Can a Differential Attack Work for an Arbitrarily Large Number of Rounds?

Nicolas T. Courtois[1 [0000−0003−0736−431X]] and Jean-Jacques Quisquater[2]

[1] University College London, Gower Street, London, UK
[2] Université Catholique de Louvain, Belgium

Abstract. Differential cryptanalysis is one of the oldest attacks on block ciphers. Can anything new be discovered on this topic? A related question is that of backdoors and hidden properties. There is substantial amount of research on how Boolean functions affect the security of ciphers, and comparatively, little research, on how block cipher wiring can be very special or abnormal. In this article we show a strong type of anomaly: where the complexity of a differential attack does not grow exponentially as the number of rounds increases. It will grow initially, and later will be lower bounded by a constant. At the end of the day the vulnerability is an ordinary single differential attack on the full state. It occurs due to the existence of a hidden polynomial invariant. We conjecture that this type of anomaly is not easily detectable if the attacker has limited resources.

Keywords: Feistel ciphers· Boolean functions · Multivariate polynomials · T-310 · Generalized Linear Cryptanalysis · Polynomial invariants · Hidden polynomial problems · Annihilators · Markov ciphers · k-normality · Algebraic cryptanalysis

1 Introduction

Differential Cryptanalysis (DC) is a well-known basic attack on block ciphers [4, 32] and it may seem that what remains to study are just some fine details, cf. [28]. In order to improve DC, researchers have considered various ways to aggregate a larger number of differences [31], for example with truncated differentials of Knudsen [40]. We can hardly just combine two truncated differentials and expect that the propagation probabilities would just be multiplied [9, 29, 30]. There is a hidden complexity and a lot of non-uniformity: probabilities of individual differentials may differ very substantially. However we do not expect anything special to happen with just old ordinary DC with single differentials. In fact we do: it is the well-known question of Markov ciphers [42]. In this paper we study cases where this property is violated, and DC does not work as expected because relevant events are not independent. What is interesting is showing that this can advantage the attacker in a substantial way.

This paper is also about backdooring and hidden properties. Here we will have a hidden polynomial equation in a similar way as in certain public key cryptosystems. It is not apparent for the attacker, even if the attacker knows another, related set of polynomials, which they use for encryption. Our hidden property is going to be a non-linear invariant property, a topic which has attracted considerable attention in recent years [12–19, 43, 51]. A wider fundamental open problem is the very existence of new attacks on block ciphers, of any sort, such that their complexity would not grow exponentially with the number of rounds. Even though such attacks exist, they seem extremely complex. Surely this would not be possible with good old differential cryptanalysis? In this paper we show that this is actually possible. A similar result for a truncated differential attack was presented at Crypto 2011, cf. Section 3 of [43]. This earlier result worked only for some weak keys. Our attack works with a single differential, which is harder, as probabilities are lower. It is uniform and works for all 2^{240} keys without any exception. It also works in spite of the presence of round constants in T-310.

In this article these considerations come together. We show how to design an anomalous differential attack. The only thing that the attacker observes, will be that a certain differential propagates with a probability which will be bounded by a constant for any number of rounds. This is quite surprising and hides the existence of a hidden polynomial invariant property, the existence of which the attacker could potentially ignore forever; even if they know about the (derived) differential property. Sometimes, differential cryptanalysis does not work as predicted by a "naive" theory and the events in different rounds are not independent. However, this is not just an annoying discrepancy; a bug which was typically ignored by researchers until now. We discover that an anomaly of this sort conceals another strong property extremely useful for the attacker.

This article is organised as follows. In Section 2 we explain the philosophy of what we do. In Section 3 we study the T-310 cipher. In Section 4 we present some older examples of invariant attacks on T-310. In Section 5 we describe our attack with one main theorem and 3 technical lemmas. In Section 6 we show what happens in practice. In Section 7 we discuss several future cryptanalysis research ideas and we wonder if some sort of converse result could be true. Then comes the Conclusion. In Appendix A we look at vulnerability of Boolean functions against our attacks. In Appendix B we consider how invariant properties we study can be used for key recovery.

2 Background: Markov Ciphers and Nonlinear Invariants

The notion of Markov ciphers was introduced at Eurocrypt 1991 by Lai, Massey, and Murphy, see [42]. Probably these questions were already studied earlier, in the Eastern Bloc, cf. [23, 24, 41]. In short, we have a Markov cipher when the probability that a certain output difference is obtained, does not depend on the input value (but depends on the input difference), when the round key is chosen random. This formulation ignores the question of how the probability depends also on the key, and therefore, our current understanding is yet greatly simplified (we refer to [28, 41] to see why this matters). In short, in [42] it is simply assumed that the keys are chosen uniformly at random, similar to averaging probabilities over all possible keys. Many known ciphers are Markov ciphers, for example DES, FEAL, LOKI and IDEA, [42]. Other ciphers such as GOST behave as Markov ciphers with some degree of approximation [9, 28].

The importance of Markov ciphers is explained in page 24 of [42]: in a Markov cipher "every differential will be roughly equally likely" after sufficiently many rounds, cf. also [47]. The main goal of the present article is to show that there exists a block cipher **violating** this exact long-term derived property of Markov ciphers in an extremely strong way. Here all differentials will vanish progressively, with probability being zero in practical terms, except with very few special differentials. These differences are able to survive for an arbitrarily large number of rounds. If so, not being a Markov cipher degrades the security of our cipher in a very substantial way. Compared to earlier results in [43], our attack cf. Thm. 5.1.1 works for any key, 100 % of keys. Moreover, it works with round constants in T-310. Eliminating the round constants and the key bits alike are hard problems in non-linear cryptanalysis. Many known attacks only work for some keys, not all, see [43, 51], or only for some round constants, see Section 7.4 in [14].

What we study in this paper is very much like a backdoor, a hidden unexpected property leading to a strong attack. We emphasise the fact that events of this kind can be easily overlooked. There is an exponential number of differences to study and specific events are detectable only if we have sufficient computing power and a sufficient number of Plaintext/Ciphertext (P/C) pairs. They could also be detected if a specific difference with abnormal propagation is already known, or we are able to characterize some specific input states on n bits where the propagation behaves in an unusual way. Researchers who study this on the experimental side might also discard this result as an outlier. We found it very hard to believe that this is real. Therefore, it is important that in the present article we establish our result through rigourous mathematical proof, see Thm. 5.1.1 page 9. It is also confirmed by computer simulations in Section 6.

2.1 Weak Keys and Weak Components - Long Term Key

There is a substantial amount of research on how non-linear components (Boolean functions and S-boxes) affect the security of ciphers and comparatively little research, on how the block cipher wiring can be special or weak, for example with DES P-box, see [5] or the long-term key LZS in T-310 [21]. In cryptanalysis, we always look for special or even abnormal cases, for example, the block cipher KeeLoq can be broken in an extremely short time of type only 2^{23} for 15 % of keys, cf. [2]. A fair assessment of weakness requires the assumption that weak keys occur at random, with their “natural” probability; see the “multiple random key scenario” in Section 29 in [10]. Here we study the probability for a Boolean function that a certain product of polynomials is zero, see Appendix A. An essential observation is that in the ring of Boolean polynomials, factorization is not unique and there are typically numerous solutions to such problems, see [15], and one may eventually lead to an attack [17, 19].

2.2 Nonlinear Cryptanalysis and Higher Order Nonlinear Cryptanalysis

In recent years many authors show how to construct attacks where a certain non-linear polynomial is invariant [12–19, 43, 51]. Following ICISC 2019, a good way to study these attacks is a white box method [19]. We formulate our attacks using Boolean polynomial arithmetic. As such, the whole attack could potentially apply to another cipher modulo renaming of variables and we do not use the full specification of the cipher, see [19] and [14]. If a cipher satisfies a certain number of initial conditions on some basic polynomials, then our attack works for an arbitrarily large number of rounds. If a property involves just one encryption, we say it is a property of order 1. The invariants in [16, 19, 17] and a majority of other recent works on non-linear invariants are of order one (for one single encryption). In this paper a property of order 1 will be used to alter the behaviour of a differential attack. Overall we get an invariant property of order 2.

An important family of invariant attacks are product attacks: the invariant is a product of polynomials. Constructing a non-linear invariant attack is a difficult combinatorial problem. At Eurocrypt’96 Knudsen and Robshaw claimed that this cannot work for Feistel ciphers [44]. Initially, attempts to find a non-linear invariant attack on DES have failed, or produced a tiny improvement compared to Matsui's Linear Cryptanalysis (LC), cf. Crypto 2004 in [20]. Certain block ciphers such as T-310 use only very few key bits in each round, cf. [23], and are particularly vulnerable to this type of attack. Consequently, we have a plethora of attacks of this type [51, 14, 12] with increasing degrees [13, 16, 19], which is expected to make the attack increasingly powerful. More general attacks can work with sums of two or more products. For T-310 this is shown in [18], with an example of type $AC+BD$ which we reproduce below in Section 4.3. An example with DES is found in Remark 2 in Section 10 of [19].

