Protecting against Multidimensional Linear and Truncated Differential Cryptanalysis by Decorrelation

Céline Blondeau[1], Aslı Bay, and Serge Vaudenay[2]

[1] Department of Computer Science, School of Science, Aalto University, Finland
[2] EPFL, Lausanne, Switzerland

Abstract. The decorrelation theory provides a different point of view on the security of block cipher primitives. Results on some statistical attacks obtained in this context can support or provide new insight on the security of symmetric cryptographic primitives. In this paper, we study, for the first time, the multidimensional linear attacks as well as the truncated differential attacks in this context. We show that the cipher should be decorrelated of order two to be resistant against some multidimensional linear and truncated differential attacks. Previous results obtained with this theory for linear, differential, differential-linear and boomerang attacks are also resumed and improved in this paper.
Keywords: decorrelation theory, multidimensional linear cryptanalysis, truncated differential cryptanalysis.

1 Introduction

In the last 25 years many statistical attacks have been proposed and implemented on different symmetric key cryptographic primitives. Nowadays, new symmetric primitives are not considered secure until evaluation by the community. But it is often difficult to evaluate the security of a cipher due to the large number of known attacks.

In 1998, Vaudenay [18,21] introduced the decorrelation theory to prevent this long and tedious security evaluation. When a cipher is designed and proved secure up to a certain degree of decorrelation, it is secure against a wide range of statistical attacks. Among statistical attacks, differential cryptanalysis [8], linear cryptanalysis [17] and their generalizations have been prominent. For instance, we know that a cipher decorrelated of order two is resistant to the classical differential and linear cryptanalysis. Recently [7], it has been shown that the primitives should be decorrelated of order four to be protected against differential-linear [13,3] and boomerang [22] attacks.

Understanding the similitude of the different statistical attacks is of great importance to simplify the security analysis of the symmetric cryptographic primitives. While different works in that direction have been presented in the last couple of years [16,4,9,10], part of this unification can also be obtained by determining the order of decorrelation of the new presented attacks. However, the question of measuring the advantage of taking the information from

different differentials or linear approximations has not yet been studied in the context of decorrelation theory. In this paper, we study the decorrelation order of the multidimensional linear and truncated differential attacks. In particular, we show that a cipher is protected against multidimensional linear attacks if it is decorrelated of order two. Some elements of the proof are related to the link between multidimensional linear attacks and truncated differential attacks which was discovered by Blondeau and Nyberg [9,10]. Using the result obtained for a special truncated differential distinguisher, we have been able to determine that the truncated differential attacks involving a large number of input differences are also decorrelated of order two. Using the decorrelation theory, in this paper, we provide for the first time an intuition on the power of truncated differential and multidimensional linear attacks as a function of the number of involved differential or linear approximations used in the attack.

Outline. In Sect. 2, we recall some basic definitions and previous works in the context of the decorrelation theory. In Sect. 3 we study the multidimensional linear attack in this context. In Sect. 4, we study the decorrelation order of the truncated differential attack. In Sect. 5, we provide some improvement of the previous results for the well known differential, linear, differential-linear and boomerang attacks. Sect. 6 concludes this paper.

2 Preliminaries

2.1 Statistical Attacks

We recall in this section some basic definitions related to the statistical attacks studied in this paper.

Linear cryptanalysis [17] uses a linear relation between bits from plaintexts, corresponding ciphertexts, and the encryption key. Given a permutation Enc over $\{0,1\}^\ell$, the strength of the linear relation is measured by its correlation. The *correlation* of a function $\mathsf{Enc} : \mathbb{F}_2^\ell \to \mathbb{F}_2^\ell$ at point $(\alpha, \beta) \in \mathbb{F}_2^\ell \times \mathbb{F}_2^\ell$ is defined as

$$\mathsf{cor}(\alpha,\beta) = 2^{-\ell}\Big[\#\left\{x \in \mathbb{F}_2^\ell | \alpha \cdot x \oplus \beta \cdot \mathsf{Enc}(x) = 0\right\} - \#\left\{x \in \mathbb{F}_2^\ell | \alpha \cdot x \oplus \beta \cdot \mathsf{Enc}(x) = 1\right\}\Big],$$

where the quantity within brackets can be computed as the Walsh transform of $\alpha \cdot x \oplus \beta \cdot \mathsf{Enc}(x)$ evaluated at zero.

Through this paper, the square correlation at point $v = (\alpha, \beta) \in \mathbb{F}_2^{2\ell}$ will be denoted by $\mathsf{LP}^{\mathsf{Enc}}(v)$ and corresponds to $\mathsf{LP}^{\mathsf{Enc}}(v) = \mathsf{cor}^2(\alpha, \beta)$.

For the generalizations of linear cryptanalysis, such as multidimensional linear cryptanalysis [14], a quantity C, called *capacity*, is used for evaluating the non-uniformity of the set of linear approximations.

The capacity corresponds to the sum of the square correlations of the involved linear approximations. We let $V \subset \mathbb{F}_2^{2\ell}$ be the vector space spanned by different

(α_j, β_j) masks. In the context of multidimensional linear attacks, we define the capacity

$$\mathsf{cap}_{\mathsf{Enc}}(V) = \sum_{v \in V, v \neq 0} \mathsf{LP}^{\mathsf{Enc}}(v).$$

In the following of this paper, we denote by k the dimension of V.

In differential cryptanalysis [8], the attacker is interested in finding and exploiting non-uniformity in occurrences of plaintext and ciphertext differences. Given the differences $\Delta \in \mathbb{F}_2^\ell$ and $\Gamma \in \mathbb{F}_2^\ell$, the probability $\mathsf{DP}^{\mathsf{Enc}}(\Delta, \Gamma)$ of the differential (Δ, Γ) is defined as

$$\mathsf{DP}^{\mathsf{Enc}}(\Delta, \Gamma) = 2^{-\ell} \#\{x \in \mathbb{F}_2^\ell \,|\, \mathsf{Enc}(x) \oplus \mathsf{Enc}(x \oplus \Delta) = \Gamma\}.$$

The power of the generalization of differential cryptanalysis involving multiple differentials is measured by a sum or average of these probabilities. For the truncated differential attacks [15] with differences (Δ, Γ) in the vector space $V^\perp \subset \mathbb{F}_2^{2\ell}$ we define

$$P_{\mathsf{Enc}}^{\mathsf{STD}}(V^\perp) = 2^{-2\ell} \#\{(x, x') \in \mathbb{F}_2^\ell \times \mathbb{F}_2^\ell \,|\, (x \oplus x', \mathsf{Enc}(x) \oplus \mathsf{Enc}(x')) \in V^\perp\}.$$

We can show that,

$$P_{\mathsf{Enc}}^{\mathsf{STD}}(V^\perp) = 2^{-\ell} \sum_{(\Delta, \Gamma) \in V^\perp} \mathsf{DP}^{\mathsf{Enc}}(\Delta, \Gamma).$$

Derived from the general link between differential probability and linear correlations [12], the authors of [10,11] show a general link between multidimensional linear attacks and truncated differential attacks. To derive in Sect. 3 the decorrelation order of a multidimensional linear attack, we will use this link. Using our notations, Th. 1 of [11] corresponds to the following one.

