sciendo

TATRA MOUNTAINS
Mathematical Publications

DOI: 10.2478/tmmp-2019-0006
Tatra Mt. Math. Publ. **73** (2019), 61–82

HOW MANY WEAK-KEYS EXIST IN T-310 ?

Nicolas T. Courtois[1] — Matteo Scarlata[2] — Marios Georgiou[3]

[1]University College London, Gower Street, London, UNITED KINGDOM

[2]ETH Zurich, Department of Computer Science, Zürich, SWITZERLAND

[3]Latsia 2232, CYPRUS

ABSTRACT. T-310 is an important Cold War cipher. The cipher is extremely complex and it outputs extremely few bits from the internal state. A recent paper [Courtois, N. T.: *Decryption oracle slide attacks on T-310*, Cryptologia, **42** (2018), no. 3, 191–204] shows an example of a highly anomalous key such that T-310 can be broken by a slide attack with a decryption oracle. In this paper, we show that the same attacks are ALSO possible for regular keys which satisfy all the official KT1 requirements. Two other recent papers [Courtois, N. T.—Georgiou, M.—Scarlata, M.: *Slide attacks and LC-weak keys in T-310*, Cryptologia **43** (2019), no. 3, 175–189]; [Courtois, N. T.—Oprisanu, M. B.—Schmeh, K.: *Linear cryptanalysis and block cipher design in East Germany in the 1970s*, Cryptologia (published online), December 5, 2018] show that some of the KT1 keys are very weak w.r.t. Linear Cryptanalysis. In this paper, we show that a vast number of such weak keys exist and study the exact pre-conditions which make them weak. In addition we introduce a new third class of weak keys for RKDC (Related-Key Differential Cryptanalysis). We show that the original designers in the 1970s have ensured that these RKDC properties cannot happen for 4 rounds. We have discovered that these properties can happen for as few as 5 rounds for some keys, and for 10 to 16 rounds they become hard to avoid. The main reason why we study weak keys is to show that none of these properties occur by accident, rather that they are governed by precise pre-conditions which guarantee their existence, and countless other keys with the same properties exist. Eventually, this is how interesting attacks can be found.

1. Introduction

T-310 is an important historical cipher which was used in East Germany during the last period of the Cold War. According to [14], in 1989 there were some 3,800 T-310 cipher machines in active service in Eastern Germany.

2010 Mathematics Subject Classification: 13A50, 94A60, 68P25, 11T71, 14G50.
Keywords: Cold War, block ciphers, T-310, Block ciphers, unbalanced Feistel ciphers, linear cryptanalysis, generalised linear cryptanalysis, differential cryptanalysis, collision resistance, weak key attacks, related-key attacks.

1.1. Basic description of T-310

T-310 is a synchronous stream cipher which derives its keystream from the iteration of a relatively complex block cipher. The main component of T-310 is a keyed permutation which also takes an IV which we will call “the T-310 block cipher”. The block size in T-310 is 36 bits only, the secret key has 240 bits. The IV has 61 bits which are generated at random by the sender.

1.2. Encryption keys in T-310

T-310 has a long-term key a.k.a. LZS, in German *Langzeitschlüssel* which is valid for example for 1 year, and a short-term key on 240 bits which is valid and used for 1 week typically [9]. This key is stored on punch cards.

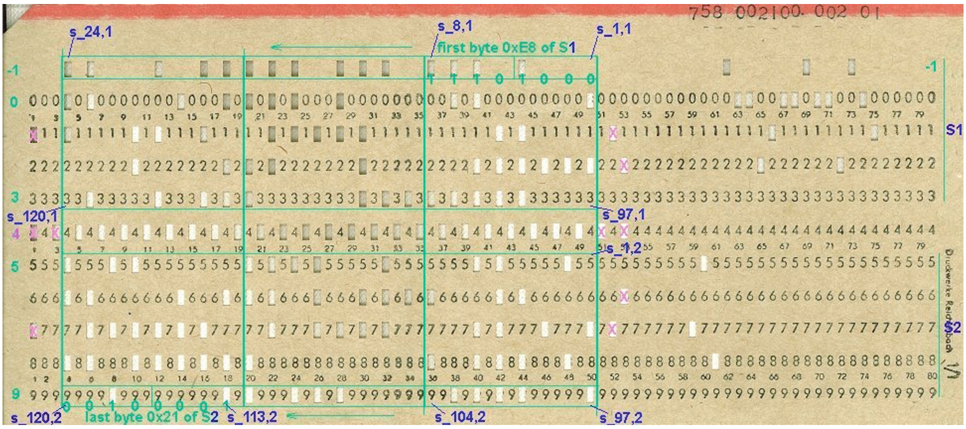

FIGURE 1. An example of an original historical key with details about encoding cf. [9].