2.3 On Success Probability and Annihilation Degree in Previous Attacks

In ICISC 2019 the best attack on T-310 was such that if our Boolean function is such that $(Z+e)(a+b)(c+d)=0$ then a certain product of 8 linear polynomials is an invariant working for any number of rounds, any key, and any choice of round constants. A Boolean function with this type of annihilation with 2 factors is called 4-weakly-normal, where $4=6-2$, cf. Appendix A and [7]. This notion was earlier studied by Dobbertin [34]. It is easy to see that a Boolean function Z chosen at random will be 4-weakly-normal with very high probability of $2^{-0.68}$, cf. Table 4. A yet stronger or more realistic attack which would only require that Z is 3-normal with $Z(a+d)(b+e)(c+f)=0$ was described in [16], and a similar attack will be studied inside this paper as a technical Lemma 5.3.1 page 12. The degree of freedom for the attacker increases at last. 100 % of all Boolean functions on 6 bits are 3-normal, see Section 5 in [19] and [35]. Moreover, several methods to annihilate with a product of 3 factors exist typically. A recent paper shows that a similar attack with 3 factors exists also with the original Boolean function used during the Cold War to protect government communications [17].

3 Short Description of T-310

We recall the definition of T-310 block cipher from [50]. T-310 operates on 36 bit blocks and a secret key on 240 bits. Each round involves two key bits K,L and one round constant bit F, which is derived from a fixed IV of 61 bits which is transmitted in clear text. The secret key of 240 bits is stored on a paper punch card and is reused after every 120 rounds. The actual encryption is done in a peculiar stream cipher mode which we will ignore here. We refer to [50] and [21] for more details. In this paper we only study the underlying block cipher (a keyed permutation on 36 bits).

The wiring or the long term key in T-310, is the equivalent of the P-box in DES, and it is known under the name of LZS or *Langzeitschlüssel*, which means a long-term key. It is changed once per year typically. Formally the LZS wiring is defined by two functions: $D:\{1\ldots9\}\rightarrow\{0\ldots36\}$, $P:\{1\ldots27\}\rightarrow\{1\ldots36\}$ which are typically injective. We need to specify which input state bits are connected to contacts named D1-D9 and v1-v27 in Fig. 2. For example $D(5)=36$ is about what happens inside the small square box with letter D in Fig. 1. $D(5)=36$ means that input bit x_{36} is connected to the wire called $D5$ in Fig. 2 which then becomes $U5=y_{17}$ after XOR with bit $g4$. Then $P(1)=25$ refers the content of the square box with letter P in Fig. 1. It means that input x_{25} is connected to v1 or the 2nd input of Z_1 in Fig. 2.

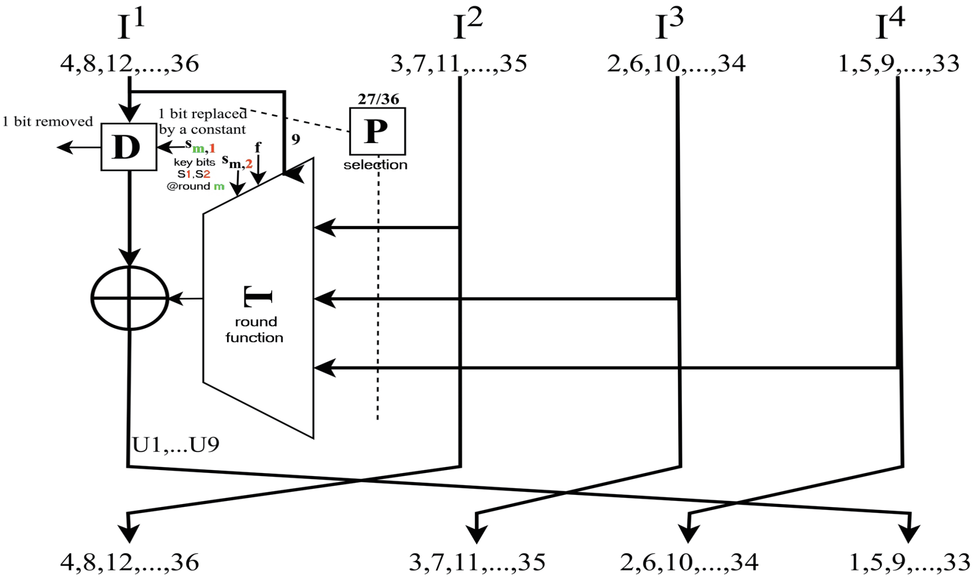


Fig. 1. High-level overview of one round of T-310.

In each round only 2 key bits K,L are used. The secret key is defined as $s_{1...120,1...2} \in \{0,1\}^{240}$ which is 240 bits. The same 2 bits are repeated after 120 rounds with

$$K = s_{m,1} \quad \text{and} \quad L = s_{m,2}$$

In addition each round has a round constant called F, which is derived from the public IV value. In all, for any $F,K,L \in \{0,1\}^3$ one round of this block cipher is a permutation on 36 bits. This requirement is not obvious and it requires some complex technical conditions on the cipher wiring, see [22].

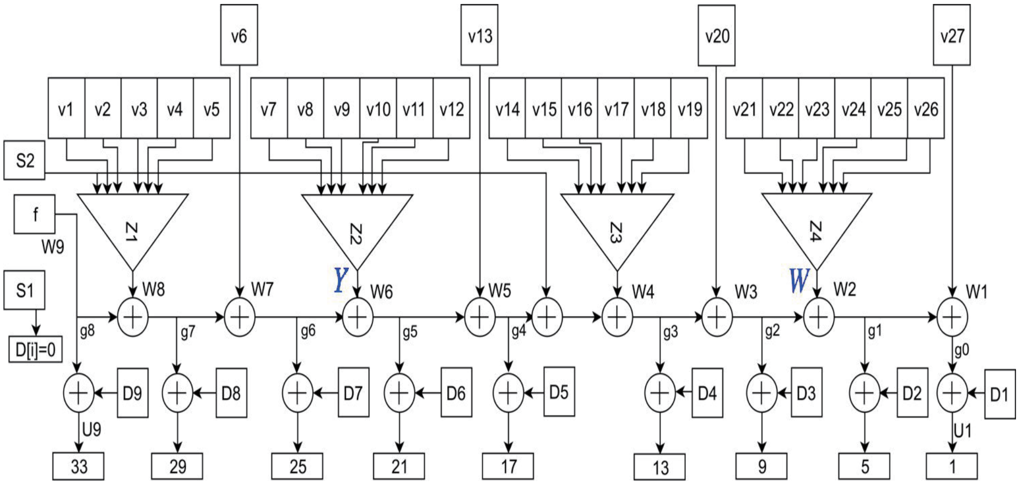


Fig. 2. The internal structure of one round of T-310 block cipher.

In Fig. 3 we give a set of closed formulas to compute the output bits y_{1-36} in each round from the input bits x_{1-36}. These formulas are self contained, i.e. everything can be derived just from these formulas. In one round 9 new bits are created and $36-9=27$ bits are shifted by one position. The cipher uses 4 identical Boolean functions of 6 bits which are denoted by Z_1, Z_2, Z_3, Z_4 on Fig. 2. A common convention is to rename these 4 Boolean functions and use 1-letter notations $Z(), Y(), X(), W()$ respectively (backwards naming convention).

$$y_{i+1} = x_i \text{ for any } i \neq 4k \qquad (\text{ with } 1 \leq i \leq 36) \qquad (\text{r}0)$$

$$y_{33} = F + x_{D(9)} \qquad (\text{r}1)$$

$$Z_1 \overset{def}{=} Z(L, x_{P(1)}, \dots x_{P(5)}) \qquad (\text{z}1)$$

$$y_{29} = F + Z_1 + x_{D(8)} \qquad (\text{r}2)$$

$$y_{25} = F + Z_1 + x_{P(6)} + x_{D(7)} \qquad (\text{r}3)$$

$$Z_2 \overset{def}{=} Y(x_{P(7)}, \dots, x_{P(12)}) \qquad (\text{z}2)$$

$$y_{21} = F + Z_1 + x_{P(6)} + Z_2 + \qquad x_{D(6)} \qquad (\text{r}4)$$

$$y_{17} = F + Z_1 + x_{P(6)} + Z_2 + \qquad x_{P(13)} + x_{D(5)} \qquad (\text{r}5)$$

$$Z_3 \overset{def}{=} X(x_{P(14)}, \dots, x_{P(19)}) \qquad (\text{z}3)$$

$$y_{13} = F + Z_1 + x_{P(6)} + Z_2 + \qquad x_{P(13)} + L + Z_3 + x_{D(4)} \qquad (\text{r}6)$$

$$y_9 = F + Z_1 + x_{P(6)} + Z_2 + \qquad x_{P(13)} + L + Z_3 + x_{P(20)} + x_{D(3)} \qquad (\text{r}7)$$

$$Z_4 \overset{def}{=} W(x_{P(21)}, \dots, x_{P(26)}) \qquad (\text{z}4)$$

$$y_5 = F + Z_1 + x_{P(6)} + Z_2 + \qquad x_{P(13)} + L + Z_3 + x_{P(20)} + Z_4 + x_{D(2)} \qquad (\text{r}8)$$

$$y_1 = F + Z_1 + x_{P(6)} + Z_2 + \qquad x_{P(13)} + L + Z_3 + x_{P(20)} + Z_4 + x_{P(27)} + x_{D(1)} \qquad (\text{r}9)$$

$$x_0 \overset{def}{=} K \qquad (\text{s}1)$$

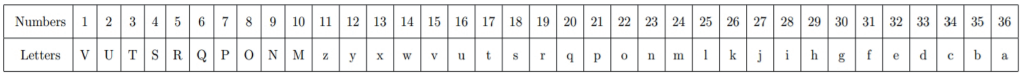
$$F \in \{0,1\} \text{ is a round constant } \quad \text{depending on a (public) IV} \qquad (f1)$$

$$K = s_{m \bmod 120,\ 1} \qquad (\text{in encryption round } \ m = 0,1,2,\dots) \qquad (k1)$$

$$L = s_{m \bmod 120,\ 2} \qquad (\text{in encryption round } \ m = 0,1,2,\dots) \qquad (k2)$$

Fig. 3. The specification of one round of T-310.