Theorem 1. *Let $V^\perp$ be the set of all u such that $u \cdot v = 0$ for all $v \in V$. Using the previous notation, we obtain the following relation between $P_{\mathsf{Enc}}^{\mathsf{STD}}(V^\perp)$ and $\mathsf{cap}_{\mathsf{Enc}}(V)$:*

$$2^{-k} \mathsf{cap}_{\mathsf{Enc}}(V) = p_{\mathsf{Enc}}^{\mathsf{STD}}(V^\perp) - 2^{-k}.$$

Proof. We provide the proof with our settings. We have

$$\begin{aligned} 1 + \mathsf{cap}_{\mathsf{Enc}}(V) &= \sum_{v \in V} \mathsf{LP}^{\mathsf{Enc}}(v) \\ &= \sum_{v \in V} 2^{-\ell} \sum_{u} (-1)^{u \cdot v} \mathsf{DP}^{\mathsf{Enc}}(u) \\ &= 2^{-\ell} \sum_{u} \mathsf{DP}^{\mathsf{Enc}}(u) \sum_{v \in V} (-1)^{u \cdot v}. \end{aligned}$$

Since $v \mapsto u \cdot v$ is a group homomorphism from V to $\mathbf{Z}_2$, either it is balanced, or identically equal to 0 (when $u \in V^\perp$, by definition). We have

$$1 + \mathsf{cap}_{\mathsf{Enc}}(V) = 2^{k-\ell} \sum_{u \in V^\perp} \mathsf{DP}^{\mathsf{Enc}}(u).$$

So, $p^{\mathsf{STD}}_{\mathsf{Enc}}(V^\perp) = 2^{-k} + 2^{-k}\mathsf{cap}_{\mathsf{Enc}}(V)$. □

Splitting the space $V^\perp$ of involved differentials to the spaces $V^\perp_{\mathsf{in}}$ and $V^\perp_{\mathsf{out}}$ of input and output differences, we can define the truncated differential probability $P^{\mathsf{TD}}_{\mathsf{Enc}}$ as follows

$$P^{\mathsf{TD}}_{\mathsf{Enc}}(V^\perp) = 2^{-\ell} \frac{1}{|V^\perp_{\mathsf{in}}|} \sum_{\Delta \in V^\perp_{\mathsf{in}}} \#\{x \in \mathbb{F}_2^\ell \,|\, \mathsf{Enc}(x) \oplus \mathsf{Enc}(x \oplus \Delta) \in V^\perp_{\mathsf{out}}\}.$$

Differential-Linear Cryptanalysis. Differential and linear attacks were used together for the first time by Langford and Hellman [13]. This was *differential-linear cryptanalysis*. The basic idea is to split the cipher under consideration into a composition of two parts. The split should be such that, for the first part of the cipher there should exist a strong truncated differential with input difference Δ and for the second part there should exist a strongly biased linear approximation with output mask β. In [13], the particular case where the differential over the first part holds with probability one has been introduced. Later on, Biham et al. [3] generalized this attack using a probabilistic truncated differential on the first rounds of the distinguisher. In [11], Blondeau et al presented a general model for this attack.

$$p^{\mathsf{DL}}_{\mathsf{Enc}}(\Delta, \beta) = 2^{-\ell} \#\left\{x \mid \beta \cdot (\mathsf{Enc}(x) \oplus \mathsf{Enc}(x \oplus \Delta)) = 0\right\}.$$

Boomerang Attack. In the boomerang attack, introduced in 1999 by Wagner [22], the advantage is taken from both the encryption and decryption. Given a difference Δ between two plaintexts x and x', the attacker is taking advantage of the probability

$$p^{\mathsf{Boo}}_{\mathsf{Enc}}(\Delta, \nabla) = 2^{-\ell} \# \left\{x \mid \mathsf{Enc}^{-1}\left(\mathsf{Enc}(x) \oplus \nabla\right) \oplus \mathsf{Enc}^{-1}\left(\mathsf{Enc}(x \oplus \Delta) \oplus \nabla\right) = \Delta\right\},$$

where ∇ is a ciphertext difference.

2.2 The Decorrelation Theory

We consider a permutation Enc over $\{0,1\}^\ell$. Sometimes, Enc will be a random permutation with uniform distribution and will be denoted by C^*. Sometimes, it will be a permutation defined by a random key K and will be denoted by C_K.

Decorrelation was first presented in [18]. The non-adaptive (resp. adaptive) decorrelation of C_K of order d is denoted by $\|[C_K]^d - [C^*]^d\|_\infty$ (resp. $\|[C_K]^d - [C^*]^d\|_a$). It is the $\|\cdot\|_\infty$- (resp. $\|\cdot\|_a$-) distance between the matrices $[C_K]^d$ and $[C^*]^d$. Given a random Enc, we define $[\mathsf{Enc}]^d$, the d-wise distribution matrix by

$$[\mathsf{Enc}]^d_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)} = \Pr[y_1 = \mathsf{Enc}(x_1), \ldots, y_d = \mathsf{Enc}(x_d)].$$

The $\|\cdot\|_\infty$-norm is defined by

$$\|M\|_\infty = \max_{x_1,\ldots,x_d} \sum_{y_1,\ldots,y_d} |M_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)}|.$$

A random variable can be considered as a random function from a set of cardinality 1, so its d-wise distribution matrix is a row vector and the $\|\cdot\|_\infty$ matrix-norm corresponds to the $\|\cdot\|_1$ vector-norm. For distributions, the $\|\cdot\|_1$-distance is also called the *statistical distance*. The $\|\cdot\|_a$-norm was defined in [20] by

$$\|M\|_a = \max_{x_1} \sum_{y_1} \cdots \max_{x_d} \sum_{y_d} |M_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)}|.$$

Here is the fundamental link between the best advantage of a distinguisher and decorrelation.

Theorem 2 (Best advantage and decorrelation, Th. 10–11 of [21]). *The $\|\cdot\|_\infty$-decorrelation of order d of C_K, $\|[C_K]^d - [C^*]^d\|_\infty$, is twice the best advantage of a non-adaptive unbounded distinguisher between C_K and C^* which is allowed to make d encryption queries.*

The $\|\cdot\|_a$-decorrelation of order d of C_K, $\|[C_K]^d - [C^*]^d\|_a$, is twice the best advantage of an adaptive unbounded distinguisher between C_K and C^* which is allowed to make d encryption queries.

We say C_K is *decorrelated* if its decorrelation is small. We have *perfect decorrelation* when the decorrelation is 0. I.e., $[C_K]^d = [C^*]^d$, meaning

$$\Pr[y_1 = C_K(x_1), \ldots, y_d = C_K(x_d)] = \Pr[y_1 = C^*(x_1), \ldots, y_d = C^*(x_d)]$$

for all $x_1, \ldots, x_d, y_1, \ldots, y_d$.

For instance, decorrelation of order $d = 2$ corresponds to that $\Pr[y_1 = C_K(x_1), y_2 = C_K(x_2)]$ is always close to $\frac{1}{2^\ell(2^\ell-1)}$ for $x_1 \neq x_2$ and $y_1 \neq y_2$. This is the notion of *pairwise independence* by Wegman and Carter [23].

Given a permutation Enc over $\{0,1\}^\ell$, we define Q_{Enc}, a function from $\{0,1\} \times \{0,1\}^\ell$ to $\{0,1\}^\ell$ by

$$Q_{\mathsf{Enc}}(0,x) = \mathsf{Enc}(x) \quad \text{and} \quad Q_{\mathsf{Enc}}(1,y) = \mathsf{Enc}^{-1}(y).$$

To study distinguishers which can make encryption and decryption queries, we just consider the decorrelation of Q_{Enc} instead of the decorrelation of Enc. For this, we study the distance between $[Q_{C_K}]^d$ and $[Q_{C^*}]^d$.

We review some general security results below.

Non-adaptive iterated distinguisher of order d. Given an encryption function Enc, a *non-adaptive iterated distinguisher of order d* (Distinguisher Iter) is characterized by a distribution D and two Boolean functions T and f. With n iterations, it works as follows:

Distinguisher Iter:
1: **for** $i = 1$ to n **do**
2: pick $(x_1, \ldots, x_d) \in (\{0,1\}^\ell)^d$ following distribution D
3: set $y_j = \mathsf{Enc}(x_j)$ for $j = 1, \ldots, d$
4: set $b_i = T(x_1, \ldots, x_d, y_1, \ldots, y_d)$
5: **end for**
6: output $f(b_1, \ldots, b_n)$

For such distinguisher, the following results have been derived in [19].