The punch cards however are not kept inside the cipher machine. Instead the key is read and stored electronically in volatile memory inside the machine and the operator has no access to the key (!!!). Moreover, the machine has a “panic button” which allows to erase this memory, in order to decrease the chance of the capture of the key by the enemy. These details are relevant for fault attacks: electronically stored key could be subject to some electric faults, perturbations or instability during cipher operation. Then potentially the cipher could be restored to the normal operation: i.e., the fault would be corrected. In this paper, we show that such event are actually possible, cf. Section 5.

1.3. Encryption internals with T-310

The block cipher is not used directly to encrypt, but it is iterated a large number of times. Some $13 \cdot 127 = 1651$ block cipher rounds[1] are performed in order to extract as few as 10 bits called (B_j, r_j) from the cipher's internal state, which will then be used to encrypt just one 5-bit character of the plaintext by a sort of double one-time pad cf. Fig. 2.

The initial key is $s_{1-120,1-2}$ which is 240 bits. The key used in different encryption rounds repeats every 120 steps:

$$s_{m+120,1-2} = s_{m,1-2}.$$

In contrast the IV bits are expanded in an aperiodic way from an initial set of 61 bits chosen at random by the sender. The expansion is based on the following LFSR which produces a sequence with a very large prime [16] period of $2^{61} - 1$

$$f_i = f_{i-61} \oplus f_{i-60} \oplus f_{i-59} \oplus f_{i-56}.$$

This peculiar aperiodic expansion makes T-310 stronger than, for example, GOST, where the same permutation is repeated many times, which could lead to various self-similarity attacks.

1.4. Block cipher inside T-310

T-310 mandates a peculiar variant of a so-called "Contracting Unbalanced Feistel cipher" with 4 branches, cf. [13]. The original Feistel cipher construction had 2 branches and was invented around 1971 [10]. Then East German cipher designers had already in 1970s [14] mandated a substantially more complex structure. The actual connections depend on the so-called long-term key, a.k.a. LZS, in German *Langzeitschlüssel*. Recent research shows that some LZS may be vulnerable to certain attacks, but in general a well chosen LZS seem secure [7,8].

[1] The number of 13 iterations with 127 rounds each is what is specified in the main historical document [16] from 1980. There is some controversy whether in the actual encryption machines this have been modified and 13 maybe needs to be replaced by 14, see Appendix I.3. of [9]. This has a very small impact on research on T-310 and all known attacks translate in a straightforward way. In this paper, we will assume that we have 13 iterations and it appears that it makes no difference to any of claims or results inside this paper.

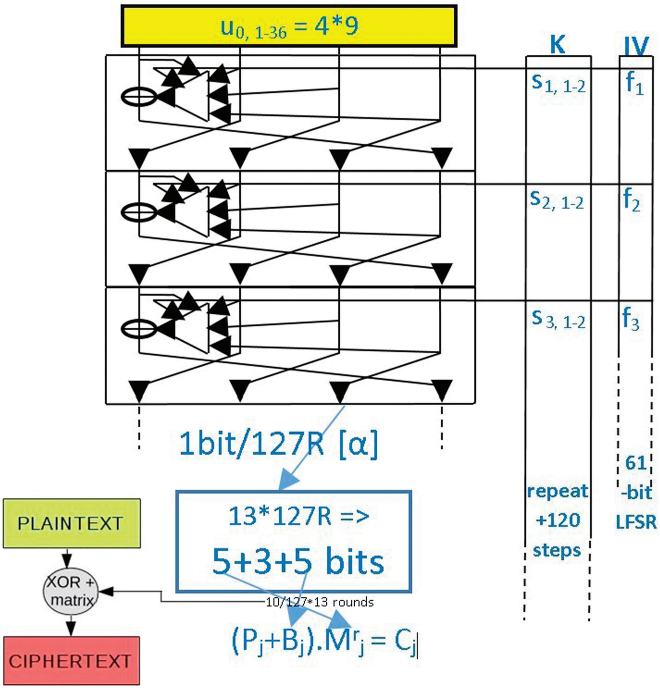

FIGURE 2. T-310 Cipher.

