior of the wrong keys in key recovery attacks. Previously, strong evidence was brought up that it is not accurate to model wrong keys to draw test statistic from the uniform distribution [12, 24]. In [12] a solution was developed in the case of Matsui's classical linear attack Algorithm 2 with one linear approximation. We generalize this approach to attacks that use multidimensional distributions. The main motivation and challenges of the work presented in this section originate from the multidimensional linear attack, but due to the generic link between linear and differential types of attacks [6], the results can also be applied to some differential attacks.

4.1 Sampling of Cipher Data with Fixed Key

Next, we will extend Lemma 1 to cover also the case of sampling with distinct plaintext. The theorem is not specific to multidimensional linear cryptanalysis but can be applied to any statistical cryptanalysis that exploits distributions of samples of cipher data over a set of values.

Let $f : \mathbb{F}_2^n \to \{0, \ldots, \ell\}$ be a function which is used to compute values for plaintext $x \in D \subset \mathbb{F}_2^n$. In the setting of multidimensional linear cryptanalysis, $f(x)$ is the value of $(x, F(x))$ restricted to the subspace $U \times V$, see Section 2. The size of the sample set D is denoted by N. Let us denote

$$p_j = 2^{-n} |\{x \in \mathbb{F}_2^n \mid f(x) = j\}|.$$

for all $j = 0, \ldots, \ell$. Then p_j is a probability distribution and we denote by C its capacity, which is computed as

$$C = \sum_{j=0}^{\ell} \frac{\left(p_j - \frac{1}{\ell+1}\right)^2}{\frac{1}{\ell+1}}.$$

In the following, we consider simultaneously the cases were the sampling is done with or without replacement. To do so we introduce the following constant

B which is defined by

$$B = \begin{cases} 1, & \text{for non-distinct plaintext,} \\ 1 - \dfrac{N-1}{2^n - 1}, & \text{for distinct plaintext.} \end{cases} \tag{10}$$

Theorem 1. *We consider the statistic $B^{-1}T(D)$ where $T(D)$ is computed from the data sample D as defined by Equation (2) and B is defined by Equation (10). Then $B^{-1}T(D)$ follows a non-central χ^2 distribution with ℓ degrees of freedom and non-centrality parameter $B^{-1}NC$. In particular, $B^{-1}T(D)$ has the expected value and variance as*

$$\begin{aligned} \mathrm{Exp}_D(B^{-1}T(D)) &= \ell + B^{-1}NC \text{ and} \\ \mathrm{Var}_D(B^{-1}T(D)) &= 2\ell + 4B^{-1}NC. \end{aligned} \tag{11}$$

Proof. For each of the data values $j = 0, \ldots, \ell$ the attacker initializes a counter $V[j]$ to value zero. Then, for each sampled plaintext $x \in D$, the attacker computes the corresponding data value and increments the counter of this data value by one. If sampling is with replacement, then the variables $V[j]$ are statistically independent and each $V[j]$ follows the binomial distribution with parameters

$$\begin{aligned} \mathrm{Exp}_D(V[j]) &= Np_j \quad \text{and} \\ \mathrm{Var}_D(V[j]) &= Np_j(1-p_j). \end{aligned}$$

If repetitions of plaintexts are prevented then the counters $V[j]$ follow multivariate hypergeometric distribution. In particular, the variables $V[j]$ are statistically independent and the expected value and variance of $V[j]$ are equal to

$$\begin{aligned} \mathrm{Exp}_D(V[j]) &= Np_j \quad \text{and} \\ \mathrm{Var}_D(V[j]) &= Np_j(1-p_j)\left(1 - \frac{N-1}{2^n-1}\right). \end{aligned}$$

To proceed, we use the normal approximation of the binomial or in the case of distinct plaintext of the hypergeometric distribution of $V[j]$. In addition we estimate that

$$\mathrm{Var}_D(V[j]) = N\frac{1}{\ell+1}B,$$

for all $j = 0, \ldots, \ell$, where B is defined by Equation (10). This variance is slightly larger than what the variance of $V[j]$ would be for a uniform distribution. In this manner, the $\mathrm{Var}_D(V[j])$ are estimated to be equal for all j and the statistic T as defined in Equation (2) can be written as

$$T = \sum_{j=0}^{\ell} \frac{(V[j] - N\frac{1}{\ell+1})^2}{N\frac{1}{\ell+1}} = B\sum_{j=0}^{\ell} \frac{(V[j] - N\frac{1}{\ell+1})^2}{\mathrm{Var}_D(V[j])}.$$

By the definition of non-central χ^2 distribution, it then follows that $B^{-1}T$ follows a non-central χ^2 distribution with ℓ degrees of freedom and with non-centrality parameter

$$\delta = \sum_{j=0}^{\ell} \frac{(Np_j - N\frac{1}{\ell+1})^2}{N\frac{1}{\ell+1}B} = B^{-1}NC.$$

□

We note that Theorem 1 holds also if $C = 0$, and therefore includes the multidimensional zero-correlation statistical model using distinct plaintext given in [11] as a special case.

In an analogical way, we can also generalize the statistical model of the multiple linear approximation, which previously exists only for non-distinct plaintext, see [4] for the non-zero capacity case and [13] for the zero-correlation case.

Theorem 2. *We consider the statistic $B^{-1}T(D)$ where $T(D)$ is computed from the data sample D of size N using a number of ℓ independent linear approximations as defined by Equation (1), where B is as defined in Equation (10). Then $B^{-1}T(D)$ follows a non-central χ^2 distribution with ℓ degrees of freedom and non-centrality parameter $B^{-1}NC$, where C is the capacity of the ℓ linear approximations. In particular, $B^{-1}T(D)$ has the expected value and variance given as in Equation (11).*

Proof. Let us denote by Z_i the random variable corresponding to the number of solutions of the i-th equation of the form $u \cdot x \oplus v \cdot F(x) = 0$ and by $N \cdot p_i$ the expected number of solutions of this equation. By the assumption about the independence of the linear approximations, we can use the hypergeometric distribution, if the plaintexts are distinct, and otherwise the multinomial distribution to obtain, since $p_i = 1/2(1 + \mathrm{cor}_i)$,

$$\mathrm{Exp}_D(Z_i) = Np_i = \frac{N}{2}(1 + \mathrm{cor}_i) \text{ and}$$
$$\mathrm{Var}_D(Z_i) = Np_i\,(1 - p_i) = \frac{N}{4}(1 - \mathrm{cor}_i^2)B,$$

where B is defined as in Equation (10). Given $X_i = 2 \cdot Z_i/N - 1$ we deduce that $\mathrm{Exp}_D(X_i) = \mathrm{cor}_i$ and $\mathrm{Var}_D(X_i) = \frac{4}{N^2}\mathrm{Var}_D(Z_i) \approx \frac{1}{N} \cdot B$.

By Equation (1), we have $T(D) = N\sum_i X_i^2$. We denote $V(D) = \sum_{i=1}^{\ell} \frac{X_i^2}{\mathrm{Var}_D(X_i)} \approx T(D)B^{-1}$. The random variable $V(D)$ follows a non-central χ^2 distribution with parameters $\mathrm{Exp}_D(V(D)) = \ell + \delta$ and $\mathrm{Var}_D(V(D)) = 2(\ell + 2\delta)$ where $\delta = \sum_i \frac{\mathrm{Exp_D}(X_i)^2}{\mathrm{Var}_D(X_i)} = NCB^{-1}$. □

Theorem 2 and the assumption of statistical independence of linear approximations is needed in practice only if ℓ is relatively small in comparison to $2^s - 1$. Otherwise, Theorem 1 gives adequate estimates.

The non-central χ^2 distribution allows accurate approximation when it has more than about 50 degrees of freedom. In such a situation we can freely use the following corollary.

Corollary 2. *If in the setting of Theorem 1 or 2 the χ^2 distribution is approximated with the normal distribution, then the statistic $T(D)$ follows the normal distribution with parameters*

$$\begin{aligned} \mathrm{Exp}_D(T(D)) &= B\ell + NC \text{ and} \\ \mathrm{Var}_D(T(D)) &= 2B^2\ell + 4BNC. \end{aligned} \tag{12}$$

The mean and variance of the statistic T are studied in experiments on SMALLPRESENT-[8] and SMALLPRESENT-[4] presented in Section 4.5. While the expected value of T corresponds to the one given in the previous corollary, the variance deviates deviates significantly from the experimental one, in particular, for distinct-known plaintext. In the next sections, we adjust the model by taking into account the variance on T due to the key. We present a general model based on the joint data and key distribution which we will apply both to the right encryption keys as well as to wrong keys.

4.2 Key Variance of Capacity

In the preceding section, we presented a statistical model for sampling a cipher in multidimensional/multiple linear cryptanalysis, or more generally, for drawing samples of cipher values. When used in practice, an accurate estimate of the capacity of the set of linear approximations is needed. In the case of a key-alternating iterated block cipher, it is common to use the linear hull theorem, see i.e. Theorem 21 of [16], and the squared correlation matrices. For a practical example, see [15]. In this manner, one gets a lower bound of the average value of the capacity over the keys. In reality, the capacity may vary a lot with the key. Next we investigate what can be said in general about the variance of the capacity considered as a random variable computed for a random key. In this section, we investigate the key variance in the general setting. The next two sections are dedicated to the modeling of the right and wrong key behavior. The details of this section are provided for the multidimensional linear case and resumed at the end of this section in Corollary 4. The case of multiple independent linear approximations is handled in Corollary 5.