Theorem 3 (Advantage of Iter bounded by decorrelation [19], Th. 18 of [21]). *For the Boolean function T, we have*

$$E(p^{\mathsf{Iter}}_{C_K}) - E(p^{\mathsf{Iter}}_{C^*}) \leq 5 \sqrt[3]{n^2 \left(2\delta + \frac{5d^2}{2 \times 2^\ell} + \frac{3}{2}\|[C_K]^{2d} - [C^*]^{2d}\|_\infty\right)} + n\|[C_K]^{2d} - [C^*]^{2d}\|_\infty$$

where δ is an upper bound on the probability that the distinguisher picks a plaintext in common between any two iterations. I.e., $\delta = \Pr[\exists i, j \quad x_i = x'_j : (x_1, \ldots, x_d) \leftarrow D, (x'_1, \ldots, x'_d) \leftarrow D]$.

Note that it was proven in [6,7] that we cannot have a general security result when δ is high or when we only have a decorrelation of order $2d - 1$.

Th. 3 was generalized in [19] to the case where the range of T has s elements instead of 2:

Theorem 4 (Advantage of Iter bounded by decorrelation, Th. 7 of [19]). *If T maps onto a set of s elements, we have*

$$E(p^{\mathsf{Iter}}_{C_K}) - E(p^{\mathsf{Iter}}_{C^*}) \leq 3s \sqrt[3]{n^2 \left(2\delta + \frac{2d^2}{2^\ell} + \frac{d^3}{2^\ell(2^\ell - d)} + \frac{3}{2}\|[C_K]^{2d} - [C^*]^{2d}\|_\infty\right)} + \frac{ns}{2}\|[C_K]^{2d} - [C^*]^{2d}\|_\infty$$

where δ is an upper bound on the probability that the distinguisher picks a plaintext in common between any two iterations. I.e., $\delta = \Pr[\exists i, j \quad x_i = x'_j : (x_1, \ldots, x_d) \leftarrow D, (x'_1, \ldots, x'_d) \leftarrow D]$.

Adaptive iterated distinguisher of order d. Th. 3 was generalized in [5,7] to adaptive plaintext-ciphertext iterated distinguishers (i.e., distinguishers which make in each iteration some adaptive queries and can also make chosen ciphertext queries): Given an encryption function Enc, an *adaptive plaintext-ciphertext iterated distinguisher of order d* (Distinguisher AIter) is characterized by $d - 1$ functions $q_1, \ldots, q_{d-1}$, and two Boolean functions T and f. With n iterations, it works as follows:

Distinguisher AIter:
1: **for** $i = 1$ to n **do**
2: pick a uniformly distributed sequence ρ of random coins
3: **for** $j = 1$ to d **do**
4: set $z_j = q_j(Q_{\mathsf{Enc}}(z_1), \ldots, Q_{\mathsf{Enc}}(z_{j-1}); \rho)$
5: **end for**
6: set $b_i = T(Q_{\mathsf{Enc}}(z_1), \ldots, Q_{\mathsf{Enc}}(z_d); \rho)$
7: **end for**
8: output $f(b_1, \ldots, b_n)$

Theorem 5 (Advantage of AIter bounded by decorrelation [5], Th. 5 of [7]). *We have*

$$E(p_{C_K}^{\mathsf{AIter}}) - E(p_{C^*}^{\mathsf{AIter}}) \leq 5\sqrt[3]{n^2\left(2\delta + e^{8d^2 2^{-\ell}} + \frac{2d^2}{2^\ell} + \frac{3}{2}\|[Q_{C_K}]^{2d} - [Q_{C^*}]^{2d}\|_\infty\right)} + n\|[Q_{C_K}]^{2d} - [Q_{C^*}]^{2d}\|_\infty$$

where δ is an upper bound on the probability that the distinguisher picks a query in common between any two iterations.

In what follows we give tighter results for specific classes of iterated attacks for which we can get rid of δ and sometimes rely on a lower decorrelation order.

2.3 Previous Results in the Context of Decorrelation Theory

To obtain the decorrelation order as well as the order of the different statistical attacks we have to describe the distinguishers we are working with. In this section, we describe the differential, linear, differential-linear and boomerang attacks, and recall the different results obtained for these distinguishers. A comparison with the results obtained for the multidimensional linear and truncated differential attacks will be presented later in this paper.

Differential Cryptanalysis. Given an encryption function Enc, a *differential distinguisher* (Distinguisher DC) is characterized by two differences Δ and Γ and a Boolean function f. With n iterations, it works as follows:

Distinguisher DC:
1: **for** $i = 1$ to n **do**
2: pick $x \in \{0,1\}^\ell$ uniformly
3: set $x' = x \oplus \Delta$
4: set $y = \mathsf{Enc}(x)$ and $y' = \mathsf{Enc}(x')$
5: set $b_i = 1_{y \oplus y' = \Gamma}$
6: **end for**
7: output $f(b_1, \ldots, b_n)$

This is a non-adaptive iterated attack of order 2.

Theorem 6 (Advantage of DC bounded by decorrelation, Th. 13 of [21]). *For the function $f(b_1, \ldots, b_n) = \max_i b_i$, we have*

$$E(p^{\mathsf{DC}}_{C_K}) - E(p^{\mathsf{DC}}_{C^*}) \leq \frac{n}{2^\ell - 1} + \frac{n}{2}\|[C_K]^2 - [C^*]^2\|_\infty.$$

Linear Cryptanalysis. Given an encryption function Enc, a *linear distinguisher* (Distinguisher LC) is characterized by two masks α and β, and a Boolean function f. With n iterations, it works as follows:

Distinguisher LC:
1: **for** $i = 1$ to n **do**
2: pick $x \in \{0,1\}^\ell$ uniformly
3: set $y = \mathsf{Enc}(x)$
4: set $b_i = \alpha \cdot x \oplus \beta \cdot y$
5: **end for**
6: output $f(b_1, \ldots, b_n)$

This is a non-adaptive iterated attack of order 1.

Theorem 7 (Advantage of LC bounded by decorrelation, Th. 17 of [21]). *We have*

$$E(p^{\mathsf{LC}}_{C_K}) - E(p^{\mathsf{LC}}_{C^*}) \leq 3\sqrt[3]{n\|[C_K]^2 - [C^*]^2\|_\infty + \frac{n}{2^\ell - 1}} + 3\sqrt[3]{\frac{n}{2^\ell - 1}}.$$

Differential-Linear Cryptanalysis. Given a function Enc, a *differential-linear distinguisher* is characterized by a difference Δ, a mask β, and a Boolean function f. With n iterations, it works as follows:

Distinguisher DL:
1: **for** $i = 1$ to n **do**
2: pick $x_1 \in \{0,1\}^\ell$ uniformly
3: set $x_2 = x_1 \oplus \Delta$
4: set $y_1 = \mathsf{Enc}(x_1)$ and $y_2 = \mathsf{Enc}(x_2)$
5: set $b_i = \beta \cdot (y_1 \oplus y_2)$
6: **end for**
7: output $f(b_1, \ldots, b_n)$

This is a non-adaptive iterated attack of order 2.