Notation. When we work on invariant attack, we use more compact notations. and the 36 bits $x_1, \dots, x_{36}$ are replaced by single letters, cf. Fig. 4.



Numbers	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Letters	V	U	T	S	R	Q	P	O	N	M	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

Fig. 4. Variable naming conventions.

We work on invariants, and variables y_1 and x_1 will be treated likewise and denoted by the same letter (!). Letters were chosen to avoid certain letters like F or W used for a different purpose. Traditionally, if we want to avoid ambiguity, we will distinguish between the variable a at input denoted by a^i and the same variable at output denoted by a^o. Moreover later inside this paper we study two distinct encryptions, in which case we can distinguish the two instances of a by a^1 or a^2 added in the exponent.

4 Some Early Attacks on T-310 and Related Questions

The T-310 block cipher is a good target for cryptanalysis with non-linear invariants. The key reason for this is that extremely few key bits and other round constants are used in each round. This is a crucial property, which distinguishes block ciphers made in the West, typically stronger, and weaker block ciphers made in the Eastern Bloc, a question which was discussed in [23, 24]. For this reason, DES is substantially more secure than T-310, even though apart from this property, both ciphers are extremely similar, and can be attacked in the same way. The difference is mainly quantitative: many more key bits are involved in each round of DES. Consequently, attacks on DES typically only work for a small fraction of the key space. This was shown very clearly in ICISC 2019 [19] where two ciphers are studied side-by-side, and earlier in [16].

In Section 7 of [27] the authors propose to look for a non-linear invariant property for T-310, yet at the time no such property was known. For many decades researchers knew about this type of attack [38, 20], and yet failed to find convincing examples, except for contrived ciphers [25]. More recently, only with T-310 we get powerful invariants working for any number of rounds, any key, and any choice of round constants.

4.1 Linear and Non-Linear Invariants and Phase Transitions

A good way to study such attacks, is the so called “white box” algebraic approach [14, 19]. We operate in the cipher specification space and we characterise exactly in which cases the attack works by formal polynomial algebra. The goal of the attacker is to find an invariant and eliminate all the internal state bits, this including the key bits and round constants. As a toy example, we consider the cipher wiring known as 847 in [12].

```
847: P=32,22,26,14,21,36,30,17,15,29,27,13,4,23,1,8,35,20,
5,16,24,9,10,6,7,28,12 D=24,12,8,16,36,4,20,28,32
```

We consider two cycles shown in Fig. 5, which show the group action of one encryption round, cf. Fig. 3, instantiated with wiring 847 above, on some very basic polynomials:

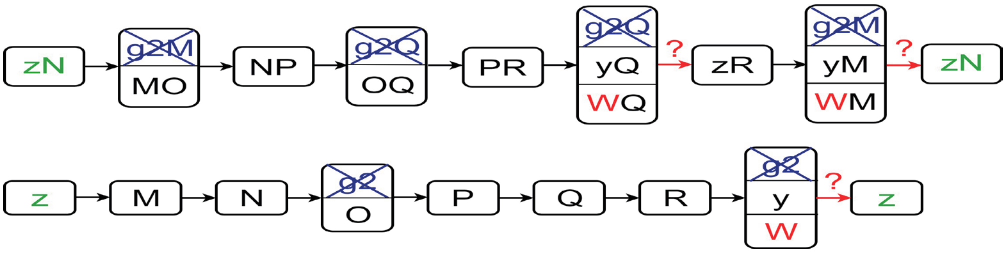


Fig. 5. Transitions between polynomials in an older attack from [12].

Let polynomial $\mathscr{P}$ be the addition of all polynomials of degree 1 and 2 in Fig. 5, excluding those with W, which represents the Boolean function. Here $g2$ depends on the cipher state and the key in a complex way, see Fig. 2, and yet all terms with $g2$ appear an even number of times modulo 2 and are cancelled. Then, it is easy to see that this $\mathscr{P}$ will be a degree 2 polynomial invariant for our cipher, IF the Boolean function W satisfies the following equation:

$$W(1+M+Q)=0$$

This is known in general as the Fundamental Equation (FE). Terms W, WM and WQ are eliminated when we add them, not individually. This was not a very good attack. Extremely few Boolean functions satisfy this equation, cf. Table 3 in Appendix A, and our Boolean function cannot be balanced, cf. Theorem 6.4 in [19].

4.2 Phase Transitions or How Impossible Becomes Possible

Here the crucial question is the one of phase transition, cf. Section 2.4 in [16]. This is how ciphers with stronger components can eventually be attacked. The idea is that a spectacular improvement can occur as the degree of the invariant polynomial grows. The paper [14] contains a large body of examples with growing degree and effectively demonstrates this. This leads to the methodology of attack "hopping" or/and attack "lifting". Sometimes the cipher can be modified and fundamental equation does not change. In [18] the attacker modifies a cycle and adds additional polynomials to it. Finally, we also can add one more cycle to our attack, while avoiding our invariant polynomial becoming zero, cf. [19]. We can then hope to obtain a Fundamental Equation which has more roots, or to find an attack which will work for a larger set of Boolean functions, or even find an attack in a real-life setting, cf. Section 3 in [15] and [17].

4.3 Invariant Hopping and Attack Lifting - Example

A short self-contained introduction which shows this process at work can be found in [18]. For example in Section 7.1. and Thm. 7.3. in [18], we find that for a certain cipher wiring known as 551, if we have

$$(Z(a,b,c,d,e,f)+f)(d+e)=0$$

then the polynomial

$$\mathscr{P}=(e+m)\cdot(g+o)+(f+n)\cdot(h+p)$$

is an invariant for our cipher where $e=x_{32}$ etc, which is different than input e of Z above, following the cipher state variable naming convention of Fig. 4.

In contrast a better product invariant attack of degree 4 can be constructed with

$$\mathscr{P}=(e+m)(f+n)(g+o)(h+p)$$

which invariant works for a substantially larger proportion of Boolean functions. In this case it was shown in [18] that we only need something like:

$$(Z+f)(d+e)(a+b)(c+f)=0$$

and this happens for any Boolean function with large probability of 2^{-8}, cf. Appendix A or Appendix C in [16]. In general as the degree grows, it becomes easier to find a Boolean function where our polynomial invariant actually works. At this stage, if for a particular function our cipher is still not broken, this is rather accidental than deliberate. Eventually it can also be made to work with a real-life Boolean function, see [17].

Note. All the attacks above were invariant attacks of order 1, dealing with just one encryption. In this paper we will construct an invariant attack of order 2.

5 Constructing An Anomalous Differential Invariant Attack

We define the following 8 basic polynomials:

$$\begin{cases} A \overset{def}{=} (m+i) & \text{which is bits } 24,28 \text{ cf. Fig. 4.} \\ B \overset{def}{=} (n+j) & \text{which is bits } 23,27 \\ C \overset{def}{=} (o+k) & \text{which is bits } 22,26 \\ D \overset{def}{=} (p+l) & \text{which is bits } 21,25 \\ E \overset{def}{=} (O+y) & \text{which is bits } 8,12 \\ F \overset{def}{=} (P+z) & \text{which is bits } 7,11 \\ G \overset{def}{=} (Q+M) & \text{which is bits } 6,10 \\ H \overset{def}{=} (R+N) & \text{which is bits } 5,9. \end{cases}$$

These polynomials allow to greatly simplify our attack. We start by observing that we have the following incomplete cycle, or pseudo-cycle, also shown in later Fig. 7:

$$H \to G \to F \to E \to ?\, D \to C \to B \to A \to ?\, H$$

Here six transitions are completely trivial for example $H \to G$ and due to the internal wiring: these bits are just shifted inside this cipher. Two other transitions, namely $E \to ?\, D$ and $A \to ?\, H$ are in contrast just impossible. They would be true only if certain complex Boolean functions namely $W()$ and $Y()$ were equal to zero for every input, which is not the case and will not be the case. However certain multiples of these polynomials will be annihilated (i.e. 0 for every input, and formally 0 as a polynomial). For example, the attacker discovers that under certain conditions a certain polynomial such as $\mathscr{P} = ABCD$ or $AC + BD$ will be invariant, and its value will not change cf. [14–19].