We consider distributions of data values as in the previous section, but now add the variable K to the notation to highlight the dependency of the key, and write

$$p_j(K) = 2^{-n}|\{x \in \mathbb{F}_2^n \mid f_K(x) = j\}|,$$

for all $j = 0, 1, \ldots, \ell$. In particular, the function f used in the previous section is now depending on the key K. If we consider K as a random variable, then also

the values $p_j(K)$ can be considered as random variables. Moreover, the capacity

$$C(K) = \sum_{j=0}^{\ell} \frac{(p_j(K) - \frac{1}{\ell+1})^2}{\frac{1}{\ell+1}}$$

is also consider as a random variable. The problem is, how to estimate the variance of $C(K)$. We take two approaches, first starting from the distribution definition of $C(K)$ and then looking at the more specific case of independent linear approximations. In both cases, we need additional assumptions.

Let us state the following assumption:

Hypothesis 1 *(Key-Variance Hypothesis) For all fixed data values j, the random variable $p_j(K)$ follows the normal distribution, that is,*

$$p_j(K) \sim \mathcal{N}(p_j, \sigma^2),$$

where the variance σ^2 is equal for all $j = 0, \ldots, \ell$.

With the notation used in Hypothesis 1, we indicate that the expected values $p_j = \mathrm{Exp}_K(p_j(K))$ of $p_j(K)$ taken over the random key K may be different while the variance $\mathrm{Var}_K(p_j(K))$ of $p_j(K)$ has the same value $\sigma^2 = \mathrm{Var}_K(p_j(K))$ for all $j = 0, \ldots, \ell$.

Under this hypothesis we can determine the distribution of a constant multiplier of $C(K)$.

Theorem 3. *Suppose that Hypothesis 1 holds for the distributions $p_j(K)$. Let us denote by C_0 the capacity of the expected distribution p_j, $j = 0, 1, \ldots, \ell$. Then*

$$\frac{C(K)}{(\ell+1)\sigma^2} \sim \chi^2_\ell(\delta),$$

where

$$\delta = \frac{C_0}{(\ell+1)\sigma^2}. \tag{13}$$

Proof. Let us denote $Q(K) = C(K)/(\ell+1)\sigma^2$. Then by Hypothesis 1 and the definition of the χ^2 distribution we get

$$Q(K) = \sum_{j=0}^{\ell} \frac{(p_j(K) - \frac{1}{\ell+1})^2}{\sigma^2} \sim \chi^2_\ell(\delta). \quad \square$$

In some cases, it is possible to derive the following relation between σ^2 and the expected capacity

$$\mathrm{Exp}_K(C(K)) = (\ell + \delta)(\ell+1)\sigma^2.$$

Such cases will be shown in the next two corollaries. Recall that the expected capacity, or an accurate estimate of it, may be available from an offline analysis of the cipher. If we can compute σ^2 given the expected capacity, then the parameters of the distribution of capacity will be determined. Let us denote the expected value of $C(K)$ taken over random K by the symbol C.

Corollary 3. *Suppose that the distributions $p_j(K)$ satisfy Hypothesis 1, and that $\ell > 50$. Then*

$$C(K) \sim \mathcal{N}\left(C, \frac{2\ell + 4\delta}{(\ell+\delta)^2} C^2\right).$$

Proof. By Theorem 3

$$\mathrm{Exp}_K\left(\frac{C(K)}{(\ell+1)\sigma^2}\right) = \ell + \delta,$$

from where we obtain $C = \mathrm{Exp}_K C(K) = (\ell+\delta)(\ell+1)\sigma^2$. □

In the second case, $\delta = 0$, that is, we have a central χ^2 distribution. Recall that if $X \sim \chi^2_\ell$ and $a > 0$ then $aX \sim \Gamma\left(\frac{\ell}{2}, 2a\right)$ with $\mathrm{Exp}(aX) = a\ell$ and $\mathrm{Var}(aX) = 2\ell a^2$.

Corollary 4. *(Multidimensional case) Suppose that the distributions $p_j(K)$ satisfy Hypothesis 1, and $p_j = \frac{1}{\ell+1}$, that is, $C_0 = 0$. Then $\delta = 0$, and $C(K)$ follows gamma distribution*

$$C(K) \sim \Gamma\left(\frac{\ell}{2}, 2(\ell+1)\sigma^2\right)$$

and its expected value and variance are

$$\mathrm{Exp}_K(C(K)) = \ell(\ell+1)\sigma^2 = C,$$
$$\mathrm{Var}_K(C(K)) = 2\ell\left((\ell+1)\sigma^2\right)^2 = \frac{2}{\ell}C^2.$$

Note that Hypothesis 1 holds trivially for $\ell = 1$ and for one-dimensional linear approximations with a large number of characteristics. Moreover, for a long-key cipher the expected value of the correlation is equal to zero. Then we get Theorem 22 of [16] as a special case of Corollary 4 with $\ell = 1$, and moreover, can apply it to linear approximations with i.i.d correlations (as the key varies) to obtain the following result.

Corollary 5. *(Multiple case) Suppose that we have multiple statistically independent linear approximations (u_i, v_i) such that $\mathrm{cor}(u_i, v_i) = \mathrm{cor}_i(K) \sim \mathcal{N}(0, \lambda)$, for all $i = 1, \ldots, \ell$. Then*

$$\frac{C(K)}{\lambda} = \frac{\sum_{i=1}^{\ell} \mathrm{cor}_i^2}{\lambda} \sim \chi^2_\ell,$$

and $C(K)$ has the following expected value and variance

$$\mathrm{Exp}_K(C(K)) = \ell\lambda = C,$$
$$\mathrm{Var}_K(C(K)) = 2\ell\lambda^2 = \frac{2}{\ell}C^2.$$

4.3 Statistical Model for the Right Key

In this section we will show how to build a comprehensive statistical model of the right-key behavior of the statistic T given in Equations (1) and (2) by considering it as a random variable over the random data sample D of size N and the random key K. To highlight this approach we denote $T = T(D, K)$, and compute its expected value and variance over D and K using the common rules as follows:

$$\begin{aligned} &\mathrm{Exp}_{D,K}\left(T(D,K)\right) = \mathrm{Exp}_K\left(\mathrm{Exp}_D(T(D,K))\right), \\ &\mathrm{Var}_{D,K}\left(T(D,K)\right) = \mathrm{Exp}_K\left(\mathrm{Var}_D(T(D,K))\right) + \mathrm{Var}_K\left(\mathrm{Exp}_D(T(D,K))\right) \end{aligned} \quad (14)$$

The values $\mathrm{Exp}_D(T(D,K))$ and $\mathrm{Var}_D(T(D,K))$ were derived in Section 4.1. To compute the variance over the key $\mathrm{Var}_K\left(\mathrm{Exp}_D(T(D,K))\right.$ we use the results from Section 4.2 and must make some assumptions about the behavior of the cipher.

In the special case of a key alternating block cipher with independent round keys, it is well known that the average of the correlation $\mathrm{cor}_{u,v}(K)$ taken over the keys is equal to zero, which is easy to prove directly. Then by using the well known fact

$$p_j(K) = \frac{1}{\ell+1}\sum_{u,v}(-1)^{(u,v)\cdot j}\mathrm{cor}_{u,v}(K)$$

we obtain that the average value of $p_j(K)$ taken over all keys K is equal to $\frac{1}{\ell+1}$ for all $j = 0, \ldots, \ell$.

In general, if the round keys are not independent, it is difficult to compute the averages of $p_j(K)$ over the keys and to check how uniform they are. In Figure 1 of [27] such computations have been done over 7 rounds of PRESENT using correlation matrices, but this approach is not feasible over many more rounds due to the details of the key schedule. Nevertheless, it may be quite realistic to assume that practical ciphers with strong key schedules have this property.

Next we state assumptions under which we can build the model for the right-key behavior. The statistical models presented in [19] are based on the same assumptions although only the first one is highlighted there as a hypothesis.

Hypothesis 2 *(Right-Key Hypothesis - Multidimensional) For each fixed value $j \in \{0, 1, \ldots, \ell\}$, the random variables $p_j(K)$ computed for random encryption keys K follow the normal distribution, that is,*

$$p_j(K) \sim \mathcal{N}(\frac{1}{\ell+1}, \sigma^2),$$

where the variance σ^2 is equal for all $j = 0, 1, \ldots, \ell$.

Hypothesis 3 *(Right-Key Hypothesis - Multiple) For each fixed value $i \in \{1, \ldots, \ell\}$, the random variables $\mathrm{cor}_i(K)$ computed for random encryption keys K follow the normal distribution, that is,*

$$\mathrm{cor}_i(K) \sim \mathcal{N}(0, \lambda),$$

where the variance λ, that is, the average squared correlation (also denoted as ELP), is equal for all $i = 0, 1, \ldots, \ell$.

Then by Theorems 1 and 2 and Corollaries 4 and 5 we obtain the following result:

Theorem 4. *Suppose that the random variables $p_j(K)$, $j = 0, 1, \ldots, \ell$ satisfy Hypothesis 2, or alternatively, $\mathrm{cor}_i(K)$, $i = 1, \ldots, \ell$ satisfy Hypothesis 3. Let us denote by C_R the expected value of the capacity for the right key. Then the statistic $T_R(D, K)$ computed either as in Equation (2) or as in Equation (1), respectively, has the following mean and variance*

$$\begin{aligned} \mathrm{Exp}_{D,K}\left(T_R(D,K)\right) &= B\ell + NC_R \text{ and} \\ \mathrm{Var}_{D,K}\left(T_R(D,K)\right) &= \frac{2}{\ell}\left(B\ell + NC_R\right)^2, \end{aligned} \tag{15}$$

where B is defined as in Equation (10).