1.5. Inside the block cipher of T-310

Following [14] we denote by $u_{m,1-36}$ the 36-bit state of the cipher at moment $m = 0, 1, \ldots$ We denote by

$$\phi : \{0,1\}^3 \times \{0,1\}^{36} \to \{0,1\}^{36}$$

the function of one round. We have

$$(u_{m,1-36}) = \phi\left(s_{m,1}, s_{m,2}, f_m;\ u_{m-1,1-36}\right).$$

The numbering in the cipher is such that the bits numbered $1, 5, 9, \ldots, 33$ will be those created in one encryption round, and the bits numbered $4, 8, \ldots, 36$ are those which are replaced, and all the other bits get shifted by one position, i.e.,

$$u_{m+1,i+1} = u_{m,i} \quad \text{for any} \quad i \neq 4k.$$

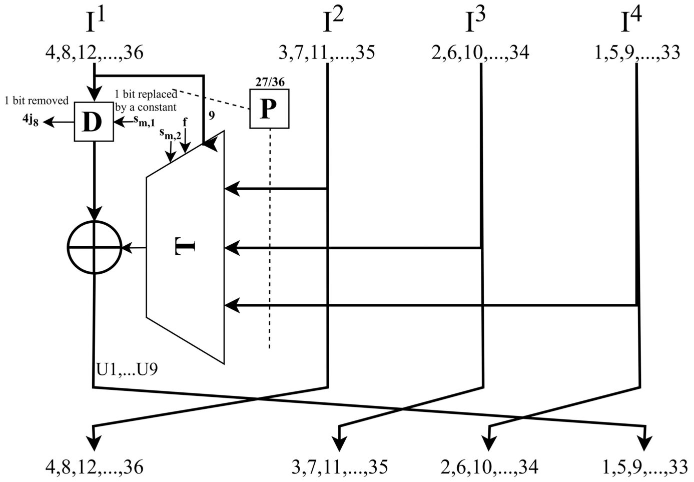

FIGURE 3. The internal structure of one encryption round for T-310 in the KT1 case.

1.6. One block cipher round ϕ

Let U_{1-9} be the 9 newly created bits. By definition after one round we have

$$(u_{m+1,1}, u_{m+1,5}, u_{m+1,9}, \ldots, u_{m+1,29}, u_{m+1,33}) = (U_1, U_2, U_3, \ldots, U_8, U_9).$$

It remains to specify how the U_{1-9} are computed inside one round. To cut a long story short, we recall from [8,9] that when $D(i) = 0$ (mandatory for KT1 keys) we assign input

$$u_{m,0} \overset{def}{=} s_{m+1,1}, \quad m \geq 0$$

which is a part of the secret key and a constant for any given round and that overall for all KT1 keys we have the following equations (1-9):

$$U_1 \oplus s_1 = U_2 \oplus u_{D(2)} \oplus u_{P(27)}, \tag{1}$$

$$U_2 \oplus u_{D(2)} = U_3 \oplus u_{D(3)} \oplus Z_4(u_{P(21-26)}), \tag{2}$$

$$U_3 \oplus u_{D(3)} = U_4 \oplus u_{D(4)} \oplus u_{P(20)}, \tag{3}$$

$$U_4 \oplus u_{D(4)} = U_5 \oplus u_{D(5)} \oplus Z_3(u_{P(14-19)}) \oplus s_2, \tag{4}$$

$$U_5 \oplus u_{D(5)} = U_6 \oplus u_{D(6)} \oplus u_{P(13)}, \tag{5}$$

$$U_6 \oplus u_{D(6)} = U_7 \oplus u_{D(7)} \oplus Z_2(u_{P(7-12)}), \tag{6}$$

$$U_7 \oplus u_{D(7)} = U_8 \oplus u_{D(8)} \oplus u_{P(6)}, \tag{7}$$

$$U_8 \oplus u_{D(8)} = U_9 \oplus u_{D(9)} \oplus Z_1(s_2, u_{P(1-5)}), \tag{8}$$

$$U_9 \oplus u_{D(9)} = f. \tag{9}$$

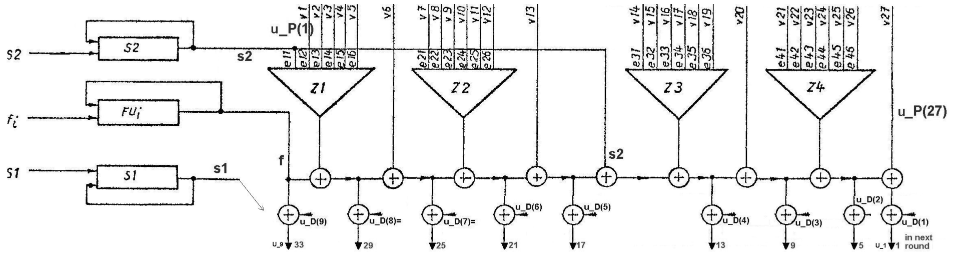

FIGURE 4. Internal structure of one round of T-310 based on original drawings [16].