5.1 Our Main Theorem - An Order Two Invariant Property

Theorem 5.1.1 (An Anomalous Differential Attack).
Given the eight basic polynomials $A - H$ defined as above and reproduced also in Fig. 7, AND for each cipher wiring for T-310 s.t.

$$\begin{cases} \{D(2), D(3)\} = \{6 \cdot 4, 7 \cdot 4\} \\ \{D(6), D(7)\} = \{2 \cdot 4, 3 \cdot 4\} \end{cases}$$

AND and if these four multiples of four being 8,12,24,28 are absent from the set of 27 inputs in $\{P(1) \dots P(27)\}$, where $P : \{1 \dots 27\} \to \{1 \dots 36\}$ is an injective wiring, AND for any[1] Boolean function[2] which is such, that we have:

$$Z(a+d)(b+e)(c+f) = 0$$

AND if the 6 inputs of $W()$ defined by integers $P(21), \dots, P(26)$, are mapped to any 3 out of 6 polynomials B, C, D, F, G, H, in a way which preserves[3] the partitioning in three sets or pairs in (a+d)(b+e)(c+f), for example the inputs of W can be $5, 22, 7, 9, 26, 11$

[1] This happens with probability at least 2^{-8} for any Boolean function, see Appendix A.

[2] This function is used twice as W and as Y for 2 disjoints sets of 6 inputs.

[3] For example if one input A is b the other must be e.

AND the 6 inputs of $Y()$ defined by integers $P(7),\ldots,P(12)$ are the mapped to remaining 3 out of 6 polynomials B,C,D,F,G,H, while also preserving a partitioning in 3 sets of pairs in (a+d)(b+e)(c+f), for example in order $25,10,27,21,6,23$,

THEN for any short term key of 240 bits, and for any initial state on 36 bits, and for any IV, the input difference $[7,11]$ corresponding to F, i.e. we flip both bits 7 and 11, will be preserved at the output after any number of rounds being a multiple of 8 with probability of at least 2^{-8}.

Remark. This theorem can be transposed by considering arbitrary permutations of 6 inputs a,b,c,d,e,f. These do not need to be applied consistently at both $W()$ and $Y()$, for example inputs 5 and 9 could be exchanged. However, we need to get the same partitioning of 6 inputs into 3 sets of 2 which needs to be consistent in W, in Y and with the partitioning which actually annihilates our Boolean function. We can also consider an arbitrary choice of 3 out of 6 polynomials in $BCDFGH$ to split between W and Y. In our example D,G,B are 3x2 inputs of $W()$ and the remaining 3 go to $Y()$, but it could be any choice of 3 out of 6. For the sake of simplicity and to make our theorem and its proof shorter and easier to follow, we work with a fixed mapping of these 12 variables.

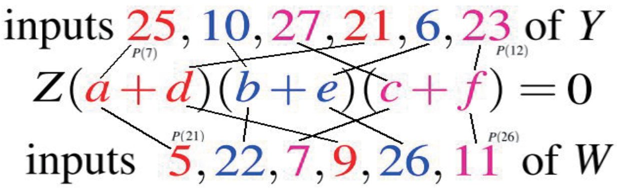

inputs 25, 10, 27, 21, 6, 23 of Y
P(7)
P(12)
Z(a + d)(b + e)(c + f) = 0
P(21)
P(26)
inputs 5, 22, 7, 9, 26, 11 of W

Fig. 6. For both W and Y we divide inputs in 3 sets of 2 variables in a consistent way.

5.2 A Concrete Example

This is for example achieved for the following full cipher wiring:

```
268: P=1,20,33,34,15,13,25,10,27,21,6,23,16,14,2,4,3,19,
35,29,5,22,7,9,26,11,17 D=16,28,24,20,32,8,12,4,36
```

and the following Boolean function $Z(a,b,c,d,e,f) = 1+a+b+bc+d+$

$$abd+cd+acd+bcd+e+ae+abe+ce+ace+de+ade+abde+af+bf+abf+acf+df+$$

$$bdf+abdf+cdf+bcdf+ef+abef+bcef+adef+abdef+acdef+abcdef$$

In Table 1 page 15 we show what happens as the number of round grows. This choice of Boolean function is in no way special: any Boolean function chosen at random will work with high probability of at least 2^{-8}, see Appendix A, or Appendix C in [16].

5.3 Proof of Thm. 5.1.1

We will show that a certain polynomial expression is invariant for any number of rounds. This for each of two encryptions we consider. The difference we study, $[7,11]$, is the same as flipping both bits active in our polynomial F. If we have $A^1 = c_A, B^1 = c_B, \ldots H^1 = c_H$ for the first encryption, for some constants $c_A, \ldots c_H \in \{0,1\}^8$, then we

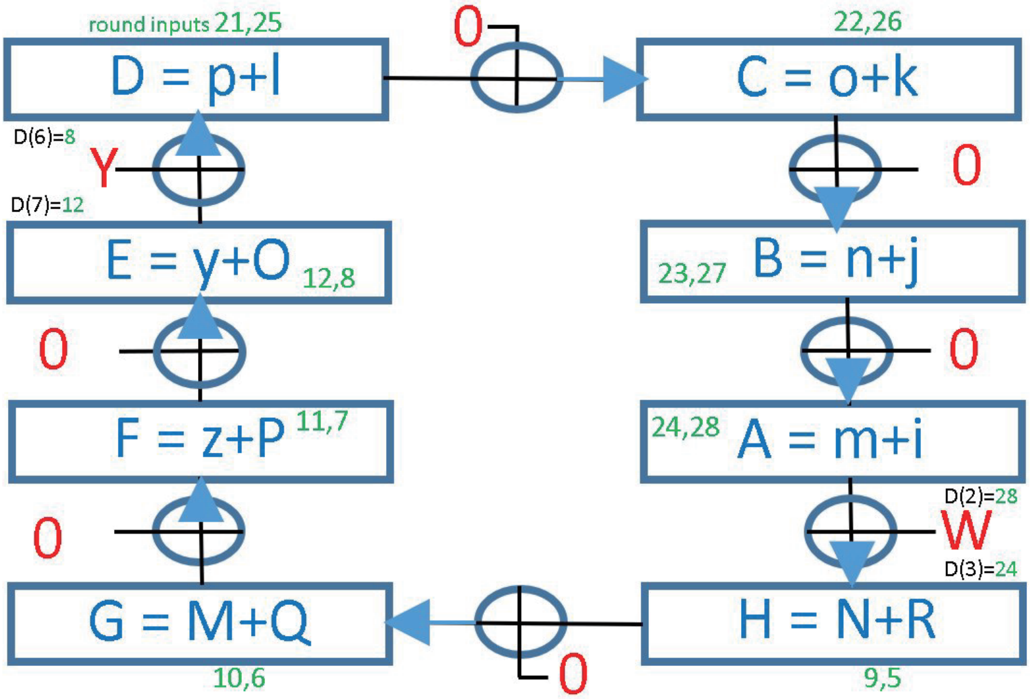


Fig. 7. A cycle on 8 basic polynomials used in our attack with LZS 268 which conceals the existence of a hidden polynomial invariant with $\mathscr{P} = ABCDEFGH$.

also have $A^2 = c_A, B^2 = c_B, \ldots H^2 = c_H$ for the second encryption. Since our hidden polynomial is built from $A, B, C, D, \ldots$ flipping bits $[7, 11]$ will also preserve this invariant, see Lemma 5.3.1 below. Two invariants will remain linked together for any number of rounds.

The fact that we have two invariants propagating for any number of rounds, which remains yet to be shown, makes that the difference (a bitwise XOR) between both encryptions is mapped to zero, through the linear application $\psi : \{0,1\}^{36} \to \{0,1\}^8$. Here ψ is defined precisely by the set of 8 linear polynomials $A \ldots H$ we defined earlier. This polynomial invariant attack is yet a weak constraint in itself. The fact that $\mathscr{P} = ABCDEFGH$ is an invariant in both encryptions makes that the output difference Δ after any number of rounds can take only 2^{28} possible values with $\psi(\Delta) = 0^8$, on 8 bits. It remains therefore quite surprising that one of these values, namely exactly $F = [7, 11]$ on 28+8 bits, is reproduced after any multiple of 8 rounds. This is 28 bits more than expected. Additional things must happen here for our theorem to be true. There is limited diffusion for a few rounds, and these is a finite number of possible output differences Δ which can at all be obtained from the initial difference $F = [7, 11]$. Since the image of the difference $\psi(\Delta)$, is fixed and strongly constrained, we expect that Δ takes fewer values than expected. In fact will show that Δ is fixed, only one value is possible. A rigourous proof with some technical lemmas is given below.