Proof. By the above mentioned results, we have

$$\begin{aligned} &\mathrm{Exp}_K\left(\mathrm{Var}_D(B^{-1}T_R(D,K)\right) = 2\ell + 4B^{-1}NC_R \text{ and} \\ &\mathrm{Var}_K\left(\mathrm{Exp}_D(B^{-1}T_R(D,K)\right) = \mathrm{Var}_K\left(\ell + B^{-1}NC_R(K)\right) = 2B^{-2}N^2\ell^{-1}C_R^2. \end{aligned}$$

Combining these using Equation (14) gives the variance of $B^{-1}T_R(D, K)$ as $\frac{2}{\ell}\left(\ell + B^{-1}NC_R\right)^2$, from where we get the claimed value of the variance of $T_R(D, K)$. □

4.4 Statistical Model for the Wrong Keys

In this section, the results from Section 4.2 are applied to determine the parameters of the distribution of the test statistic computed for a wrong key.

Another important class of applications are the data distributions obtained using wrong keys in key-recovery algorithms. Next we formulate a general wrong-key randomization hypothesis which generalizes the one given in [12] to the case where the distinguisher is based on a distribution of a data value of more than one bit.

Hypothesis 4 *(Wrong-Key Hypothesis - Multidimensional) For any fixed j the random variables $p_j(K)$ over the wrong keys K follow the normal distribution with*

$$p_j(K) \sim \mathcal{N}\left(\frac{1}{\ell+1}, 2^{-n}\frac{1}{\ell+1}(1 - \frac{1}{\ell+1})\right).$$

The rationale behind this hypothesis is that when the key is wrong and the full plaintext space of size 2^{-n} is sampled the number of plaintexts that give the value j is binomially distributed with uniform probability $\frac{1}{\ell+1}$.

For the special case $\ell = 1$ studied in [12] this hypothesis means that the bias $p_0(K) - \frac{1}{2}$ is normally distributed with the mean equal to zero and the variance

equal to 2^{-n-2} thus agreeing with the wrong-key hypothesis stated in [12], see also [16], Corollary 6.

Under this wrong-key hypothesis and by substituting $\sigma^2 = 2^{-n}\frac{1}{\ell+1}(1-\frac{1}{\ell+1})$ to the result of Corollary 4 we get the following capacity distribution for the wrong keys.

Corollary 6. *(Multidimensional case) For the wrong keys K the quantity $C(K)$ corresponding to the capacity of the distribution $p_j(K)$ follows gamma distribution*

$$C(K) \sim \Gamma\left(\frac{\ell}{2}, 2^{1-n}(1-\frac{1}{\ell+1})\right).$$

The mean and the variance are as follows

$$\begin{aligned}\mathrm{Exp}_K(C(K)) &= 2^{-n}\ell(1-\frac{1}{\ell+1})\\ \mathrm{Var}_K(C(K)) &= 2^{1-2n}\ell(1-\frac{1}{\ell+1})^2 = \frac{2}{\ell}\mathrm{Exp}_K(C(K))^2.\end{aligned}$$

Let us note that Corollary 7 of [16] is a special case of this result with $\ell = 1$.

When the linear attack involves multiple independent linear approximations we make the following assumption about the behavior of wrong keys.

Hypothesis 5 *(Wrong-Key Hypothesis - Multiple) The correlations $\mathrm{cor}_i(K)$, $i = 1, \ldots, \ell$ over the wrong keys K are i.i.d. and follow the normal distribution with*

$$\mathrm{cor}_i(K) \sim \mathcal{N}\left(0, 2^{-n}\right).$$

We apply Corollary 5 again to get the following capacity distribution for the wrong keys when multiple independent linear approximations are used, and we get another generalization of Corollary 7 of [16].

Corollary 7. *(Multiple case) For the wrong keys K the quantity $C(K)$ corresponding to the capacity of the ℓ independent linear approximations (u_i, v_i) follows a gamma distribution*

$$C(K) \sim \Gamma\left(\frac{\ell}{2}, 2^{1-n}\right).$$

The mean and the variance are as follows

$$\begin{aligned}\mathrm{Exp}_K(C(K)) &= 2^{-n}\ell\\ \mathrm{Var}_K(C(K)) &= \frac{2}{\ell}\mathrm{Exp}_K(C(K))^2 = 2^{1-2n}\ell.\end{aligned}$$

If we denote the expected wrong-key capacity by C_W we have also in the multidimensional case

$$\begin{aligned}C_W &= \mathrm{Exp}_K(C(K)) \approx 2^{-n}\ell \text{ and}\\ \mathrm{Var}_K(C(K)) &= \frac{2}{\ell}C_W^2 \approx 2^{1-2n}\ell\end{aligned} \tag{16}$$

for larger ℓ. We will use this estimate in the following.

Analogically to the case of the right-key distribution we apply the results from Sections 4.1 and 4.2 and combine them to get the following distribution of the statistic $T(D,K)$ which we now denote by $T_W(D,K)$ as it is computed from the wrong-key data.

Theorem 5. *Suppose that the random variables $p_j(K)$, $j = 0, 1, \ldots, \ell$ satisfy Hypothesis 4, or alternatively, the correlations $\mathrm{cor}_i(K)$, $i = 1, \ldots, \ell$ satisfy Hypothesis 5. Then the statistic $T_W(D,K)$ computed either as in Equation (2) or as in Equation (1), respectively, has the following mean and variance*

$$\begin{aligned} \mathrm{Exp}_{D,K}\left(T_W(D,K)\right) &\approx B\ell + NC_W \text{ and} \\ \mathrm{Var}_{D,K}\left(T_W(D,K)\right) &\approx \frac{2}{\ell}\left(B\ell + NC_W\right)^2, \end{aligned} \tag{17}$$

where B is defined as in Equation (10).

We highlight the following special case and state it as a separate corollary.

Corollary 8. *In the context of Theorem 5 suppose that sampling is done using distinct plaintexts. Then the statistic $T_W(D,K)$ has the following mean and variance*

$$\begin{aligned} \mathrm{Exp}_{D,K}\left(T_W(D,K)\right) &\approx \ell \text{ and} \\ \mathrm{Var}_{D,K}\left(T_W(D,K)\right) &\approx 2\ell. \end{aligned}$$

Proof. By substituting $C_W = \ell 2^{-n}$ and $B = (2^n - N)/(2^n - 1)$ to Equation (17) we get the result. □

Interestingly, these are exactly the parameters that have been used in previous works to model the wrong-key distribution for sampling without replacement in multidimensional zero-correlation attacks, for example, in the derivation of Lemma 3 in [9, 11]. However, no justification of these parameter values can be found in the previous literature. As sampling with replacement from a uniform distribution has the same parameters, it is possible that those parameters have been reused in the lack of anything better. Fortunately, the parameter values were correct and the existing zero-correlation attacks that use distinct plaintext remain correct.

The situation is not that fortunate for general multidimensional linear attacks that use non-distinct plaintext. The data complexity estimate as given in Equation (5) has been derived under the hypothesis that the wrong-key data is drawn from the uniform distribution with $\mathrm{Exp}_{D,K}\left(T_W(D,K)\right) = \ell$ and $\mathrm{Var}_{D,K}\left(T_W(D,K)\right) = 2\ell$, see Equation (17) of [18]. This is certainly too optimistic for the attacker, since the true cipher data distributions in multidimensional linear approximations never become completely uniform, independently of how many rounds of the cipher is considered. At the lowest, the capacity tends to be around $2^{-n}\ell$, that is, equal to the wrong-key capacity estimated by our analysis above. The more realistic values of parameters in the case of non-distinct plaintext are $\mathrm{Exp}_{D,K}\left(T_W(D,K)\right) = \ell(1 + N2^{-n})$ and $\mathrm{Var}_{D,K}\left(T_W(D,K)\right) = 2\ell(1 + N2^{-n})^2$ as given by our analysis in Theorem 5.

In the last two sections we have determined the means and variances of the joint data and key distributions for the right and wrong keys. If the number ℓ of approximations is large the non-central data distribution of the test statistic can be approximated with the normal distribution. Then also the gamma distribution of capacity over the key (right or wrong) can be approximated by the normal distribution, and consequently, the joint distribution is approximately normal.

Taking an alternative approach and considering the joint data and key distributions of the observed frequences $V[j] = V[j](D, K)$ and observed correlations $\hat{cor}_i = \hat{cor}_i(D, K)$ and assuming that they approximately follow normal destributions we can show that the test statistic $T(D, K)$ has a gamma distribution for all values of ℓ. Note that if for each fixed key the observed frequency (or the correlation) is assumed normal deviate, as previously done in this paper, and if as assumed in the key distribution hypothesis that its expected value over the key is also a normal deviate, then the assumption is satisfied for the joint data key distribution.

Theorem 6. *Suppose that in the context of Theorem 4 or Theorem 5 the observed random variables $V[j](D, K)$, $j = 0, 1, \ldots, \ell$ or $\hat{cor}_i(D, K)$, $i = 1, \ldots, \ell$ approximately follow normal distributions. Then*

$$T(D, K) \sim \Gamma\left(\frac{\ell}{2}, 2(B + N\frac{C}{\ell})\right),$$

in both the right key case $K = K_R$, $C = C_R$, and wrong key case $K = K_W$, $C = C_W$. Its mean and variance agree with the previously derived values in Equation (15) and, respectively, Equation (17).