Theorem 8 (Advantage of DL bounded by decorrelation, Th. 7 of [7]). *We have*

$$E(p^{\mathsf{DL}}_{C_K}) - E(p^{\mathsf{DL}}_{C^*}) \leq 3\sqrt[3]{n\|[C_K]^4 - [C^*]^4\|_\infty + n\frac{2 \times 2^\ell - 5}{(2^\ell - 1)(2^\ell - 3)}} + 3\sqrt[3]{n\frac{2 \times 2^\ell - 5}{(2^\ell - 1)(2^\ell - 3)}}.$$

This results say that if a cipher is decorrelation to the order 4, it is protected against differential- linear cryptanalysis. It was further proven in [1, pp. 77–78] that some ciphers decorrelated to the order 3 can have a high advantage with DL. Which means that the decorrelation of order 4 is really what is needed.

Remark 9. The result from [7] was stated for a function f based on a counter $b_1 + \cdots + b_n$ but it is easy to see that the proof holds for a more general f as it is very similar to that of Th. 7.

Boomerang Cryptanalysis. Given an encryption function Enc, a *boomerang distinguisher* is characterized by two differences Δ and ∇ and a Boolean function f. With n iterations, it works as follows:

Distinguisher Boo:

1: **for** $i = 1$ to n **do**
2: pick $x_1 \in \{0,1\}^\ell$ uniformly
3: set $x_2 = x_1 \oplus \Delta$
4: set $y_1 = \mathsf{Enc}(x_1)$ and $y_2 = \mathsf{Enc}(x_2)$
5: set $y_3 = y_1 \oplus \nabla$ and $y_4 = y_2 \oplus \nabla$
6: set $x_3 = \mathsf{Enc}^{-1}(y_3)$ and $x_4 = \mathsf{Enc}^{-1}(y_4)$
7: set $b_i = 1_{x_3 \oplus x_4 = \Delta}$
8: **end for**
9: output $f(b_1, \ldots, b_n)$

This is an *adaptive plaintext-ciphertext* iterated attack of order 4.

Theorem 10 (Advantage of Boo bounded by decorrelation, Th. 8 of [7]). *For the function $f(b_1, \ldots, b_n) = \max_i b_i$, we have*

$$E(p^{\mathsf{Boo}}_{C_K}) - E(p^{\mathsf{Boo}}_{C^*}) \leq n\frac{2 \times 2^\ell - 5}{(2^\ell - 1)(2^\ell - 3)} + \frac{n}{2}\|[C_K]^4 - [C^*]^4\|_a.$$

It was further proven in [1, pp. 79–80] that some ciphers decorrelated to the order 3 can have a high advantage with Boo. We deduce that decorrelation of order 4 is really what is needed.

A summary of the results presented in this section (and new ones) is given in Table 1.

3 Multidimensional Linear Cryptanalysis

In this section we study the multidimensional linear (ML) attack. To do so we consider the following multidimensional linear distinguisher (Distinguisher ML):

Distinguisher ML:

for $i = 1$ to n **do**
  pick a random $x \in \{0,1\}^\ell$
  set $y = \mathsf{Enc}(x)$
  for $j = 1$ to k **do**
    set $b_{i,j} = (\alpha_j \cdot x) \oplus (\beta_j \cdot y)$
  end for
  set $b_i = (b_{i,1}, \ldots, b_{i,k})$
end for
output $f(b_1, \ldots, b_n)$

I.e., we look at the observed distribution of the bits $(b_{1,1}, \ldots, b_{n,k})$ and we take a decision by following a function f. According to this algorithm, this attack looks like a non-adaptive iterated attack of order 1, except that a vector b_i is kept instead of a bit at each iteration. We want to bound the advantage of this distinguisher for any function f. We let $p^{\mathsf{ML}}_{\mathsf{Enc}}$ be the probability (over the selection of the random x's) to output 1 by using the fixed function Enc. We want to bound

$$E(p^{\mathsf{ML}}_{C_K}) - E(p^{\mathsf{ML}}_{C^*})$$

where K is a random key, C_K is the encryption under the key K, and $E(p^{\mathsf{ML}}_{C_K})$ is the expected value over the distribution of K, and where C^* is a uniformly distributed random permutation and $E(p^{\mathsf{ML}}_{C^*})$ is the expected value over the distribution of C^*.

For Enc fixed, all vectors b_i are independent and identically distributed. We let D_{Enc} be the distribution of the vector b_i.

We let V be the vector space spanned by the (α_j, β_j) masks. We recall that k denotes the dimension of V.

We could apply Th. 4 with $d = 1$, $s = 2^k$, $\delta = 2^{-\ell}$, and obtain

$$E(p^{\mathsf{ML}}_{C_K}) - E(p^{\mathsf{ML}}_{C^*}) \leq 3 \times 2^k \sqrt[3]{n^2 \left(\frac{4}{2^\ell} + \frac{1}{2^\ell(2^\ell - 1)} + \frac{3}{2} \|[C_K]^2 - [C^*]^2\|_\infty \right)} + \frac{n 2^k}{2} \|[C_K]^2 - [C^*]^2\|_\infty.$$

With a negligible decorrelation, we would obtain a security for a data complexity n up to approximately $2^{\frac{\ell}{2} - 3k}$. Nevertheless, this is meaningless when the dimension k of V is such that $k > \frac{\ell}{6}$. With the technique to develop in this section, we aim at $n \approx 2^{\frac{\ell - k}{2}}$. This makes sense until k is close to ℓ.

We note that if $k > \ell$, there exists a Boolean function $\mathsf{bit}(y)$ on the ciphertext and a mapping from $b_i = (b_{i,1}, \ldots, b_{i,k})$ to $(x, \mathsf{bit}(y))$. For n relatively small, the vectors $(b_1, \ldots, b_n)$ uniquely identify the key K. So, there exists a function f (maybe with high complexity) leading to a very high advantage. Hence, we cannot prove any security without assuming any complexity on f.

For $k = \ell - \mathsf{cste}$, we could have cases in which there is a mapping from b_i to $(x_1, \ldots, x_{k-1}, \mathsf{bit}(y))$ so $2^{\mathsf{cste}+1}$ possible values for x. We can eliminate keys for

which none of these x lead to $\mathsf{bit}(y)$. This eliminates a fraction $2^{-2^{\mathsf{cste}+1}}$ of the keys. So, for n within the order of magnitude of $2^{2^{\mathsf{cste}+1}}$, we uniquely determine the key. So, no information-theoretic security is feasible for these values of n.

Remark 11 (Relation with [14] and [10,11]). In [14], the function f used to evaluate the multidimensional linear approximation is based on LLR or χ^2 statistical test. In [10,11], where the relation between the truncated differential and multidimensional linear key-recovery attacks is derived, the function f is based on the χ^2 test.

To provide a bound on $p^{\mathsf{ML}}_{\mathsf{Enc}} - p^{\mathsf{ML}}_{\mathsf{Enc}^*}$ we consider the following distinguisher, which is a special truncated differential (STD) distinguisher:

Distinguisher STD:
1: pick two plaintexts x and x' at random
2: set $y = \mathsf{Enc}(x)$ and $y' = \mathsf{Enc}(x')$
3: output $1_{(x'-x,\mathsf{Enc}(x')-\mathsf{Enc}(x))\in V^\perp}$

This distinguisher is a known plaintext truncated differential distinguisher using only one pair of samples. It corresponds to a non-adaptive attack using two queries.