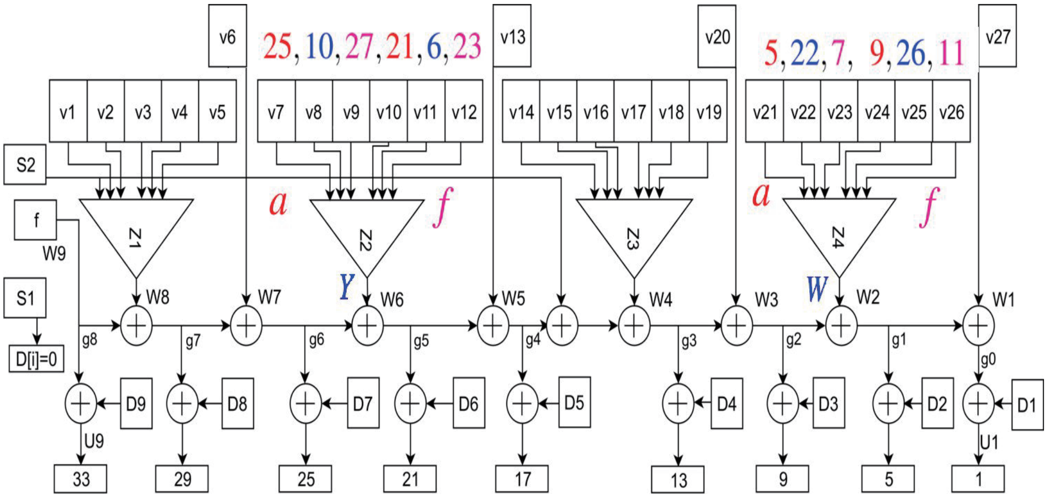


Fig. 8. Internal structure of one round of T-310 block cipher with focus on W and Y in our attack.

We will first prove that $\mathscr{P} = ABCDEFGH$ an invariant in both/any encryption.

Lemma 5.3.1. The polynomial $\mathscr{P} = ABCDEFGH$ is a non-zero polynomial and under conditions of Thm. 5.1.1 it is invariant after 1 round of encryption $\forall F,K,L \in \{0,1\}^3$.

Proof: We distinguish input and output-side polynomials by an index in the exponent such as A^o vs. A^i. We try to eliminate all output-side variables and express everything in input-side polynomials only. Later when there is no ambiguity we will just write A again instead of A^i.

By following the (shortest) path from output 9 to 5 in Fig. 8, or by XORing together the equations (r7) and (r8) in Fig. 3 we get:

$$H^o = y_9 + y_5 = x_{D(3)} + W(.) + x_{D(2)} = W(.) + x_{6\cdot 4} + x_{7\cdot 4} = W(.) + A^i$$

then following the path from output 25 to 21 in Fig. 8, or by XORing together the equations (r3) and (r4) in Fig. 3 we get:

$$D^o = y_{25} + y_{21} = x_{D(7)} + Y(.) + x_{D(6)} = Y(.) + x_{2\cdot 4} + x_{3\cdot 4} = Y(.) + E^i$$

At the input side $\mathscr{P}$ is equal to $\mathscr{P}^i = ABCDEFGH$ and at the output of our cipher

$$\mathscr{P}^o = A^oB^oC^oD^oE^oF^oG^oH^o = B^iC^iD^i(Y(.) + E^i)F^iG^iH^i(W(.) + A^i) =$$

at this moment only input variables are left and we can drop the exponents ^{i} and we have:

$$\mathscr{P}^o = BCD(Y(.) + E)FGH(W(.) + A) =$$

Now we observe that the inputs of $W()$ are $5, 22, 7, 9, 26, 11$, and our assumption $Z(a+d)(b+e)(c+f) = 0$ translated to $W(H)(C)(F) = 0$. Since HCF is a factor of $BCDFGH$ here, we can simply erase $W()$ as it is annihilated, and we get:

$$\mathscr{P}^o = BCD(Y(.) + E)FGH(A) =$$

Likewise, inputs of $Y()$ are $25, 10, 27, 21, 6, 23$, and therefore $Z(a+d)(b+e)(c+f) = 0$ translates to $Y(D)(G)(B) = 0$. Therefore we can also erase $Y()$ and we get:

$$\mathscr{P}^o = ABCDEFGH$$

which is the same as $\mathscr{P}^i$ and hence $\mathscr{P}$ is an invariant after 1 round of encryption. which ends the proof the our invariant work for any input and any F, K, L and any number of rounds. We have a formal equality of two polynomials. □

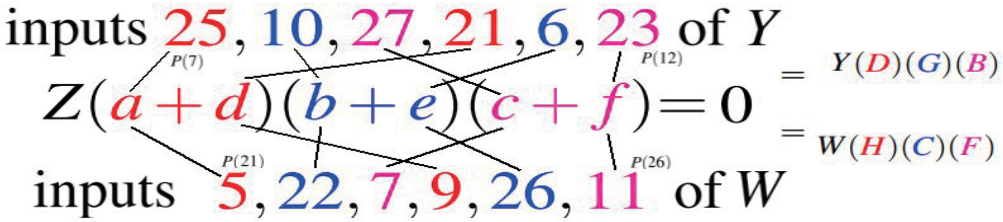

inputs 25, 10, 27, 21, 6, 23 of Y
P(7)
P(12)
Z(a + d)(b + e)(c + f) = 0
= Y(D)(G)(B)
= W(H)(C)(F)
P(21)
P(26)
inputs 5, 22, 7, 9, 26, 11 of W

Fig. 9. We map inputs of W and Y to 3 sets with 2 variables in a way consistent with our annihilation property. In some sense we get two annihilations for the price of one (amplification).

This was just a proof of our lemma. We need yet to show that $F = [7, 11]$ propagates in a certain way which implies our Thm. 5.1.1. In order to lower bound the propagation probability in general, we need to show that the propagation is special in some cases, so that the invariant $F = [7, 11]$ will be reproduced after 8 rounds, and we can ignore all other cases. It is easy to see that we have for any input I on 36 bits:

$$\mathscr{P}(I) = \prod_{i=1}^{8} (\psi(I))_i$$

which simply means that $\mathscr{P}$ is the same as applying a single 8-ary multiplication $\prod$ to the 8 outputs of ψ. More precisely we are going to show that:

Lemma 5.3.2. If for 2 different encryptions with $I_1 \oplus I_2 = [8, 12]$ of E we have

$$\mathscr{P}(I_1) = 1$$

then we have $O_1 \oplus O_2 = [21, 25]$ a.k.a. D after one round of encryption.

Proof: If $I_1 \oplus I_2 = [8, 12]$ and $\mathscr{P}(I_1) = 1$ then we also have $\mathscr{P}(I_2) = 1$ due to the fact that flipping both bits of $F = [8, 12]$ preserves all the values of $\psi()$ including the E coordinate, which is also unchanged due to double negation. We can then apply Lemma 5.3.1 and we obtain that $\mathscr{P}(O_1) = 1$ and $\mathscr{P}(O_2) = 1$ after one round for each respective encryption. If $\Delta = O_1 \oplus O_2$ we already know that $\psi(\Delta) = 0$. However Δ has 36 bits, not only 8.

We now observe that flipping 8,12 changes nothing else from the equations (r3) and (r4) in Fig. 3 we have

$$y_{25} = F + Z() + x_{P(6)} + x_{D(7)}$$

$$y_{21} = F + Z() + x_{P(6)} + Y() + x_{D(6)}$$

and that outputs of (r5) and all further equations in Fig. 3 are unchanged because, actually all the g_i in Fig. 8 are the same in both encryptions and the inputs $8, 12$ are used only once with $D(6)$ and $D(7)$, due to the fact that in Thm. 5.1.1 we assume that 8,12 are absent from the set of 27 outputs $\{P(1) \ldots P(27)\}$. Thus the only effect of flipping bits $E = 8, 12$ and is to flip bits $D = 21, 25$ in the next round. Similarly we have:

Lemma 5.3.3. If for 2 different encryptions with $I_1 \oplus I_2 = [24,28]$ from A we have

$$\mathscr{P}(I_1) = 1$$

then we have $O_1 \oplus O_2 = [5,9]$ a.k.a. H after one round of encryption.

Proof: If $I_1 \oplus I_2 = [24,28]$ and $\mathscr{P}(I_1) = 1$ then we also have $\mathscr{P}(I_2) = 1$ due to the fact that flipping both bits of $F = [24,28]$ preserves all the values of $\psi()$ including the A coordinate. We now observe that flipping 24,28 changes nothing else from the equations (r7) and (r8) in Fig. 3 we have

$$y_9 = F + Z() + x_{P(6)} + Y() + x_{P(13)} + L + X() + x_{P(20)} + x_{D(3)}$$

$$y_5 = F + Z() + x_{P(6)} + Y() + x_{P(13)} + L + X() + x_{P(20)} + W() + x_{D(2)}$$

and that outputs of all other equations in Fig. 3 are unchanged because and all internal values in Fig. 8 are the same in both encryptions except y_9 and y_5. This is because inputs $24,28$ are used only once with $D(2)$ and $D(3)$, due to the fact that in Thm. 5.1.1 we assumed that 24,28 are absent from the set of 27 outputs $\{P(1) \ldots P(27)\}$. Thus the only effect of flipping bits of $A = 24,28$ is to flip just bits of $H = 5,9$ in the next round.