Proof. We give the complete proof for the multidimensional case. The case of multiple independent approximations is analogical. By taking the fixed-key parameters as given in the proof of Theorem 1 and combining them with the ones assumed in Hypothesis 2, or respectively, Hypothesis 4, we obtain

$$\begin{aligned}
\mathrm{Exp}\left(\frac{1}{N}V[j](D, K)\right) &= \frac{1}{\ell + 1} \\
\mathrm{Var}\left(\frac{1}{N}V[j](D, K)\right) &= \frac{B}{N(\ell + 1)} + \sigma^2,
\end{aligned}$$

where by Corollary 4 we have $\sigma^2 = \dfrac{C}{\ell(\ell + 1)}$. It follows that

$$\begin{aligned}
T(D, K) &= \sum_{j=0}^{\ell} \frac{\left(V[j](D, K) - N\frac{1}{\ell+1}\right)^2}{N\frac{1}{\ell+1}} \\
&= (B + N\frac{C}{\ell}) \sum_{j=0}^{\ell} \frac{\left(\frac{1}{N}V[j](D, K) - \frac{1}{\ell+1}\right)^2}{\frac{B}{N(\ell+1)} + \frac{C}{\ell(\ell+1)}}.
\end{aligned}$$

By the assumption of the variables $V[j](D, K)$ have normal distribution, the claim follows. □

In the next section, we present results of our experiments. In particular we compare the theoretical estimates of the mean and the variance from Equations (12) and (15) with the experimental ones.

Further, in Section 5, we present the impact of this theory on the data complexity of multiple/multidimensional linear attacks. In all experiments the theoretical models we assume the joint data and key distribution to be close to the normal distribution.

4.5 Experiments on SMALLPRESENT-[8] and SMALLPRESENT-[4]

In this section, we compare the experimental and theoretical mean $\mathrm{Exp}_{D,K}(T_R(D,K))$ of the variable T_R in the cases of distinct-known-plaintext and of known-plaintext distinguishing attacks. The experiments have been conducted on two scale versions [21] of the block cipher PRESENT [10]. SMALLPRESENT-[8] is a 32-bit cipher designed with the 80-bit original key-schedule of PRESENT. SMALLPRESENT-[4] is a 16-bit cipher. The round functions of both ciphers are depicted in Figure 3. For the experiments on SMALLPRESENT-[4], a 20-bit key-schedule has been defined. The multidimensional distributions are respectively involving $\ell = 255$ and $\ell = 63$ linear approximations.

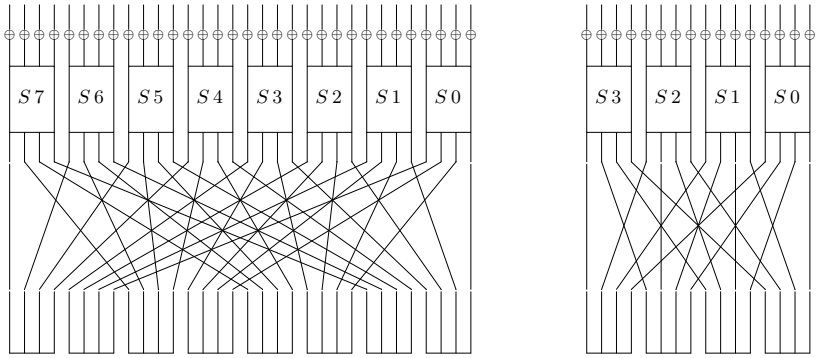


Fig. 3: The round function of SMALLPRESENT-[8] (left) and SMALLPRESENT-[4] (right).

In all cases the capacity of the multidimensional approximation used in the theoretical models is the true value determined from the cipher.

In Figures 4 and 5, we compare the theoretical means given by Equations (12) and (15) of statistic T_R with the experimental ones for both distinct and non-distinct plaintext. For this cipher, the values seem to match very well.

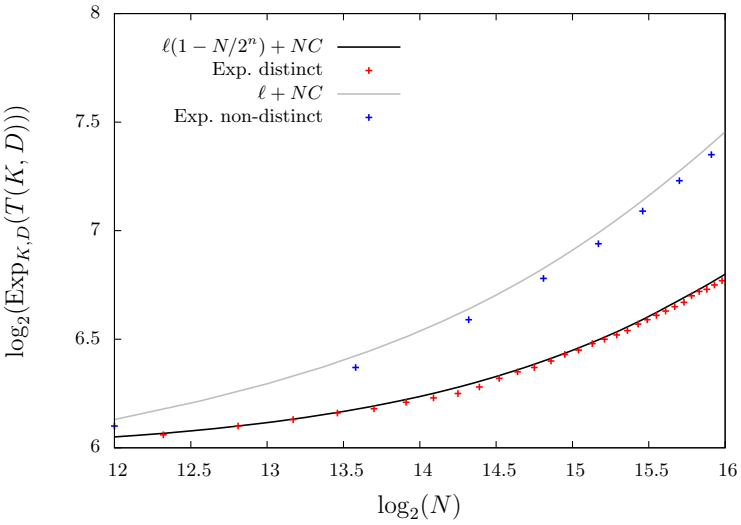


Fig. 4: The mean $\mathrm{Exp}_{D,K}(T_R(D,K))$ for a 6-bit multidimensional distribution ($\ell = 2^6 - 1$) over 4 rounds of SMALLPRESENT-[4] with capacity $C_R = 2^{-9.20}$.

In Figures 6 and 7, the corresponding variances are analyzed. We observe that the theoretical value is significantly improved when the key variance is taken into account. Still there is in all cases a clear gap between the theoretical value $\mathrm{Var}_{D,K}(T_R(D,K))$ given by Equation (15) and the experimental values of the variance.

In the computation of the theoretical value ℓ is taken equal to $2^s - 1$ where s is the dimension of the multidimensional linear approximation. It means that the model relies on the multidimensional Hypothesis 2. We checked the validity of the hypothesis, and only small deviation from it was observed in simulations on these SMALLPRESENT variants. On the other hand, it is known that due to the linear properties of the S-box, PRESENT ciphers allow accurate estimation of the capacity using single-bit linear characteristics that can be considered statistically independent. Therefore also the alternative approach of multiple independent linear approximations, that is, the use of Hypothesis 3 would be justified.

Let us examine these alternative approaches in the case of SMALLPRESENT-[8]. The observed multidimensional linear approximation consists of 4 bits of input to one S-box and 4 bits output of one S-box after 9 rounds. If Hypothesis 2 is applied, we take $\ell = 2^8 - 1$. By this approach we get an underestimate of the variance of T_R which is depicted in Figure 7. On the other hand, the

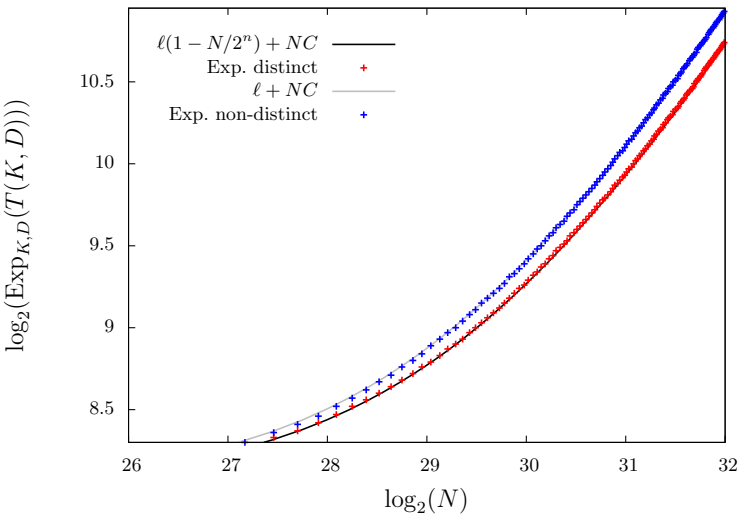


Fig. 5: The mean $\mathrm{Exp}_{D,K}(T_R(D,K))$ for a 8-bit multidimensional distribution ($\ell = 2^8 - 1$) over 9 rounds of SMALLPRESENT-[8] with capacity $C_R = 2^{-21.29}$.

capacity of this distribution can be estimated using the most dominant linear characteristics between these S-boxes, that is, by taking all single-bit characteristics leading from the three leftmost bits from the output of first S-box to the three leftmost bits of the input to the last S-box. If we then apply Hypothesis 3 to compute the variance, we take $\ell = 9$ in Corollary 4, meaning that instead of $2 \cdot 255 \cdot B^2 + 4BNC_R + \frac{2}{255}N^2C_R^2$ as given in Theorem 4 we have $\mathrm{Var}_{D,K}(T_R(D,K)) = 2 \cdot 255 \cdot B^2 + 4BNC_R + \frac{2}{9}N^2C_R^2$. This value, however, gives in our experiments an overestimate of the variance of T_R. The true value lies between these two extremes. While the gap between them seems quite big, its impact to the accuracy of the data complexity estimates turn out, however, to be relatively small as is demonstrated in the next section.