Let $p^{\mathsf{STD}}_{\mathsf{Enc}}$ be the probability that the output is 1 with Enc fixed. Clearly, as given in Sect. 2.1, we have

$$p^{\mathsf{STD}}_{\mathsf{Enc}} = \sum_{(\Delta,\Gamma)\in V^\perp} 2^{-\ell}\mathsf{DP}^{\mathsf{Enc}}(\Delta,\Gamma).$$

Lemma 12 (Euclidean distance vs. capacity). *We let U be the uniform distribution. We have*

$$\|D_{\mathsf{Enc}} - U\|_2^2 = 2^{-k}\mathsf{cap}_{\mathsf{Enc}}(V).$$

Proof. If $v \in V$, we can write $v = \sum_j \lambda_j(\alpha_j, \beta_j)$. Then,

$$\begin{aligned}
\mathsf{LP}^{\mathsf{Enc}}(v) &= \left(E\left((-1)^{v\cdot(x,\mathsf{Enc}(x))}\right)\right)^2 \\
&= \left(E\left((-1)^{\sum_j \lambda_j(\alpha_j,\beta_j)\cdot(x,\mathsf{Enc}(x))}\right)\right)^2 \\
&= \left(E\left((-1)^{\sum_j \lambda_j b_j}\right)\right)^2 \\
&= E\left((-1)^{\sum_j \lambda_j (b_j+b'_j)}\right)
\end{aligned}$$

so,

$$\sum_{v\in V}\mathsf{LP}^{\mathsf{Enc}}(v) = 2^k \Pr[b_1 = b'_1, \ldots, b_k = b'_k] = 2^k \sum_{b_1,\ldots,b_k} \Pr[b_1,\ldots,b_k]^2$$

from which we deduce

$$\sum_{v\in V, v\neq 0} \mathsf{LP}^{\mathsf{Enc}}(v) = 2^k \|D_{\mathsf{Enc}} - U\|_2^2.$$

□

Lemma 13 (Statistical distance of iterated distribution). *Let n be an integer and D_β be a probability distribution for $\beta \in \{0,1\}$. Let $D_\beta^{\otimes n}$ be the distributions of vectors of n independent samples following D_β. We have*

$$\|D_0^{\otimes n} - D_1^{\otimes n}\|_1 \leq n\|D_0 - D_1\|_1.$$

Proof. We use

$$aa' - bb' = (a-b)\frac{a'+b'}{2} + (a'-b')\frac{a+b}{2}.$$

We have

$$\begin{aligned}
\|D_0^{\otimes n} - D_1^{\otimes n}\|_1 &= \frac{1}{2}\sum_{u,v} |D_0(u)D_0^{\otimes(n-1)}(v) - D_1(u)D_1^{\otimes(n-1)}(v)| \\
&\leq \frac{1}{2}\sum_u |D_0(u) - D_1(u)| \sum_v \frac{D_0^{\otimes(n-1)}(v) + D_1^{\otimes(n-1)}(v)}{2} + \\
&\quad \frac{1}{2}\sum_v |D_0^{\otimes(n-1)}(v) - D_1^{\otimes(n-1)}(v)| \sum_u \frac{D_0(u) + D_1(u)}{2} \\
&= \|D_0 - D_1\|_1 + \|D_0^{\otimes(n-1)} - D_1^{\otimes(n-1)}\|_1.
\end{aligned}$$

We conclude by proving the result by induction. □

Lemma 14 (Advantage of ML vs. Euclidean distance). *For any fixed* Enc *and* Enc^**, we have*

$$p^{\mathsf{ML}}_{\mathsf{Enc}} - p^{\mathsf{ML}}_{\mathsf{Enc}^*} \leq \frac{n2^{\frac{k}{2}}}{2}\|D_{\mathsf{Enc}} - D_{\mathsf{Enc}^*}\|_2.$$

Proof. Thanks to Th. 2, we have $p^{\mathsf{ML}}_{\mathsf{Enc}} - p^{\mathsf{ML}}_{\mathsf{Enc}^*} \leq \frac{1}{2}\|D^{\otimes n}_{\mathsf{Enc}} - D^{\otimes n}_{\mathsf{Enc}^*}\|_1$. Then, we have $\|D^{\otimes n}_{\mathsf{Enc}} - D^{\otimes n}_{\mathsf{Enc}^*}\|_1 \leq n\|D_{\mathsf{Enc}} - D_{\mathsf{Enc}^*}\|_1$ due to Lemma 13. Next, we use $\|D_{\mathsf{Enc}} - D_{\mathsf{Enc}^*}\|_1 \leq 2^{\frac{k}{2}}\|D_{\mathsf{Enc}} - D_{\mathsf{Enc}^*}\|_2$ due to the Cauchy-Schwarz Inequality. □

Remark 15. For $k = 1$ (linear cryptanalysis), we have $\mathsf{cap}_{\mathsf{Enc}}(V) = \mathsf{LP}^{\mathsf{Enc}}(\alpha_1, \beta_1)$. From Lemma 12 and Lemma 14, we obtain

$$|p^{\mathsf{ML}}_{\mathsf{Enc}} - p^{\mathsf{ML}}_{\mathsf{Enc}^*}| \leq \frac{n}{2}\sqrt{\mathsf{LP}^{\mathsf{Enc}}(\alpha_1,\beta_1)} + \frac{n}{2}\sqrt{\mathsf{LP}^{\mathsf{Enc}^*}(\alpha_1,\beta_1)}$$

for any fixed Enc and Enc^*. From [21, Lemma 15], we know that there is a constant p_0 such that for any fixed Enc, we have $|p^{\mathsf{ML}}_{\mathsf{Enc}} - p_0| \leq 2\sqrt{n\mathsf{LP}^{\mathsf{Enc}}(\alpha_1, \beta_1)}$. So,

$$|p^{\mathsf{ML}}_{\mathsf{Enc}} - p^{\mathsf{ML}}_{\mathsf{Enc}^*}| \leq 2\sqrt{n\mathsf{LP}^{\mathsf{Enc}}(\alpha_1, \beta_1)} + 2\sqrt{n\mathsf{LP}^{\mathsf{Enc}^*}(\alpha_1, \beta_1)}.$$

As we can see, the bound obtained from Lemma 14 is not tight in the case where $k = 1$. We are loosing a factor $\sqrt{n}$. The loss comes from Lemma 13 which is far from being tight.

Lemma 16 (Link between ML and STD). *For any fixed* Enc *and* Enc^**, we have*

$$p^{\mathsf{ML}}_{\mathsf{Enc}} - p^{\mathsf{ML}}_{\mathsf{Enc}^*} \leq \frac{n2^{\frac{k}{2}}}{2}\sqrt{p^{\mathsf{STD}}_{\mathsf{Enc}} - 2^{-k}} + \frac{n2^{\frac{k}{2}}}{2}\sqrt{p^{\mathsf{STD}}_{\mathsf{Enc}^*} - 2^{-k}}.$$

Proof. We apply Th. 1, Lemma 12, Lemma 14, and the triangular inequality $\|D_{\mathsf{Enc}} - D_{\mathsf{Enc}^*}\|_2 \leq \|D_{\mathsf{Enc}} - U\|_2 + \|D_{\mathsf{Enc}^*} - U\|_2$. □

Lemma 17 (Using decorrelation in STD). *We have*

$$E(p^{\mathsf{STD}}_{C_K}) \leq E(p^{\mathsf{STD}}_{C^*}) + \frac{1}{2}\|[C_K]^2 - [C^*]^2\|_\infty.$$

Proof. $E(p^{\mathsf{STD}}_{C_K}) - E(p^{\mathsf{STD}}_{C^*})$ expresses as the advantage of STD, a non-adaptive distinguisher limited to two queries. We conclude by using Th. 2. □

Lemma 18 (The ideal case in STD). *We have*

$$E(p^{\mathsf{STD}}_{C^*} - 2^{-k}) \leq 2^{-\ell}\frac{1 - 2^{-k}}{1 - 2^{-\ell}}.$$

Assuming that all α_j *are linearly independent and that all* β_j *are linearly independent, we further have*

$$E(p^{\mathsf{STD}}_{C^*} - 2^{-k}) = 2^{-\ell}\frac{1 - 2^{-k}}{1 - 2^{-\ell}}.$$