So far, Lemmas 5.3.2 and 5.3.3 only cover 2 transitions out of 6 for 8 rounds. What if both bits of $F = [7,11]$ are flipped? Do they flip only $E = [8,12]$ inside the next round? This is not so obvious as these bits are inputs c,f of W and the output of W could change if we flip both. Now we have twice $Z(a+d)(b+e)(c+f) = 0$ in each encryption, which was already shown to imply $W(H)(C)(F) = 0$ and $Y(D)(G)(B) = 0$. in each encryption. Now if at the input side all the polynomials $ABCDEFGH$ are at 1, due to $ABCDEFGH = 1$, we conclude that outputs of W and Y must be zero. This carries on forever, again assuming $\mathscr{P}(I_1) = 1$ for the beginning round input. This also implies $\mathscr{P}(I_2) = 1$, as already seen in Lemma 5.3.2. If the value of W is zero in both encryptions, flipping two bits of $F = [7,11]$ has no effect on both Boolean functions W,Y.

Likewise, flipping bits $[21,25]$ has no effect, and likewise, for all the 6 possibilities corresponding to B,C,D and F,G,H knowing that cases of $E = [8,12]$ and $A = [24,28]$ were already covered by Lemmas 5.3.2 and 5.3.3 respectively. Overall we see that we can do a full circle, exactly as in Fig. 7), and the difference $F = [7,11]$ will after 8 round will become $F = [7,11]$ again, and all this because the polynomial invariant propagates and remains valid at each round input. More precisely we have in order

$$F \to E \to D \to C \to B \to A \to H \to G \to F$$

This ends the proof that the difference $[7,11]$ propagates with probability at least 2^{-8}.

□

Linear Spaces. It is easy to see that the same result holds for any linear combination of 8 basic differences $A = [24,28]$ to $H = [5,9]$ shown in Fig. 7. The set of anomalous differentials forms a linear space of dimension 8.

6 Computer Simulations and the Choice of the Boolean Function

Is our Thm. 5.1.1 confirmed by computer simulations? The question is really whether our cipher behaves like a typical Markov cipher (in approximation) outside of the proportion of 2^{-8} anomalous input states with $\mathscr{P} = 1$. The answer is yes as it seems. We show two "typical" cases, essentially chosen at random. Our first table is obtained with the exact Boolean function listed as an example after Thm. 5.1.1 in page 9.

Table 1. Probabilities observed with our Boolean function as the number of rounds grows.

rounds	8	16	24	32	40	48	56	64
proba	$2^{-2.40}$	$2^{-4.82}$	$2^{-6.74}$	$2^{-7.71}$	$2^{-7.95}$	$2^{-7.99}$	$2^{-8.00}$	$2^{-8.00}$

We see very clearly that, at the beginning, the probability grows exponentially, $2^{-4.82}$ is almost exactly the square of $2^{-2.40}$. Then, however, for 24 rounds there is already a substantial deviation: we would predict $2^{-3\cdot 2.40} = 2^{-7.20}$ and we obtain $2^{-6.74}$, a substantially lower result. The results vary very substantially for other Boolean functions which satisfy $Z(a+d)(b+e)(c+f) = 0$. For example, it is easy to see that if we add $(a+d+1)b$ to our Boolean function which works, we also obtain a function which works. In this case, the cipher is stronger and our differential property less visible, see Table 2.

Table 2. Probabilities observed with a stronger Boolean function.

rounds	8	16	24	32	40	48	56	64
proba	$2^{-4.53}$	$2^{-7.51}$	$2^{-7.98}$	$2^{-8.00}$	$2^{-8.00}$	$2^{-8.00}$	$2^{-8.00}$	$2^{-8.00}$

6.1 On Hiding Differentials

We conjecture that this sort of anomaly is not detectable if we have limited computing power or a limited number of samples. There are countless works about backdoors in block ciphers. In 1990s, authors typically concluded that this was infeasible and "hiding differentials" was claimed particularly difficult, Section 3.4. in [48]. The main idea in our work is that we do **not** need to hide high probability events. We hide low probability differentials, the probability of which can be as low as we want, if our invariant polynomial $\mathscr{P}$ had more than 8 factors. Therefore, it appears that we have discovered a valid method of concealing an attack inside a block cipher so that it is not easily detected. In our 2 examples above, we also see that the number of rounds where the propagation will stop decaying exponentially, and the anomaly becomes visible, is not constant and depends on the exact Boolean function used.

7 The Reciprocal Question, Nash Postulate, and Future Research

In this article, we show that with a well-chosen invariant property we can have a strong anomaly in the propagation of ordinary differentials in Differential Cryptanalysis (DC). The key observation is that the complexity of our attack does NOT tend to zero and remains constant for any number of rounds. The probability success first decreases, but eventually it becomes constant. In contrast, with ordinary DC, typically and in the "regular" Markov cipher case, we expect that the complexity will grow exponentially and eventually every differential will be "roughly equally likely" following [42]. An interesting question is whether intermediate cases are possible: where the probability of a single differential in a block cipher is **not constant** but grows polynomially or sub-exponentially with the number of rounds. This would violate the postulate of exponential complexity proposed by John Nash in his letter from 1955 exposed at NSA crypto museum, cf. [46]. More precisely Nash postulated that "For almost all sufficiently complex types of enciphering" where "different portions of the key interact complexly with each other in the determination of their ultimate effects" the computation cost should increase "exponentially with the length of the key". The words of Nash from 1955 are substantially older than modern block ciphers which were invented in 1970s, cf. [36, 27, 32, 24]. However, very clearly these words are what block cipher designers have been aiming at ever since. John Nash also had an intuition that this sort of strong or absolute security claim or result cannot be taken for granted, nor it can be proven in mathematics (today most security results are relative). He wrote: "The nature of this conjecture is such that I cannot prove it, even for a special type of ciphers. Nor do I expect it to be proven." In this article, we suggest that the Nash and many cipher designers were very optimistic and their security will sometimes increase at a slower rate than expected.

7.1 Some Conjectures - Differential Anomalies vs. Invariants

Moreover, we conjecture that there exists a third possibility, e.g. sub-exponential curve. In present work we show that sometimes, the success probability of a plain ordinary differential attack, does not decrease exponentially, when the number of rounds tends to infinity. The main reason for this is that there is more than just one property. A non-linear invariant property is present, and is acting behind the scenes distorting the input probability distribution forever, each time the differential property propagates. We can then wonder if some sort of reciprocal result exists. Maybe each time when a differential propagates with a probability which does not depend on the number of rounds, some sort of a non-linear invariant would be always present.

This conjecture seems quite strong. However, we do not see any other reason why differential cryptanalysis would behave in such a strongly anomalous way. The space of non-linear invariant attacks is in fact extremely large, and in this way maybe we can **efficiently discover** further new invariant attacks such as $\mathscr{P}$ in present article and possibly attacks more complex than just product attacks.

There is abundant literature about differential cryptanalysis, and it may seem that this topic is well understood. In this article, we show that this topic is not yet well understood and some major questions regarding how the attack could behave asymptotically, when the number of rounds grows, and why this happens, remain actually widely open.

7.2 Related Research - Special Contrived Ciphers

In [26] a toy cipher is presented which is not secure for as many as 2^n rounds, yet it is provably secure if we further increase the number of rounds. We generate the group of all possible permutations on n bits, cf. Appendix A and B in the extended version of [25]. In contrast, in our Thm. 5.1.1 the differential never vanishes, the cipher is not secure no matter how large is the number of rounds.

7.3 Weak is Beautiful - the World of Periodic Attacks and Weak Keys

It is a major misconception in cryptography research that the interesting attacks to study are those which work for every key. We claim that the special cases are the most interesting ones. Sometimes, they lead to spectacular improvements w.r.t. best attack known in the general case. In addition all differential and polynomial invariant properties we study here are periodic (with a period of 8).

This is particularly interesting in the context of block ciphers when the key scheduling is also periodic. In this (very common) case the key question is to exploit this periodicity and show that in some cases a large number of rounds can be broken for the price of breaking fewer rounds. In this precise sense, a periodic key schedule is a tremendous weakness with T-310, KeeLoq in [1, 2], in GOST, but not in DES. The best known single key attack on GOST with truncated differentials has a running time of 2^{179} in [29]. Now, if we study anomalous events with data encrypted with multiple random keys, the (imperfect) periodic structure of GOST is exploited better, and there exists an attack with total running time of 2^{101} in [33]. A wider comprehensive picture is shown in Section 29 in [10]. We see a near-continuous space with various attacks, improving as the proportion of weak keys goes down. Many of these attacks involve differentials. In T-310 the period in the key scheduling is 120, cf. Fig. 3, and our differential property of Thm. 5.1.1 has a period of 8 which divides 120. Unhappily keystream for encryption is extracted in T-310 with a different prime period, cf. Section 3 in [15] and key recovery could be difficult, see Appendix B. Interestingly, previous research has not exhibited differential anomalies as strong as in the present paper for ordinary single differentials. Overall, it appears that the question of weak keys in periodic block ciphers, and in particular the question of anomalous choice of constants (a weak long term key question), has yet not received sufficient attention.

8 Conclusion

In this paper we have demonstrated that the propagation of differentials inside a block cipher can in some cases be truly pathological. This is to the point that the complexity of the attack does not grow exponentially with the number of rounds, and that an arbitrarily large number of rounds can be attacked. After an initial period of quasi-exponential growth, which does not at all look unusual, cf. Table 1, the anomaly begins.