5 Data Complexity

5.1 Data Complexity Estimates

Corollary 9. *Let C_R and C_W the expected values of the capacity for respectively the right and wrong keys, as given in Section 4.3 and Section 4.4. Taking $\mathrm{Var}_{D,K}(T_R(D,K)) = \frac{2}{\ell}(B\ell + NC_R)^2$, we obtain that the data complexity estimates $N^{\mathrm{non-distinct}}$ and N^{distinct} in respectively the non-distinct and distinct*

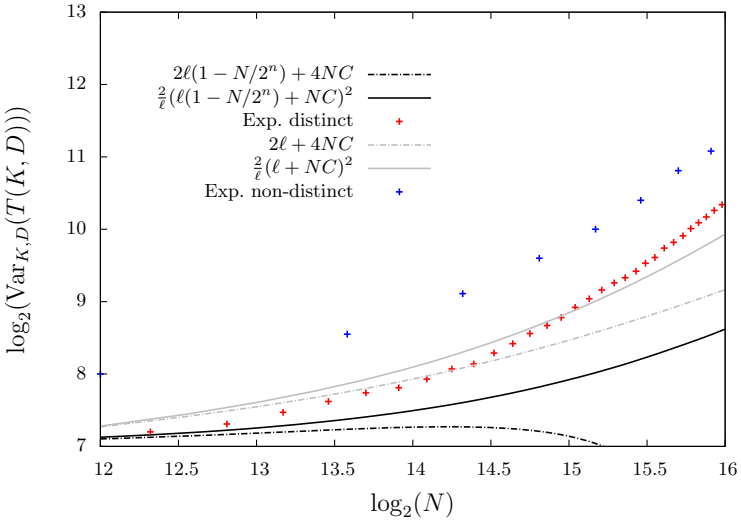


Fig. 6: The variance $\mathrm{Var}_{D,K}(T_R(D,K))$ for a 6-bit multidimensional distribution ($\ell = 2^6-1$) over 4 rounds of SMALLPRESENT-[4] with capacity $C_R = 2^{-9.20}$.

context are given by the following formulas.

$$N^{\text{non-distinct}} \approx \frac{\sqrt{2\ell}(\varphi_{P_S}+\varphi_a)}{|C_R-C_W| - \sqrt{2/\ell}(C_W\varphi_a + C_R\varphi_{P_S})}. \tag{18}$$

$$N^{\text{distinct}} \approx \frac{\sqrt{2\ell}(\varphi_{P_S}+\varphi_a)}{|C_R-C_W| - \sqrt{2/\ell}(C_W\varphi_a + C_R\varphi_{P_S}) + 2^{-n}\sqrt{2\ell}(\varphi_{P_S}+\varphi_a)}. \tag{19}$$

Proof. According to Equation (3) and Theorems 4, 5, we have

$$P_S \approx \Phi\left(\frac{N|C_R-C_W| - \sqrt{2/\ell}(B\ell+NC_W)\varphi_a}{\sqrt{2/\ell}(B\ell+NC_R)}\right). \tag{20}$$

We then deduce that

$$\sqrt{2/\ell}(B\ell+NC_R)\varphi_{P_S} \approx N|C_R-C_W| - \sqrt{2/\ell}(B\ell+NC_W)\varphi_a$$

and that

$$N\left(|C_R-C_W| - \sqrt{2/\ell}(C_W\varphi_a + C_R\varphi_{P_S})\right) \approx \sqrt{2\ell}B(\varphi_{P_S}+\varphi_a).$$

When the sampling is with replacement then $B=1$ and we obtain the result. If we consider distinct plaintexts then $B \approx 1 - \dfrac{N}{2^n}$ and

$$N\left(|C_R-C_W| - \sqrt{2/\ell}(C_W\varphi_a + C_R\varphi_{P_S}) + 2^{-n}\sqrt{2\ell}(\varphi_{P_S}+\varphi_a)\right) \approx \sqrt{2\ell}(\varphi_{P_S}+\varphi_a).\square$$

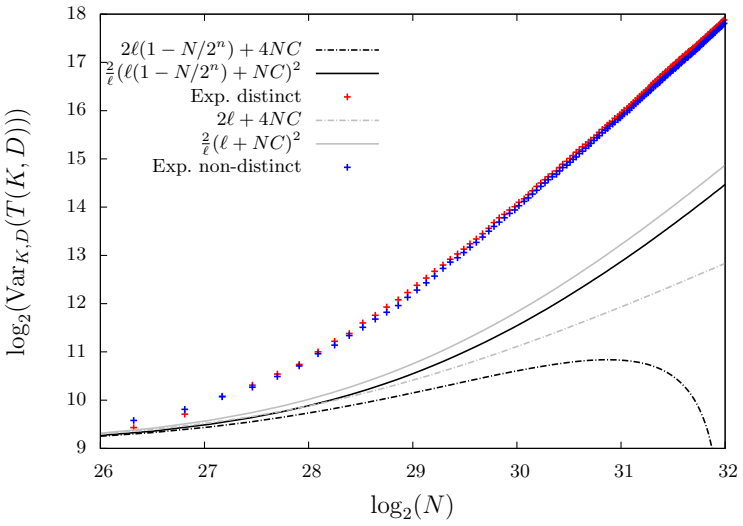


Fig. 7: The variance $\mathrm{Var}_{D,K}(T_R(D,K))$ for a 8-bit multidimensional distribution ($\ell = 2^8 - 1$) over 9 rounds of SMALLPRESENT-[8] with capacity $C_R = 2^{-21.29}$.

In the following to compare Equations (18) and (19) we denote by $\lambda \geq 0$ the quantity defined by $C_R = \lambda \cdot C_W$, $\lambda \geq 0$. As given by Equation (16) we have $C_W = \ell/2^n$ and Equation (18) becomes

$$N^{\mathrm{non-distinct}} \approx \frac{2^n(\varphi_a + \varphi_{P_S})}{|\lambda - 1|\sqrt{\ell/2} - (\varphi_a + \lambda\varphi_{P_S})},$$

and Equation (19) becomes

$$N^{\mathrm{distinct}} \approx \frac{2^n(\varphi_a + \varphi_{P_S})}{|\lambda - 1|\sqrt{\ell/2} - (\lambda - 1)\varphi_{P_S}}.$$

In the zero-correlation context we have $\lambda = 0$ and we obtain the results recalled in Section 3 for respectively the non-distinct and distinct sampling methods.

Remark 1. For practical attacks we have $P_S \geq 0.5$ and $a \geq 1$ meaning that φ_{P_S} and φ_a are positive values, and that $(\lambda - 1)\varphi_{P_S} \leq \varphi_a + \lambda\varphi_{P_S}$. Therefore we deduce that $N^{\mathrm{distinct}} \leq N^{\mathrm{non-distinct}}$.

5.2 Experiments on SMALLPRESENT-[4]

To perform a meaningful key-recovery attack, we simulated an attack on the 16-bit reduced version of PRESENT. For this attack we selected a multidimensional linear approximation of size $\ell = 2^6 - 1$ over 4 rounds. The key-recovery attack

was on 6 rounds meaning that 2 rounds were partially inverted. In Figure 8, we give the results of the experiments.

When repetition of plaintexts is allowed, our model provides an underestimate of the success probability at least up to the data complexity corresponding to the full codebook. In that case, it seems that it is also possible to have a data complexity larger than the full codebook.

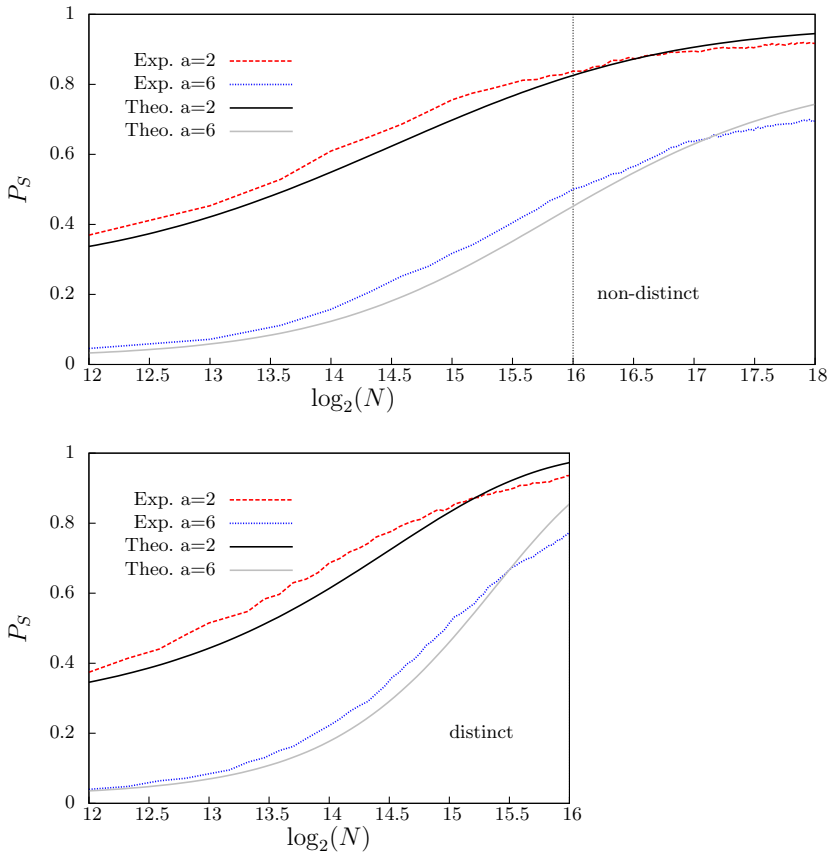


Fig. 8: Success probability of a key-recovery attack. The theoretical (Theo.) success probability is computed from Equation (20). The parameters are $n = 16$, $\ell = 2^6 - 1$, $C_R = 2^{-9.20}$, $C_W = 2^{-10}$. Top: Using non-distinct plaintexts ($B = 1$). Bottom: Using distinct plaintexts ($B = 1 - N/2^{16}$).

5.3 Impact on Existing Attacks

As explained in the end of Section 4.4, the previously developed theory to estimate the data complexity of a multidimensional attack assumes a wrong expec-

tation of $C_W(K)$. In particular, it was assumed that $C_W = \mathrm{Exp}_K(C_W(K)) = 0$, while we now show that this one is close to $2^{-n}\ell$.