Proof. From Th. 1, we have

$$p^{\mathsf{STD}}_{\mathsf{Enc}} = 2^{-k} + 2^{-k}\sum_{v \in V, v \neq 0} \mathsf{LP}^{\mathsf{Enc}}(v).$$

There are exactly $2^k - 1$ vectors v which are non-zero. When all α_j resp. all β_j are linearly independent, neither the left half nor the right half of v is zero. Based on [21, Lemma 14], we deduce $E(\mathsf{LP}^{C^*}(v)) = \frac{1}{2^\ell - 1}$ and obtain

$$E(p^{\mathsf{STD}}_{C^*}) = 2^{-k} + 2^{-k}\frac{2^k - 1}{2^\ell - 1}.$$

Without the assumption of independence, there are some of the vectors $v \neq 0$ such that either the left half or the right half is zero but not both. Therefore, we have $\mathsf{LP}^{C^*}(v) = 0$. Since this satisfies $E(\mathsf{LP}^{C^*}(v)) \leq \frac{1}{2^\ell - 1}$, we still have

$$E(p^{\mathsf{STD}}_{C^*}) \leq 2^{-k} + 2^{-k}\frac{2^k - 1}{2^\ell - 1}.$$

□

Theorem 19 (Advantage of ML bounded by decorrelation). *We have*

$$E(p^{\mathsf{ML}}_{C_K}) - E(p^{\mathsf{ML}}_{C^*}) \leq n\sqrt{2^{k-\ell} + 2^{k-1}\|[C_K]^2 - [C^*]^2\|_\infty}.$$

Proof. We first apply Lemma 16. Then, since $\sqrt{\cdot}$ is concave, the Jensen inequality says that

$$E\left(\sqrt{p^{\mathsf{STD}}_{\mathsf{Enc}} - 2^{-k}}\right) \leq \sqrt{E(p^{\mathsf{STD}}_{\mathsf{Enc}} - 2^{-k})}.$$

By using Lemma 17 and Lemma 18, we obtain

$$E(p^{\mathsf{ML}}_{C_K}) - E(p^{\mathsf{ML}}_{C^*}) \leq n\sqrt{2^{k-\ell}\frac{1 - 2^{-k}}{1 - 2^{-\ell}} + 2^{k-1}\|[C_K]^2 - [C^*]^2\|_\infty}.$$

The bound in Th. 19 is trivial for $k > \ell$. For $k \leq \ell$, we bound $\frac{1-2^{-k}}{1-2^{-\ell}} \leq 1$ and conclude. □

4 Truncated Differential Attack

As in [10,11], we restrict to V of form $V_{\mathsf{in}} \times V_{\mathsf{out}}$ with V_{in} and V_{out} subspaces of $\{0,1\}^\ell$ of dimension s and q, respectively. We have $V^\perp = V^\perp_{\mathsf{in}} \times V^\perp_{\mathsf{out}}$. The dimension of $V^\perp$ is $2\ell - k = \ell - s + \ell - q$. We consider the following distinguisher:

Distinguisher TD:
1: **for** $i = 1$ to n **do**
2: pick $(x, x') \in (\{0,1\}^\ell)^2$ uniformly such that $x \oplus x' \in V^\perp_{\mathsf{in}}$
3: set $y = \mathsf{Enc}(x)$ and $y' = \mathsf{Enc}(x')$
4: set $b_i = 1_{((x,y)\oplus(x',y')) \in V^\perp}$
5: **end for**
6: output $f(b_1, \ldots, b_n)$

The function f which computes the output depending on the vector b is left arbitrary. For instance, with $f(b_1, \ldots, b_n) = b_1 \cdots b_n$, this captures *impossible differentials* [2]. This is a non-adaptive iterated attack of order 2.

Lemma 20 (Link between TD and STD). *For any fixed* Enc *and* Enc^**, we have*

$$|p^{\mathsf{TD}}_{\mathsf{Enc}} - p^{\mathsf{TD}}_{\mathsf{Enc}^*}| \leq n2^s|p^{\mathsf{STD}}_{\mathsf{Enc}} - p^{\mathsf{STD}}_{\mathsf{Enc}^*}|.$$

Proof. We let p^1 denote the best distinguisher with same D and $n = 1$. We apply Lemma 13 and we obtain

$$|p^{\mathsf{TD}}_{\mathsf{Enc}} - p^{\mathsf{TD}}_{\mathsf{Enc}^*}| \leq n|p^1_{\mathsf{Enc}} - p^1_{\mathsf{Enc}^*}|.$$

Clearly, depending on the sign of $p^1_{\mathsf{Enc}} - p^1_{\mathsf{Enc}^*}$, either p^1 is the probability that a differential is found, or it is the probability that it is not found. In any case, we have $2^{-s}|p^1_{\mathsf{Enc}} - p^1_{\mathsf{Enc}^*}| = |p^{\mathsf{STD}}_{\mathsf{Enc}} - p^{\mathsf{STD}}_{\mathsf{Enc}^*}|$, and we obtain the result. □

Theorem 21 (Advantage of TD bounded by decorrelation). *For the TD differential distinguisher described in this section, we have*

$$E(p^{\mathsf{TD}}_{C_K}) - E(p^{\mathsf{TD}}_{C^*}) \leq n2^{1+s-\ell}\frac{1-2^{-k}}{1-2^{-\ell}} + n2^{s-1}\|[C_K]^2 - [C^*]^2\|_\infty.$$

Proof. Due to Lemma 20, we have

$$\begin{aligned} p^{\mathsf{TD}}_{\mathsf{Enc}} - p^{\mathsf{TD}}_{\mathsf{Enc}^*} &\leq n2^s|p^{\mathsf{STD}}_{\mathsf{Enc}} - 2^{-k}| + n2^s|p^{\mathsf{STD}}_{\mathsf{Enc}^*} - 2^{-k}| \\ &= n2^s\left(p^{\mathsf{STD}}_{\mathsf{Enc}} - 2^{-k}\right) + n2^s\left(p^{\mathsf{STD}}_{\mathsf{Enc}^*} - 2^{-k}\right) \end{aligned}$$

since we know from Th. 1 that $p^{\mathsf{STD}}_{\mathsf{Enc}} - 2^{-k}$ is positive. Based on Lemma 17, we have, $E(p^{\mathsf{STD}}_{C_K}) - E(p^{\mathsf{STD}}_{C^*}) \leq \frac{1}{2}\|[C_K]^2 - [C^*]^2\|_\infty$. So,

$$E(p^{\mathsf{TD}}_{C_K}) - E(p^{\mathsf{TD}}_{C^*}) \leq 2n2^s\left(E(p^{\mathsf{STD}}_{C^*}) - 2^{-k}\right) + n2^{s-1}\|[C_K]^2 - [C^*]^2\|_\infty.$$

Due to Lemma 18, we obtain the result. □

Remark 22. The critical term for ML in Th. 19 is $n^2 2^{k-1}\|[C_K]^2 - [C^*]^2\|_\infty$. The one for TD in Th. 21 is $n2^{s-1}\|[C_K]^2 - [C^*]^2\|_\infty$. Presumably, we have lost a factor n in Th. 19 and the difference between ML and TD should only be k vs. s, the dimension of V vs. the one of V_{in}.

Remark 23. For $s = \ell - 1$ and $q = 1$, $V^{\perp}_{\mathsf{in}}$ has a single non-zero vector (which can be seen as a difference vector Δ) and V_{out} has a single non-zero vector (which can be seen as a mask Γ). However, our bound is useless in that case since $2^{1+s-\ell} = 1$. Here, we used again the loose bound of Lemma 13, but changing n into $\sqrt{n}$ would not change this fact. Actually, TD becomes equivalent to DL in this case, and it is known that 4-decorrelation is needed to protect against DL [1]. Since our TD-security results uses 2-decorrelation, improving this bound to get a more useful one in the case of DL would require to use 4-decorrelation. Except for the equivalence to DL, these observations extend to all values of q.