We see that block ciphers can become extremely weak due to a weaker cipher wiring. Interestingly, such modifications are officially allowed, in the sense of being 100 % compatible with the original T-310 encryption hardware. The long term key in T-310 took the form of a printed board, and was changed roughly once per year [21]. This result is particularly significant for T-310, a government encryption system, the hardware implementation cost of which is very large; thousands of times larger than with modern ciphers such as DES or AES, see [23]. However, increasing the number of rounds does not help if the complexity of an attack is constant and it works for an arbitrarily large number of rounds.

This paper is a proof of concept in just one case. We make the unthinkable happen, and show that this works beyond any doubt with a mathematical proof. We conjecture that this sort of anomaly is not detectable, if we have limited computing power or a limited quantity of encrypted data. We conjecture that this kind of Non-Markovian vulnerability exists also in other ciphers. If the hidden polynomial has a higher degree, it will become very hard to know if such a property is present or not, in any given cipher.

In comparison to an earlier result of this type presented at Crypto 2011, see [43], our Thm. 5.1.1 works with ordinary single differentials, for any key, and in spite of the presence of round constants in T-310. The vulnerability is principally a question of cipher wiring, which is without doubt very special. In contrast, no Boolean function should be considered to be resistant to our attack. Our vulnerability works with any Boolean function chosen at random with a probability of 2^{-8}, which is not at all small. Several works such as [16] and [17] show, that 100 % of Boolean functions are vulnerable against polynomial invariant attacks. Now we also have a similar result for ordinary differential cryptanalysis. The security of the whole block cipher cannot be taken for granted, cf. [47], just on the basis of avoiding high probability iterative differentials.

References

1. Gregory V. Bard, Nicolas Courtois, David Wagner: *Algebraic and Slide Attacks on KeeLoq,* In FSE 2008, pp. 97-115, LNCS 5086, Springer, 2008.
2. Gregory V. Bard and Nicolas T. Courtois: *Random Permutation Statistics and An Improved Slide-Determine Attack on KeeLoq,* in Quisquater Festschrift, LNCS 6805, pp. 35-54, Springer, 2012.
3. Gregory Bard, Nicolas Courtois, Jorge Nakahara Jr, Pouyan Sepehrdad and Bingsheng Zhang: *Algebraic, AIDA/Cube and Side Channel Analysis of KATAN Family of Block Ciphers,* In Indocrypt 2010, LNCS 6498, pp 176-196, Springer. `http://link.springer.com/chapter/10.1007/978-3-642-17401-8_14`
4. Eli Biham, Adi Shamir, *Differential Cryptanalysis of DES-like Cryptosystems,* Journal of Cryptology, vol. 4, pp. 3-72, IACR, 1991.
5. L.P. Brown, J. Seberry, *On the design of permutation P in DES type cryptosystems*. In Eurocrypt 89, LNCS 434, pp. 696-705. Springer, 1990.
6. Cagdas Calik and Meltem Sonmez Turan and Rene Peralta: *The Multiplicative Complexity of 6-variable Boolean Functions,* `https://ia.cr/2018/002.pdf`
7. Pascale Charpin: *Normal Boolean functions,* Journal of Complexity, vol. 20, Issues 2–3, pp 245–265, 2004.
8. Nicolas T. Courtois: *The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime,* In SECRYPT 2009 pp. 331-338. INSTICC Press 2009, ISBN 978-989-674-005-4.
9. Nicolas T. Courtois, Theodosis Mourouzis: *Propagation of Truncated Differentials in GOST,* In SECURWARE 2013, avail. at `http://www.thinkmind.org/download.php?articleid=securware_2013_7_20_30119`
10. Nicolas T. Courtois: *Algebraic Complexity Reduction and Cryptanalysis of GOST,* Monograph study on GOST cipher, 224 pages, available at `https://ia.cr/2011/626`.

11. Nicolas Courtois, Jerzy A. Gawinecki, Guangyan Song: *Contradiction Immunity and Guess-Then-Determine Attacks On GOST,* In CECC 2912, Tatra Mt. Math. Publ. Vol. 53 no. 3 (2012), pp. 65-79. `http://www.sav.sk/journals/uploads/0114113604CuGaSo.pdf`.
12. Nicolas T. Courtois, Marios Georgiou: *Variable elimination strategies and construction of nonlinear polynomial invariant attacks on T-310,* In Cryptologia, vol. 44, Iss. 1, pp. 20-38. At `https://doi.org/10.1080/01611194.2019.1650845`
13. Nicolas T. Courtois, Aidan Patrick, Matteo Abbondati: *Construction of a polynomial invariant annihilation attack of degree 7 for T-310,* In Cryptologia, vol. 44, Iss. 4, pp. 289–314, 2020.
14. Nicolas T. Courtois: *On the Existence of Non-Linear Invariants and Algebraic Polynomial Constructive Approach to Backdoors in Block Ciphers,* `https://ia.cr/2018/807`, last revised 27 Mar 2019.
15. Nicolas T. Courtois, Aidan Patrick: *Lack of Unique Factorization as a Tool in Block Cipher Cryptanalysis,* Preprint, `https://arxiv.org/abs/1905.04684` submitted 12 May 2019.
16. Nicolas T. Courtois: *Structural Nonlinear Invariant Attacks on T-310: Attacking Arbitrary Boolean Functions,* `https://ia.cr/2018/1242`, revised 12 Sep 2019.
17. Nicolas T. Courtois: *A nonlinear invariant attack on T-310 with the original Boolean function,* In Cryptologia, published online 23 Apr 2020, `https://www.tandfonline.com/doi/full/10.1080/01611194.2020.1736207`, to appear also in paper version in 2020.
18. Nicolas T. Courtois: *Invariant Hopping Attacks on Block Ciphers,* presented at WCC'2019, Abbaye de Saint-Jacut de la Mer, France, 31 March - 5 April 2019. Extended version available at `https://arxiv.org/pdf/2002.03212.pdf`, 8 February 2020.
19. Nicolas T. Courtois, Matteo Abbondati, Hamy Ratoanina, and Marek Grajek: *Systematic Construction of Nonlinear Product Attacks on Block Ciphers,* In ICISC 2019, LNCS 11975, pp. 20-51, Springer, 2020.
20. Nicolas Courtois: *Feistel Schemes and Bi-Linear Cryptanalysis,* in Crypto 2004, LNCS 3152, pp. 23–40, Springer, 2004.
21. Nicolas T. Courtois, Klaus Schmeh, Jörg Drobick, Jacques Patarin, Maria-Bristena Oprisanu, Matteo Scarlata, Om Bhallamudi: *Cryptographic Security Analysis of T-310,* Monography study on the T-310 block cipher, 132 pages, received 20 May 2017, last revised 29 June 2018, `https://ia.cr/2017/440.pdf`
22. Nicolas T. Courtois, Maria-Bristena Oprisanu: *Ciphertext-only attacks and weak long-term keys in T-310,* in Cryptologia, vol 42, iss. 4, pp. 316–336, May 2018. `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1362065`.
23. Nicolas Courtois, Jörg Drobick and Klaus Schmeh: *Feistel ciphers in East Germany in the communist era,* In Cryptologia, vol. 42, Iss. 6, 2018, pp. 427-444.
24. Nicolas T. Courtois: *Block Ciphers: Lessons from the Cold War,* slides presented at 2019 biennial Symposium on Cryptologic History, October 2019, Laurel, Maryland, US. At `http://www.nicolascourtois.com/papers/Feistel_East_Cold_War_US_Oct2019.pdf`
25. Nicolas Courtois: *The Inverse S-box, Non-linear Polynomial Relations and Cryptanalysis of Block Ciphers,* in AES 4 Conference, Bonn May 10-12 2004, LNCS 3373, pp. 170-188, Springer, 2005. `https://www.researchgate.net/publication/221005723_The_Inverse_S-Box_Non-linear_Polynomial_Relations_and_Cryptanalysis_of_Block_Ciphers`
26. Nicolas Courtois: *The Inverse S-box and Two Paradoxes of Whitening,* Long extended version of the Crypto 2004 rump session presentation, *Whitening the AES S-box,* `http://www.nicolascourtois.com/papers/invglc\_rump\_c04.pdf`.
27. Nicolas Courtois, Maria-Bristena Oprisanu and Klaus Schmeh: *Linear cryptanalysis and block cipher design in East Germany in the 1970s,* in Cryptologia, 05 Dec 2018, `https://www.tandfonline.com/doi/abs/10.1080/01611194.2018.1483981`