In practice, except for zero-correlation attacks where $C_R = 0$, we often only obtain an underestimate of C_R. If this underestimate is smaller that C_W then $|C_R - C_W|$ is overestimated and according to Equations (18) and (19), the data complexity is underestimated. Therefore, it seems reasonable to assume that we can estimate the complexity of a multiple/multidimensional linear attack only if the computed value of C_R is larger than C_W. For instance in the multidimensional linear attack on PRESENT [15], the parameters are $\ell = 9 \cdot (2^8 - 1)$ and $n = 64$ meaning that $C_W = 2^{-52.83}$. The estimate of C_R derived from [15] for different number of rounds are resumed in Table 3. As for the attack on 26 rounds we have $C_R < C_W$, thanks to the theory developed in this paper we now know that using the multidimensional linear approximation of [15] with the current known estimate of the capacity, the multidimensional linear attack on 26 rounds of PRESENT is not possible. An attack on 25 rounds is only possible for an advantage of 1 bit and will require high time complexity.

		Data complexity		
r attacked rounds	Estimate of C_R (over $r-2$ rounds)	Previously (5)	$N^{\text{non-distinct}}$ (18)	N^{distinct} (19)
22	$2^{-44.94}$ (20 rounds)	$2^{53.06}$	$2^{53.2126}$	$2^{53.2118}$
23	$2^{-47.55}$ (21 rounds)	$2^{55.66}$	$2^{55.8584}$	$2^{55.8533}$
24	$2^{-50.16}$ (22 rounds)	$2^{58.28}$	$2^{58.7086}$	$2^{58.6723}$
25	$2^{-52.77}$ (23 rounds)	$2^{60.88}$	Not possible	Not possible
26	$2^{-55.38}$ (24 rounds)	$2^{63.50}$	Not possible	Not possible

Table 3: Multidimensional linear attacks on PRESENT. Computation with an advantage of 8 bits and $P_S = 0.95$.

In Table 3, we also compare the different estimates of the data complexity. The third columns corresponds to the estimate of the data complexity made in [18] and used in [15]. This estimate of the data complexity does not take into consideration the variance of the capacity for the right and wrong keys. Note that the estimate of the data complexity obtained in [19] takes into consideration the deviation for the right key but not for the wrong keys. The estimate of the data complexity is similar that that of Equation (5). When taking into consideration the deviation of the capacity for the different keys as well as the fact that $C_W = 2^{-n}\ell$ we obtain in paper the estimates of the data complexity given in the last two columns.

In this table, the difference in data complexity between the distinct and non-distinct models is relatively small. However in some cases this one can be larger. For instance, for the attack on 24 rounds of PRESENT if we take $a = 32$ instead of $a = 8$ and $P_S = 0.99$ we then have $N^{\text{non-distinct}} = 2^{59.77}$ and $N^{\text{distinct}} = 2^{59.69}$. More generally, using the previous results, to have $N^{\text{non-distinct}} > 2N^{\text{distinct}}$, we

should have $2\varphi_a + (\lambda+1)\varphi_{P_S} > |\lambda - 1|\sqrt{\ell/2}$. In the zero-correlation context ($\lambda = 0$), for a success probability of 0.5 ($\varphi_{P_S} = 0$) this is possible if $\varphi_a > \sqrt{\ell/8}$. Using for large advantages the approximation $\varphi_a \approx \sqrt{2a\log(2)}$ we obtain that $N^{\text{non-distinct}} > 2N^{\text{distinct}}$ if $a > \frac{\ell}{16\log(2)}$.

The results of this paper show that the impact of the key variance of the capacity for the right and wrong keys is relatively small (influencing slightly the data complexity of the attack) in comparison to the impact of a wrong estimate of the capacity for the wrong keys. In particular the latter result impacts most multidimensional/multiple linear attacks that we can find in the literature. In Table 4, we summarize the best multidimensional linear attacks on some ciphers and show that because C_R is estimated smaller than $C_W = 2^{-n}\ell$ using the current estimated of the capacity for the right key these attacks can not be performed.

Cipher	Attacked Rounds	n	ℓ	$C_W = 2^{-n}\ell$	C_R	Ref
PRESENT	27	64	$27 \cdot (2^4 - 1)^\star$	$2^{-55.34}$	$2^{-55.33}$	[34]
SERPENT	11	128	$2^{56} - 1$	2^{-72}	2^{-114}	[25]
SERPENT	12	128	$2^{56} - 1$	2^{-72}	2^{-116}	[25]
MIBS-80	19	64	$2^{12} - 1$	2^{-52}	$2^{-53.415}$	[2]

Table 4: Multidimensional linear attacks on some ciphers where $C_R < 2^{-n}\ell$. $\star$: according to the value given in [34].

From a similar analysis other attacks are also impacted. In the next section we show how the key variance influence the data complexity of truncated differential attacks.

6 Other Statistical Attacks

6.1 Classical Linear Attacks

In this section we present the impact of taking into consideration the key-variance on the data complexity estimate of the classical Matsui's Algorithm 2 which based on a single linear approximation (u, v) with only one dominant characteristic.

Let us first summarize the classical statistical model. The test statistic is based on the observed correlation $\hat{c} = \hat{\text{cor}}(u, v)$. Analogically to T_R and T_W in the previous sections, we denote by $\hat{c}_R$ and $\hat{c}_W$ the corresponding random variables for the right and wrong keys. By using the same notation as in Section 2.2 and by denoting $\varphi'_a = \Phi^{-1}(1 - 2^{-a-1})$ the success probability of a classical key-recovery linear attack is expressed as

$$P_S \approx \Phi\left(\frac{c - \sqrt{\text{Var}_{D,K}(\hat{c}_W)}\varphi'_a}{\sqrt{\text{Var}_{D,K}(\hat{c}_R)}}\right)$$

where c is the absolute value of the correlation of the dominant characteristic. For details, we refer to [26].

Until 2013 only the data variance of the observed correlation had been considered. In [12] the variance in the case of the wrong key was correctly adjusted to

$$\mathrm{Var}_{D,K}\left(\hat{c}_W(D,K)\right) = \frac{1}{N} + 2^{-n}.$$

We now complete the model by making the corresponding adjustment to the variance of the test statistic also in the right key case. It is well known by the linear hull theorem [16] that the average of the squared correlations of a characteristic is equal to the average squared correlation of the linear hull of the linear approximation with mask pair (u, v) usually denoted by $\mathrm{ELP}(u, v) = \mathrm{ELP}$, see [16, 17]. Then the variance of the distribution of the observed correlation for the encryption keys that have positive expected observed correlation is equal to $\mathrm{ELP} - c^2$ and similarly for the case of negative expected observed correlation. Hence the variance of the joint key and data distribution of the test statistic for the right key to be used in the computation of the success probability is equal to

$$\mathrm{Var}_{D,K}(\hat{c}_R(D,K)) = \frac{1}{N} + \mathrm{ELP} - c^2.$$

By substituting the adjusted variances to the formula of the success probability we get

$$P_S \approx \Phi\left(\frac{c\sqrt{N} - \sqrt{1 + N2^{-n}}\varphi'_a}{\sqrt{N(\mathrm{ELP} - \mathrm{c}^2) + 1}}\right).$$

If we take $\mathrm{ELP} = c^2$ for all encryption keys as in previous approaches, then this formula is identical to Equation (6) in [12].

In reality, assuming that there is a large number of other characteristics, the value $\mathrm{ELP} - c^2$ is bounded from below by the variance of random noise which is equal to 2^{-n}. Using this estimate, we obtain the following lower bound of the data complexity N, to achieve the given success probability P_S and advantage a,

$$N \geq \frac{(\varphi'_a + \varphi_{P_S})^2}{c^2 - (\mathrm{ELP} - c^2)(\varphi'_a + \varphi_{P_S})^2 + \varphi'^2_a(\mathrm{ELP} - c^2 - 2^{-n})}.$$

6.2 Impact on Truncated Differential Attacks

In [6], the following close relation between truncated differential and multidimensional linear attacks has been disclosed.

Theorem 7. *Let $F : \mathbb{F}_2^s \times \mathbb{F}_2^t \to \mathbb{F}_2^q \times \mathbb{F}_2^r$ and $n = s + t = q + r$. Let a truncated differential $[(0, \delta_t), (0, \Delta_r)]_{\delta_t \in \mathbb{F}_2^t, \Delta_r \in \mathbb{F}_2^r}$ with probability p equal to*

$$p = 2^{-t} \sum_{\delta_t \in \mathbb{F}_2^t, \Delta_r \in \mathbb{F}_2^r} P[(0, \delta_t) \xrightarrow{F} (0, \Delta_r)].$$

Let a multidimensional linear approximation $[(a_s, 0), (b_q, 0)]_{a_s \in \mathbb{F}_2^s,\, b_q \in \mathbb{F}_2^q}$ *with capacity* C *equal to*

$$C = \sum_{(a_s, b_q) \neq (0,0)} \mathrm{cor}^2 \left(a_s \cdot x_s \oplus b_q \cdot y_q\right).$$

We have

$$p = 2^{-q}(C + 1). \tag{21}$$

In the following we denote by p^*, the probability of the truncated differential when removing the input difference 0 from the set of differences.

$$p^* = 2^{-t} \sum_{\delta_t \in \mathbb{F}_2^t, \Delta_r \in \mathbb{F}_2^r, \delta_t \neq 0} P[(0, \delta_t) \xrightarrow{F} (0, \Delta_r)].$$

In [5], it was shown that $p^* = \dfrac{2^t}{2^t - 1} p - \dfrac{1}{2^t - 1}$. In the following, we use the approximation $p^* \approx p - 2^{-t}$.

Given N_S the number of generated pairs from the N plaintexts, and p^* the probability of the truncated differential, it was previously assumed (see for instance [5]) that the expected number of pairs fulfilling the differential was $N_s \cdot p^*$. The variance was assumed to be $N_S \cdot p^* \cdot (1 - p^*)$.