5 Improvement of Previous Results

5.1 Improvement in the Linear and Differential-Linear Contexts

If $\|[C_K]^2 - [C^*]^2\|_\infty \approx 2^{-\ell}$, the bound derived in Th. 7, for linear attacks, is approximately equal to $3(1 + \sqrt[3]{2})\sqrt[3]{n2^{-\ell}}$ and is useful only if the attacker can

take advantage of up to $2^\ell/311$ plaintext-ciphertext pairs. For a 64-bit cipher, it would corresponds to attacks with data complexity less than $2^{55.71}$. In this section we provide a new bound, for linear attacks, useful for n up to $2^\ell/24$ which is $2^{59.42}$.

Th. 7, which is given in Sect. 2.1, has been originally derived in 2003 [21]. The following result consists of an improvement of the upper bound of $E(p^{\mathsf{LC}}_{C_K}) - E(p^{\mathsf{LC}}_{C^*})$. This improvement is obtained thanks to the Jensen equality.

Theorem 24 (Advantage of LC bounded by decorrelation, improvement of Th. 7). *For the linear distinguisher of Sect. 2.3, we have*

$$E(p^{\mathsf{LC}}_{C_K}) - E(p^{\mathsf{LC}}_{C^*}) \leq 2\sqrt{n\|[C_K]^2 - [C^*]^2\|_\infty + \frac{n}{2^\ell - 1}} + 2\sqrt{\frac{n}{2^\ell - 1}}.$$

Proof. Based on [21, Lemma 15], we know that there is some p_0 such that for every Enc, we have $|p^{\mathsf{Enc}} - p_0| \leq 2\sqrt{n\mathsf{LP}^{\mathsf{Enc}}(a,b)}$.

To prove Th. 7, the method used in [21] consisted in getting for any A that[3] $E(p^{\mathsf{LC}}_{\mathsf{Enc}}) - p_0 \leq 2 \cdot A\sqrt{n} + \frac{1}{A^2}E(\mathsf{LP}^{\mathsf{Enc}}(\alpha,\beta))$ and then in minimizing the sum in terms of A. In [21], $A = n^{-\frac{1}{6}}\sqrt[3]{E(\mathsf{LP}^{\mathsf{Enc}}(\alpha,\beta))}$ was taken, to get $E(p^{\mathsf{LC}}_{\mathsf{Enc}}) - p_0 \leq 3\sqrt[3]{nE(\mathsf{LP}^{\mathsf{Enc}}(\alpha,\beta))}$.

To derive the improved bound, instead, we use the Jensen inequality to obtain $|E(p^{\mathsf{Enc}}) - p_0| \leq 2\sqrt{nE(\mathsf{LP}^{\mathsf{Enc}}(\alpha,\beta))}$.

We consider the elementary non-adaptive distinguisher picking x and x' and checking if $\alpha \cdot (x \oplus x') = \beta \cdot (\mathsf{Enc}(x) \oplus \mathsf{Enc}(x'))$. The probability of the equality is $p^2 + (1-p)^2 = \frac{1}{2}(2p-1)^2 + \frac{1}{2}$ where $p = \Pr[\alpha \cdot x = \beta \cdot \mathsf{Enc}(x)]$. Therefore, it is $\frac{1}{2}\mathsf{LP}^{\mathsf{Enc}}(\alpha,\beta) + \frac{1}{2}$ and $\mathsf{LP}^{\mathsf{Enc}}(\alpha,\beta)$ expresses the advantage of a non-adaptive distinguisher using two queries. From Th. 2, we have $E(\mathsf{LP}^{C_K}(\alpha,\beta)) \leq E(\mathsf{LP}^{C^*}(\alpha,\beta)) + \|[C_K]^2 - [C^*]^2\|_\infty$. From [21, Lemma 14] we obtain that

$$E(\mathsf{LP}^{C^*}(\alpha,\beta)) = \frac{1}{2^\ell - 1}.$$

□

In the same way the bound derived for the differential-linear attack, in Th. 8 is approximately equal to $3(\sqrt[3]{3} + \sqrt[3]{2})\sqrt[3]{n2^{-\ell}}$ and is useful for an attacker which can take advantage to up to $2^\ell/532$ plaintext-ciphertext pairs. Using the same technique, meaning the Jensen inequality, we can improve Th. 8 and derive a new bound in the differential-linear context which is valid for any attack using up to $2^\ell/39$ plaintext-ciphertext pairs.

[3] The last term bounds the probability that $\mathsf{LP}^{\mathsf{Enc}}(\alpha,\beta)$ exceeds A^2 and the first is a consequence of [21, Lemma 15].

Theorem 25 (Advantage of DL bounded by decorrelation, improvement of Th. 8). *For the differential-linear distinguisher of Sect. 2.3, we have*

$$E(p^{\mathsf{DL}}_{C_K}) - E(p^{\mathsf{DL}}_{C^*}) \leq 2\sqrt{n\|[C_K]^4 - [C^*]^4\|_\infty + n\frac{2\times 2^\ell - 5}{(2^\ell-1)(2^\ell-3)}} + 2\sqrt{n\frac{2\times 2^\ell - 5}{(2^\ell-1)(2^\ell-3)}}.$$

5.2 In the Context of Differential and Boomerang Attacks, Extension of Th. 6 and Th. 10

Before providing, in this section, an extension of Th. 6 and Th. 10, we present an extension of [21, Lemma 15] for the following iterative distinguisher:

Distinguisher Dist:
1: **for** $i = 1$ to n **do**
2: pick a bit b_i with expected value p_{Enc}
3: **end for**
4: output $f(b_1, \ldots, b_n)$

Lemma 26. *Let p_{Enc} be a probability depending on a cipher* Enc. *We have $|E(p^{\mathsf{Dist}}_{\mathsf{C_K}}) - E(p^{\mathsf{Dist}}_{\mathsf{C^*}})| \leq n.\max(E(p_{C_K}), E(p_{C^*}))$.*

Proof. If $f(0,\ldots,0) = 0$, then $p^{\mathsf{Dist}}_{\mathsf{Enc}} \leq np_{\mathsf{Enc}}$ and $E(p^{\mathsf{Dist}}_{C_K}) - E(p^{\mathsf{Dist}}_{C^*}) \leq E(p^{\mathsf{Dist}}_{C_K}) \leq nE(p_{C_K})$. Similarly, we have $E(p^{\mathsf{Dist}}_{C^*}) - E(p^{\mathsf{Dist}}_{C_K}) \leq E(p^{\mathsf{Dist}}_{C^*}) \leq nE(p_{C^*})$, and the result holds in this case.

If $f(0,\ldots,0) = 1$, we change f to $1-f$ without changing $|E(p^{\mathsf{Dist}}_{C^*}) - E(p^{\mathsf{Dist}}_{C_K})|$ and go back to the previous case. □

Differential Distinguisher. In Sect. 2.1, the differential distinguisher is defined for a given Boolean function f corresponding to $f(b_1, \cdots b_n) = \max_i b_i$. In practice, for many differential attacks more than one valid pair is necessary to distinguish the cipher from a random permutation. In this section we generalize this distinguisher to any Boolean function f.

Theorem 27 (Advantage of DC bounded by decorrelation, improved Th. 6). *For the distinguisher DC, we have*

$$E(p^{\mathsf{DC}}_{C_K}) - E(p^{\mathsf{DC}}_{C^*}) \leq \frac{n}{2^\ell - 1} + \frac{n}{2}\|[C_K]^2 - [C^*]^2\|_\infty.$$

Proof. The proof is similar to the proof of Th 6 which can be found in [21, Th. 13]. The difference is that we use Lemma 26 to get rid of the arbitrary f.