28. Nicolas Courtois: *The Best Differential Characteristics and Subtleties of the Biham-Shamir Attacks on DES*, On `https://ia.cr/2005/202`.
29. Nicolas Courtois: *An Improved Differential Attack on Full GOST,* in “The New Codebreakers – a Festschrift for David Kahn”, LNCS 9100, pp. 278-299, Springer, 2016.
30. Nicolas Courtois: *An Improved Differential Attack on Full GOST,* In Cryptology ePrint Archive, Report 2012/138. 15 March 2012, updated December 2015, `https://ia.cr/2012/138`.
31. Nicolas Courtois, Michał Misztal: *Aggregated Differentials and Cryptanalysis of PP-1 and GOST,* In CECC 2011, 11th Central European Conference on Cryptology. In Periodica Mathematica Hungarica Vol. 65 (2), 2012, pp. 11-26, Springer.
32. Nicolas T. Courtois, Theodosis Mourouzis, Michał Misztal, Jean-Jacques Quisquater, Guangyan Song: *Can GOST Be Made Secure Against Differential Cryptanalysis?,* In Cryptologia, vol. 39, Iss. 2, 2015, pp. 145-156.
33. Nicolas Courtois: *On Multiple Symmetric Fixed Points in GOST,* in Cryptologia, Iss. 4, vol 39, 2015, pp. 322-334.
34. Hans Dobbertin: *Construction of bent functions and balanced Boolean functions with high nonlinearity,* in: FSE’94, LNCS 1008, Springer, Berlin, pp. 61–74, 1994.
35. S. Dubuc: *Etude des propriétés de dégénérescence et de normalité des fonctions booléennes et construction de fonctions q-aires parfaitement non-linéaires,* Ph.D. Thesis, Université de Caen, 2001.
36. H. Feistel, W.A. Notz, J.L. Smith, *Cryptographic Techniques for Machine to Machine Data Communications,* Dec. 27, 1971, Report RC-3663, IBM T.J.Watson Research.
37. Jovan Golic, *Cryptanalytic Attacks on MIFARE Classic Protocol,* In CT-RSA 2013, LNCS 7779, pp. 239–258, Springer, 2013.
38. C. Harpes, G. Kramer, and J. Massey: *A Generalization of Linear Cryptanalysis and the Applicability of Matsui’s Piling-up Lemma,* Eurocrypt’95, LNCS 921, Springer, pp. 24–38.
39. C. Harpes, J. L. Massey: *Partitioning cryptanalysis,* in FSE 97, LNCS 1267, pp. 13–27, 1997.
40. Lars R. Knudsen: *Truncated and Higher Order Differentials,* In FSE 1994, pp. 196-211, LNCS 1008, Springer.
41. L.V. Kovalchuk: *Generalized Markov ciphers: evaluation of practical security against differential cryptanalysis,* in: Proc. 5th All-Russian Sci. Conf. MaBIT-06, 25-27 Oct. 2006, MGU, Moscow, pp. 595-599, 2006 [in Russian].
42. X. Lai, J. Massey, and S. Murphy: *Markov Ciphers and Differential Cryptanalysis,* In Eurocrypt 1991, LNCS 547, pp. 17-38, 1991.
43. G. Leander, M.A. Abdelraheem, H. AlKhzaimi, E. Zenner: *A cryptanalysis of PRINTcipher: The invariant subspace attack,* In Crypto 2011, LNCS 6841, pp. 206–221, 2011.
44. Lars R. Knudsen, Matthew J. B. Robshaw: *Non-Linear Characteristics in Linear Cryptoanalysis,* Eurocrypt’96, LNCS 1070, Springer, pp. 224–236, 1996.
45. James A. Maiorana: *A classification of the cosets of the Reed-Muller code R(1,6),* In Mathematics of Computation, 57(195):403–414, 1991.
46. John Nash, handwritten letters and documents relating to their evaluation, available at NSA crypto museum, at `cryptologicfoundation.org` and `https://www.nsa.gov/news-features/declassified-documents/nash-letters/assets/files/nash_letters1.pdf`, January-March 1955, declassified in 2012.
47. Kaisa Nyberg, Lars Ramkilde Knudsen: *Provable Security Against Differential Cryptanalysis,* In Crypto’92, pp 566–574, LNCS 740, Springer 1992.
48. Thomas Peyrin and Haoyang Wang: *The MALICIOUS Framework: Embedding Backdoors into Tweakable Block Ciphers,* In Crypto 2020, pp 249-278, LNCS 12172, Springer.
49. Referat 11: *Kryptologische Analyse des Chiffriergerätes T-310/50. Central Cipher Organ, Ministry of State Security of the GDR, document referenced as ‘ZCO 402/80’, a.k.a. MfS-Abt-XI-594, 123 pages, Berlin, 1980.*

50. Klaus Schmeh: The East German Encryption Machine T-310 and the Algorithm It Used, In Cryptologia, vol. 30, iss. 3, pp. 251–257, 2006.

51. Yosuke Todo, Gregor Leander, and Yu Sasaki: *Nonlinear invariant attack: Practical attack on full SCREAM, iSCREAM and Midori64,* In Journal of Cryptology, pp. 1–40, April 2018.

52. Michael Vielhaber: *AIDA Breaks BIVIUM (A&B) in 1 Minute Dual Core CPU Time,* In `https://ia.cr/2009/402`.

53. Richard Winter, Ana Salagean, Raphael C.-W. Phan: Comparison of Cube Attacks Over Different Vector Spaces. In IMACC 2015, pp. 225-238, LNCS 9496, Springer, 2015.

A On Boolean Function Vulnerability

It is possible to see that a Boolean function chosen at random will satisfy our exact property $Z(a+d)(b+e)(c+f)=0$ with probability 2^{-8}, cf. Section 5 in [13] and/or Appendix C in [16]. The result is the same as long as we have three linear factors which are linearly independent. In general, Boolean functions which are constant over large affine spaces are not an exception, it is systematic. 100% of Boolean functions in 6 variables are 3-normal and can be annihilated by a product of 3 affine polynomials. cf. Section 5 in [19] and [35]. We use another method to obtain the same result. It is sufficient to check all the 150357 classes of Boolean functions based on a database of Boolean functions of [6] based on earlier work by Maiorana [45].

Moreover, our experience shows that typically (when the Boolean function is balanced) both Z or $Z+1$ will admit numerous solutions of this type, some of which could work with an attack such as described in this paper.

Table 3. Classes of Boolean Functions with 6 Variables w.r.t. k-normality

total ↓ (any k)	k-normal Boolean functions			
k value →	6	≥ 5	≥ 4	≥ 3
150357	1	205	47446	150357
100%	$2^{-17.2}$	$2^{-9.52}$	$2^{-1.66}$	$2^{-0.0}$

Table 4. Classes of Boolean Functions with 6 Variables w.r.t. k-weak-normality

total ↓ (any k)	k-weakly-normal B. functions			
k value →	6	≥ 5	≥ 4	≥ 3
150357	1	205	93760	150357
100%	$2^{-17.2}$	$2^{-9.52}$	$2^{-0.68}$	$2^{-0.0}$

No Boolean function whatsoever should be assumed to be secure against the attacks such as described in this paper. For example with the original Boolean function used in T-310 we have $Zc(b+d)f=0$ and $Z(a+b)c(1+e)=0$ and many other relations of this type. From here it is possible to construct a product invariant attack on demand, using exactly one single relation like this, see [17]. In other words, just one such annihilation equation, which was not chosen by the attacker, can lead to an attack on T-310 working for any number of rounds. This is already for an invariant attack at order 1. Properties which involve two encryptions like in our Thm. 5.1.1 and the existence of multiple ways to annihilate polynomials further increase the freedom for the attacker.

B The Key Recovery Question

There exists multiple ways in which non-linear invariant attacks can be exploited in cryptanalysis in order to decrypt actual encrypted communications. This question was already studied in Section 9 in [16] and Section 6 in [12] and Section 6 in [13] and there are several distinct ways to approach this problem. Some invariants (not all) introduce pervasive biases made of higher order correlation properties which do not degrade as the number of rounds increases. Other invariants do directly involve some key bits. In some sense we expect that most invariants are NOT suitable for actual attacks, in the sense that other invariants are more suitable for various technical reasons.

B.1 New Ways to Exploit Polynomial Invariants

In this paper we discover a possibility to convert a non-linear invariant attack into a differential attack. This opens new possibilities for key recovery in 3 steps as follows. First, we guess some key bits, then, determine some internal values, finally, confirm through a statistical distinguisher. It is important to note that the question of which key bits should be guessed and which ones are determined, is a major practical combinatorial optimization problem in cryptanalysis. It leads to interesting security "metric" notions such as SAT immunity and UNSAT immunity, cf. [11].

B.2 Multiple Simultaneous Differentials and Cube Attacks

A more advanced method to enable key recovery would be to explore the rich world of cube attacks which is a form of a higher order differential attack. This type of discrete differential properties is much older than it is usually assumed, it was studied since at least 1976, cf. [24], and there are many flavours of cube attacks [52, 53]. It is quite rare that several differential properties can work simultaneously and that the overall combined probability remains very high. One example of this is with MiFare classic in [8, 37], and it happens again here. Our attack has 8 differences which form a linear space and could be used simultaneously in a variety of combined differential, invariant or/and cube attacks. An interesting question is then how quickly the complexity of such attacks increases as the number of rounds grows. Here we need to look at a new type of conditional cube attack: when a certain product of polynomials is at 1. We need to focus on cube properties which involve key bits, which cannot be taken for granted in general, cf. Section 4.1. in [3]. The space of possible attacks is enormous and we leave this for future research.