Meaning that given a data set D, and

$$T^{TD}(D) = \frac{1}{2} \#\{(x, x') \in D | x \oplus x' \in \mathbb{F}_2^t \setminus 0 \text{ and } F(x) \oplus F(x') \in \mathbb{F}_2^r\},$$

we have

$$\mathrm{Exp}_D(T^{TD}(D)) = N_S \cdot p^*,$$

and

$$\mathrm{Var}_D(T^{TD}(D)) = N_S \cdot p^*(1 - p^*).$$

Using the link between truncated differential and multidimensional linear attacks as well as the results of the previous section, we now integrate the key variance to this model. Note that as truncated differential attacks are usually performed in the known-plaintext model, the analysis provided in this section is derived from the distinct known plaintexts model of the previous sections.

As in the multidimensional linear context, we assume that the probability p^* is not identical for all encryption keys, and we denote by $p^*(K)$ the quantity

$$p^*(K) = \frac{1}{2} \#\{(x, x') \in \mathbb{F}_2^n | x \oplus x' \in \mathbb{F}_2^t \setminus 0 \text{ and } F_K(x) \oplus F_K(x') \in \mathbb{F}_2^r\}.$$

If we denote by $p^* = \mathrm{Exp}_K(p^*(K))$, from Equation (21) we obtain that $\mathrm{Var}_K(p^*(K)) = 2^{-2q}\mathrm{Var}_K(C(K))$. And that

$$\begin{aligned} \mathrm{Exp}_{D,K}(T^{TD}(D, K)) &= N_S \cdot p^*, \\ \mathrm{Var}_{D,K}(T^{TD}(D, K)) &= N_S \cdot p^*(1 - p^*) + N_S^2 2^{-2q} \mathrm{Var}_K(C(K)) \end{aligned} \tag{22}$$

If we take as in Section 4.3 $\mathrm{Var}_K(C_R(K)) \approx \frac{2}{\ell} C_R^2$ we obtain from $\ell = 2^{q+s} - 1$ that

$$\mathrm{Exp}_{D,K}(T_R^{TD}(D,K)) = N_S \cdot p_R^*,$$

and

$$\mathrm{Var}_{D,K}(T_R^{TD}(D,K)) \approx N_S \cdot p_R^*(1-p_R^*) + N_S^2 2^{1-q-s}(p_R^* + 2^{-t} - 2^{-q})^2. \quad (23)$$

The previous observation lead to the following hypotheses in the truncated differential context.

Hypothesis 6 *(Right-Key Hypothesis - Truncated Differential) The random variable $p_R^*(K)$ computed over the right keys follows the normal distribution, that is,*

$$p_R^*(K) \sim \mathcal{N}\left(p_R^*, 2^{1-q-s}(p_R^* + 2^{-t} - 2^{-q})^2\right),$$

Hypothesis 7 *(Wrong-Key Hypothesis - Truncated Differential) The random variable $p_W^*(K)$ computed over the wrong keys follows the normal distribution, that is,*

$$p_W^*(K) \sim \mathcal{N}\left(2^{-q}, 2^{1-q-n-t}\right),$$

In Figures 9 and 10 we plotted the mean and the variance for SMALLPRESENT-[4], using the same multidimensional distribution than in Section 5.2.

As from a similar analysis, we obtain for the wrong keys that

$$\begin{aligned} \mathrm{Exp}_{D,K}(T_W^{TD}(D,K)) &= N_S \cdot 2^{-q}, \\ \mathrm{Var}_{D,K}(T_W^{TD}(D,K)) &= N_S \cdot 2^{-q}(1-2^{-q}) + N_S^2 2^{1-q-n-t}. \end{aligned} \quad (24)$$

As showed latter in Corollary 10, this new estimate of the variance for the right and the wrong keys influence the success probability of a truncated differential attack.

Remark 2. While in previous research papers, it was wrongly assumed that for the wrong keys we have $C_W = 0$, this error was not made in the truncated differential context. Indeed, it was previously assumed that the uniform probability in the truncated differential context was $p_W^* = 2^{-q}$. Using the previous relations, we can directly find that $C_W = 2^q p_W - 1 \approx 2^q(2^{-t} + p_W^*) - 1 = 2^{q-t}$. From $\ell = 2^{q+s} - 1$ we obtain that $C_W \approx \ell \cdot 2^{-n}$. As shown by this derivation, in the link between truncated differential probability and the capacity of the associated multidimensional linear approximation, it is important to remove the input difference 0. In particular, the condition $C_R > \ell 2^{-n}$ is equivalent to the condition $p_R^* > 2^{-q}$. When we only have underestimate of the truncated differential probability, an attack in the truncated differential differential case is only possible when $p_R^* > 2^{-q}$. Meaning that when the truncated differential is derived from a multidimensional linear approximation, we should have $C_R > \ell \cdot 2^{-n}$ which is the limit for a valid attack in the multidimensional linear context.

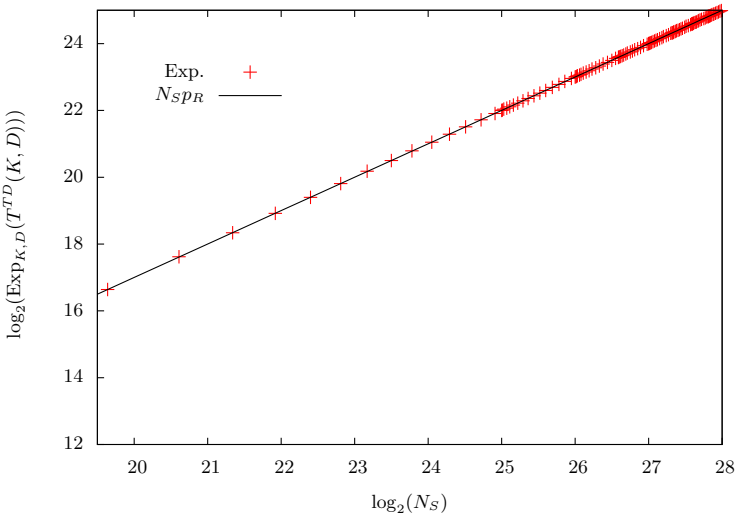


Fig. 9: Mean of T_R for a truncated differential with probability $p_R^* = 2^{-3} + 2^{-13.43}$. The size of a structure is 2^{13}, meaning that when $N_S < 2^{25}$ only one structure is used.

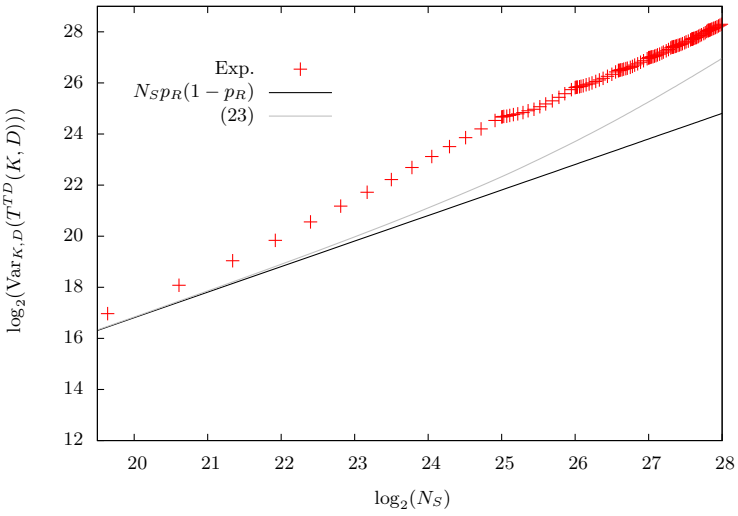


Fig. 10: Variance of T_R for a truncated differential with probability $p_R^* = 2^{-3} + 2^{-13.43}$. The size of a structure is 2^{13}, meaning that when $N_S < 2^{25}$ only one structure is used.

This analysis impacts the truncated differential on 26 rounds of PRESENT presented in [6] as well as the known-key distinguisher on the full PRESENT [7]. Indeed, in that papers, the authors assumed that $p_R^* \approx p_R$ which is not true when p_R is close to p_W. While the multidimensional linear attack of [15] makes use of 9 multidimensional approximations with total capacity $2^{-55.38}$ over 24 rounds, we provide the details for one of these multidimensional approximation of capacity close to $2^{-55.38}/9 = 2^{-58.54}$ (in [7] a capacity of $2^{-58.77}$ is taken into consideration). The dimension of this multidimensional approximation is 8 and we have $2^s = 2^q = 2^4$. In this case we have a truncated differential with probability $p_R^* = 2^{-q} + 2^{-q}C_R - 2^{n-s} = 2^{-4} + 2^{-62.54} - 2^{-60} < 2^{-4}$, making this distinguisher over 24 rounds of PRESENT impossible.

Corollary 10. *Given $\varepsilon = p_R^* - 2^{-q}$. From the expression of the mean and the variance for the right and wrong keys, we get the following estimate of success probability of a truncated differential attack involving $2^t - 1$ input differences and 2^{n-q} output differences.*

$$P_S \approx \Phi\left(\frac{\sqrt{N_S}\varepsilon - \sqrt{2^{-q}(1 + N_S 2^{1-n-t})}\varphi_a}{\sqrt{2^{-q} + \varepsilon + N_S 2^{1-q-n-t}(2^t\varepsilon + 1)^2}}\right).$$

The success probability of a last-rounds truncated differential attack using the previous distribution is plotted in Figure 11 and is comparable to Figure 8.