Boomerang Distinguisher. In the same way, we can improve the boomerang distinguisher by considering any Boolean function f. As for Th. 10, we can prove the following result.

Theorem 28 (Advantage of Boo bounded by decorrelation, improved Th. 10). *For the distinguisher Boo, we have*

$$E(p_{C_K}^{\mathsf{Boo}}) - E(p_{C^*}^{\mathsf{Boo}}) \leq n\frac{2\times 2^\ell - 5}{(2^\ell-1)(2^\ell-3)} + \frac{n}{2}\|[C_K]^4 - [C^*]^4\|_a.$$

6 Conclusion

In this paper, we studied the multidimensional linear and truncated differential attacks in the context of the decorrelation theory. We showed that these attacks are non-adaptive iterated attacks of order 2. Table 1 summarizes the considered attacks. In particular, we obtained three types of results:

- we improved the bounds for the linear and differential-linear distinguishers (Th. 7 and Th. 8 are improved by Th. 24 and Th. 25, respectively);
- we generalized the differential and boomerang distinguishers to allow an arbitrary function f (Th. 6 and Th. 10 are improved by Th. 27 and Th. 28, respectively);
- we proved the security for multidimensional linear and truncated differential with decorrelation (Th. 19 and Th. 21).

We let as open problems the seek for an improved Lemma 13 with $\sqrt{n}$ instead of n as suggested in Rem. 15. This would allow for better bounds in Th. 19 and Th. 21. We shall also find better bounds based on a higher order of decorrelation, in particular to link Th. 21 to Th. 25 (see Rem. 23).

Table 1. The decorrelation order of some statistical attacks.

Attack	Decorrelation order	Type of attack	Attack order	Maximal n
Linear LC	2	iterative	1	2^ℓ
Differential DC	2	iterative	2	2^ℓ
Differential-linear DL	4	iterative	2	$2^{\ell-1}$
Boomerang Boo	4	adaptive, iterative	4	$2^{\ell-1}$
Multidimensional linear ML	2	vector-iterative	1	$2^{\frac{\ell-k}{2}}$
Truncated differential TD	2	iterative	2	$2^{\ell-s-1}$

References

1. A. Bay. Provable Security of Block Ciphers and Cryptanalysis. PhD Thesis no. 6220, EPFL, 2014. http://library.epfl.ch/theses/?nr=6220

2. E. Biham, A. Biryukov, A. Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials, In *Advances in Cryptology EUROCRYPT'99*, Prague, Czech Republic, Lecture Notes in Computer Science 1592, pp. 12–23, Springer-Verlag, 1999.
3. E. Biham, O. Dunkelman, N. Keller. Enhancing Differential-Linear Cryptanalysis. In *Advances in Cryptology ASIACRYPT'02*, Queenstown, New Zeland, Lecture Notes in Computer Science 2501, pp. 254–266, Springer-Verlag, 2002.
4. A. Bogdanov, G. Leander, K. Nyberg, M. Wang. Integral and Multidimensional Linear Distinguishers with Correlation Zero. In *Advances in Cryptology ASIACRYPT'12*, Beijing, China, Lecture Notes in Computer Science 7658, pp. 244–261, Springer-Verlag, 2012.
5. A. Bay, A. Mashatan, S. Vaudenay. Resistance against Adaptive Plaintext-Ciphertext Iterated Distinguishers. In *Progress in Cryptology INDOCRYPT'12*, Kolkata, India, Lecture Notes in Computer Science 7668, pp. 528–544, Springer-Verlag, 2012.
6. A. Bay, A. Mashatan, S. Vaudenay. Resistance against Iterated Attacks by Decorrelation Revisited. In *Advances in Cryptology CRYPTO'12*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 7417, pp. 741–757, Springer-Verlag, 2012.
7. A. Bay, A. Mashatan, S. Vaudenay. Revisiting Iterated Attacks in the Context of Decorrelation. *Cryptography and Communications*, vol. 6, pp. 279–311, 2014.
8. E. Biham, A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In *Advances in Cryptology CRYPTO'90*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 537, pp. 2–21, Springer-Verlag, 1991.
9. C. Blondeau, K. Nyberg. New Links between Differential and Linear Cryptanalysis. In *Advances in Cryptology EUROCRYPT'13*, Athens, Greece, Lecture Notes in Computer Science 7881, pp. 388–404, Springer-Verlag, 2013.
10. C. Blondeau, K. Nyberg. Links Between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities. In *Advances in Cryptology EUROCRYPT'14*, Copenhaguen, Denmark, Lecture Notes in Computer Science 8441, pp. 165–182, Springer-Verlag, 2014.
11. C. Blondeau, G. Leander, K. Nyberg. Differential-Linear Cryptanalysis Revisited. To appear in the proceedings of FSE'14.
12. F. Chabaud, S. Vaudenay. Links Between Differential and Linear Cryptanalysis. In *Advances in Cryptology EUROCRYPT'94*, Perugia, Italy, Lecture Notes in Computer Science 950, pp. 356–365, Springer-Verlag, 1995.
13. S.K. Langford, M.E. Hellman. Differential-Linear Cryptanalysis. In *Advances in Cryptology CRYPTO'94*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 839, pp. 17-25, Springer-Verlag, 1994.
14. M. Hermelin,J.Y. Cho,K. Nyberg. Multidimensional Extension of Matsui's Algorithm 2. In *Fast Software Encryption'09*, Leuven, Belgium, Lecture Notes in Computer Science 5665, pp. 209-227, Springer-Verlag, 2009.
15. L.R. Knudsen. Truncated and Higher Order Differentials. In *Fast Software Encryption'93*, Cambridge, United Kingdom, Lecture Notes in Computer Science 809, pp. 196–211, Springer-Verlag, 1994.
16. G. Leander. On Linear Hulls, Statistical Saturation Attacks, PRESENT and a Cryptanalysis of PUFFIN. In *Advances in Cryptology EUROCRYPT'11*, Tallinn, Estonia, Lecture Notes in Computer Science 6632, pp. 303–322, Springer-Verlag, 2011.

17. M. Matsui. Linear Cryptanalysis Method for DES Cipher. In *Advances in Cryptology EUROCRYPT'93*, Lofthus, Norway, Lecture Notes in Computer Science 765, pp. 386-397, Springer-Verlag, 1994.
18. S. Vaudenay. Provable Security for Block Ciphers by Decorrelation. In *STACS'98*, Paris, France, Lecture Notes in Computer Science 1373, pp. 249–275, Springer-Verlag, 1998.
19. S. Vaudenay. Resistance Against General Iterated Attacks. In *Advances in Cryptology EUROCRYPT'99*, Prague, Czech Republic, Lecture Notes in Computer Science 1592, pp. 255–271, Springer-Verlag, 1999.
20. S. Vaudenay. Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness. In *Selected Areas in Cryptography'99*, Kingston, Ontario, Canada, Lecture Notes in Computer Science 1758, pp. 49–61, Springer-Verlag, 2000.
21. S. Vaudenay. Decorrelation: a Theory for Block Cipher Security. *Journal of Cryptology*, vol. 16, pp. 249–286, 2003.
22. D. Wagner. The Boomerang Attack. In *Fast Software Encryption'99*, Roma, Italy, Lecture Notes in Computer Science 1636, pp. 156–170, Springer-Verlag, 1999.
23. M.N. Wegman, J.L. Carter. New Hash Functions and Their Use in Authentication and Set Equality. *Journal of Computer and System Sciences*, vol. 22, pp. 265–279, 1981.