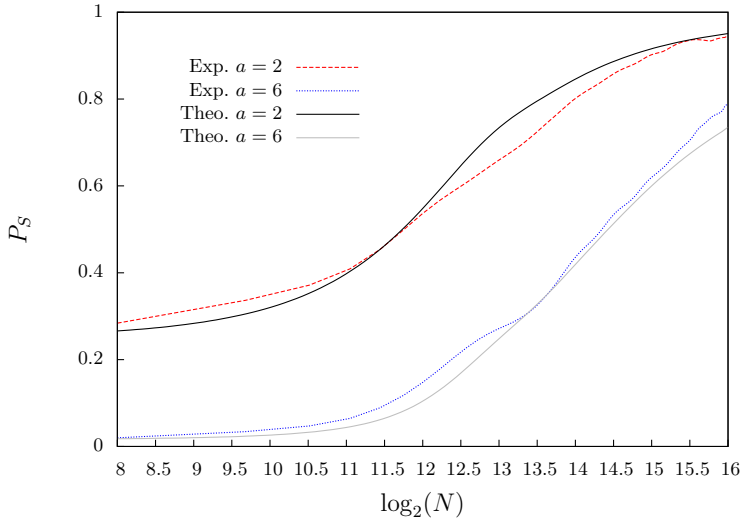


Fig. 11: Success probability of a TD attack on 6 rounds of SMALLPRESENT-[4]. The size of a structure is $2^t = 2^{13}$ meaning that when the data complexity $N < 2^{13}$, we have $N_S = N^2$.

Using the formula of the success probability, which takes into consideration the variance of the truncated differential probability for both the right and wrong keys, provided in Corollary 10 and the parameters of [7], adjusting $p_R^* = p_R - 2^{-60}$, we obtain a known-key distinguisher on 29 rounds of PRESENT with success probability 55% instead of a distinguisher on the full 31 rounds of PRESENT.

7 Conclusion

In this paper, we reconsider the theoretical model of statistical attacks on block ciphers. While a large part of the paper is dedicated to the presentation of the new statistical model for multiple and multidimensional linear attacks, we show that the same priciples can be used to obtain a tighter estimate of the data complexity of other statistical attacks.

The theoretical model based on the joint data and key distribution is not only of theoretical interest but can also be applied in practice to obtain new information about existing statistical attacks. Probably the most impactful contribution of the paper is the correction of the erroneous ad hoc estimate of the expected capacity for the wrong keys in the ordinary known-plaintext multidimensional linear attack. In particular we showed that correcting it from 0 to $2^{-n}\ell$ has fatal consequences on most of the existing multidimensional linear attacks. On the positive side, thanks to the corrected wrong-key model, we can now run the multidimensional zero-correlation attack also for non-distinct plaintext, which was previously known only for zero-correlation attacks using multiple independent linear approximations.

Another positive result we achieve from the new model is that the ad hoc parameters used for the wrong-key distribution in the distinct-known-plaintext multidimensional zero-correlation attacks are correct.

We also looked at the distinct-known plaintext sampling model in the ordinary multidimensional linear context and illustrated that in some cases this way of sampling might significantly reduce the data complexity. On the other hand, we observed in the experiments that if we increase the size of the data sample beyond the size of the full codebook in the classical known-plaintext context we can achieve the same advantage and success probability as when using the full codebook in the distinct-known-plaintext context.

Taking into consideration the key-variance of the capacity for both the right and wrong keys we improve the accuracy of the data complexity estimate of the multiple/multidimensional linear attack. While in this paper we present approaches to compute estimates of the key-variance of the capacity of the distribution obtained from the cipher data using the right key, we observed in the expriments that they are still not tight. We believe such estimates and methods for achieving them depend strongly on the cipher and leave them for future investigation. Also the actual form of the joint data and key distribution of the test statistic is left open in this paper. We provided the mean and the (esti-

mate of the) variance, which allow to compute the data complexity under the assumption that the normal approximation of the distribution is valid.

References

1. Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. In Douglas R. Stinson and Stafford E. Tavares, editors, *SAC 2000*, volume 2012 of *LNCS*. Springer, 2001.
2. Asli Bay, Jialin Huang, and Serge Vaudenay. Improved linear cryptanalysis of reduced-round MIBS. In Maki Yoshida and Koichi Mouri, editors, *Advances in Information and Computer Security - 9th International Workshop on Security, IWSEC 2014, Hirosaki, Japan, August 27-29, 2014. Proceedings*, volume 8639 of *Lecture Notes in Computer Science*, pages 204–220. Springer, 2014.
3. Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. In *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1991.
4. Alex Biryukov, Christophe De Cannière, and Michaël Quisquater. On Multiple Linear Approximations. In *CRYPTO 2004*, pages 1–22, 2004.
5. Céline Blondeau, Gregor Leander, and Kaisa Nyberg. Differential-linear cryptanalysis revisited. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 411–430. Springer, 2014.
6. Céline Blondeau and Kaisa Nyberg. Links Between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities. In Elisabeth Oswald and Phong Q. Nguyen, editors, *Eurocrypt 2014*, volume 8441 of *LNCS*. Springer-Verlag, 2014.
7. Céline Blondeau, Thomas Peyrin, and Lei Wang. Known-key distinguisher on full PRESENT. 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 455–474. Springer, 2015.
8. Andrey Bogdanov, Christina Boura, Vincent Rijmen, Meiqin Wang, Long Wen, and Jingyuan Zhao. Key Difference Invariant Bias in Block Ciphers. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013*, volume 8269 of *LNCS*, pages 357–376. Springer, 2013.
9. Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen, and Baudoin Collard. Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA. In *SAC'13*, LNCS. Springer, 2014.
10. 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 *LNCS*, pages 450–466. Springer, 2007.
11. 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 *LNCS*, pages 244–261. Springer, 2012.

12. 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.
13. Andrey Bogdanov and Meiqin Wang. Zero Correlation Linear Cryptanalysis with Reduced Data Complexity. In Anne Canteaut, editor, *FSE*, volume 7549 of *LNCS*, pages 29–48. Springer, 2012.
14. Christina Boura, María Naya-Plasencia, and Valentin Suder. Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014*, volume 8873 of *LNCS*, pages 179–199. Springer, 2014.
15. Joo Yeon Cho. Linear Cryptanalysis of Reduced-Round PRESENT. In Josef Pieprzyk, editor, *CT-RSA*, volume 5985 of *LNCS*, pages 302–317. Springer, 2010.
16. Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *IACR Cryptology ePrint Archive*, 2005:212, 2006.
17. Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *J. Mathematical Cryptology*, 1(3):221–242, 2007.
18. Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Multidimensional Extension of Matsui's Algorithm 2. In *FSE*, volume 5665 of *LNCS*, pages 209–227. Springer, 2009.
19. 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.
20. Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 196–211. Springer, 1994.
21. Gregor Leander. Small scale variants of the block cipher PRESENT. *IACR Cryptology ePrint Archive*, 2010:143, 2010.
22. Gregor Leander. On Linear Hulls, Statistical Saturation Attacks, PRESENT and a Cryptanalysis of PUFFIN. In K. G. Paterson, editor, *EUROCRYPT*, volume 6632 of *LNCS*, pages 303–322. Springer, 2011.
23. Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In Tor Helleseth, editor, *EUROCRYPT*, volume 765 of *LNCS*, pages 386–397. Springer, 1993.
24. James McLaughlin and John A. Clark. Filtered nonlinear cryptanalysis of reduced-round serpent, and the wrong-key randomization hypothesis. In *Cryptography and Coding - 14th IMA International Conference, IMACC 2013, Oxford, UK, December 17-19, 2013. Proceedings*, volume 8308 of *Lecture Notes in Computer Science*, pages 120–140. Springer, 2013.
25. Phuong Ha Nguyen, Hongjun Wu, and Huaxiong Wang. Improving the Algorithm 2 in multidimensional linear cryptanalysis. In Udaya Parampalli and Philip Hawkes, editors, *Information Security and Privacy - 16th Australasian Conference, ACISP 2011, Melbourne, Australia, July 11-13, 2011. Proceedings*, volume 6812 of *Lecture Notes in Computer Science*, pages 61–74. Springer, 2011.
26. Kaisa Nyberg. Linear cryptanalysis. *SAC Summer School, Sackville, New Brunswick*, 2015.

27. 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.
28. Ali Aydin Selçuk. On Probability of Success in Linear and Differential Cryptanalysis. *J. Cryptology*, 21(1):131–147, 2008.
29. Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-Bit Block cipher CLEFIA (Extended Abstract). In Alex Biryukov, editor, *FSE*, volume 4593 of *LNCS*, pages 181–195. Springer, 2007.
30. Hadi Soleimany and Kaisa Nyberg. Zero-correlation linear cryptanalysis of reduced-round LBlock. *Des. Codes Cryptography*, 73(2):683–698, 2014.
31. Long Wen, Meiqin Wang, Andrey Bogdanov, and Huaifeng Chen. General Application of FFT in Cryptanalysis and Improved Attack on CAST-256. In Willi Meier and Debdeep Mukhopadhyay, editors, *INDOCRYPT 2014*, volume 8885 of *LNCS*, pages 161–176. Springer, 2014.
32. Long Wen, Meiqin Wang, and Jingyuan Zhao. Related-Key Impossible Differential Attack on Reduced-Round LBlock. *J. Comput. Sci. Technol.*, 29(1):165–176, 2014.
33. Wenling Wu and Lei Zhang. LBlock: A Lightweight Block Cipher. In Javier Lopez and Gene Tsudik, editors, *ACNS*, volume 6715 of *LNCS*, pages 327–344, 2011.
34. Lei Zheng and Shao-wu Zhang. FFT-based multidimensional linear attack on PRESENT using the 2-bit-fixed characteristic. *Security and Communication Networks*, 2015. online publication.