Finally, in the above, Z are four identical copies of a Boolean function

$$Z : \mathbb{F}_2^6 \to \mathbb{F}_2$$

which is

$$\begin{aligned} Z(e_1, e_2, e_3, e_4, e_5, e_6) = {} & e_1 \oplus e_5 \oplus e_6 \\ & \oplus e_1e_4 \oplus e_2e_3 \oplus e_2e_5 \oplus e_4e_5 \oplus e_5e_6 \\ & \oplus e_1e_3e_4 \oplus e_1e_3e_6 \oplus e_1e_4e_5 \oplus e_2e_3e_6 \oplus e_2e_4e_6 \oplus e_3e_5e_6 \\ & \oplus e_1e_2e_3e_4 \oplus e_1e_2e_3e_5 \oplus e_1e_2e_5e_6 \oplus e_2e_3e_4e_6 \\ & \oplus e_1e_2e_3e_4e_5 \oplus e_1e_3e_4e_5e_6. \end{aligned}$$

1.7. How encryption is performed — double one-time pad

In this paper, we ignore the question how the encryption is performed. Extremely few bits extracted from the cipher state, 1 every 1651 rounds are used for the actual encryption. The exact single bit which is used for encryption is $U_{i,\alpha}$ for a fixed $\alpha \in \{1, \ldots, 36\}$ which can be viewed as a part of the long-term key LZS, and for certain i distant by multiples of 127 rounds. We refer to [9] for a detailed description. In KT1 specification there are also rules which forbid to use certain α values, cf. [9].

2. On three classes of weak keys

Numerous types of weak keys for T-310 exist and have been already studied [9]. This includes old Eastern-German sources which, for example, contain a list of various historical anomalous keys such as 27, which are very clearly marked as bad keys which should never ever be used [9].

In this paper, we study almost exclusively weak keys which are expected to be strong: i.e., weak keys which satisfy all numerous requirements for the so called KT1 keys specified by the designers cf. [16]. Such keys could have been approved for being used in actual government communications.

Cryptanalysis of such a cipher can be seen as a combinatorial constraint satisfaction problem: what are the constraints on $D()$ and $P()$, which will lead to particular weakness and attack. We call such constraints **pre-conditions**. This question requires numerous weak key classes to be studied one by one and determine the exact pre-conditions for each case. The ability to generate and validate such pre-conditions is an important task in cryptanalysis. Most of the results in this paper are of this type and have been constructed as paper and pencil mathematical proofs. Machine learning was also used for this purpose and the results were disappointing: the process is quite slow and not always accurate. Therefore we only present exact results with proofs. With pre-conditions it becomes easier to know if a specific attack can be compatible with the KT1 conditions or if two properties could be combined in an advanced attack.

3. On keys with alpha to alpha correlations

In [2] a slide attack on T-310 is presented. The possibility to execute this specific attack is restricted to the case where certain type of correlations exist, between the exact single bit which is used for encryption $U_{i,\alpha}$ and the same bits 7 round later $U_{i+7,\alpha}$. At this moment the attack surface seemed very very small. Not only we knew only one very special key such that this attack would work, but also this key was clearly very bad and could never been adopted or used by anyone: it is possible to see that for key 701 presented in [2], the round function is not bijective. In this paper, we do better: we show that the same sort of attack can be made to work for keys of type KT1[2]. For example, the key 741 is of type KT1, and has the same property also for $d = 7$ rounds. This shows that the attack presented in [2] is in fact a realistic attack which can break T-310 in a real-life setting, which is not at all obvious if we read [2].

```
701: P= 31,10,33,6,32,8,5,3,9,15,13,26,19,28,21,7,16,25,34,12,
        22,17,35,29,30,23,4;
     D= 4,2,17,32,12,35,0,24,20.

741: P= 15,24,33,27,19,12,5,22,9,31,3,7,8,34,21,36,32,25,18,28,
        35,20,4,29,16,14,2;
     D= 0,36,24,4,32,16,8,12,20.
```

[2] Therefore the round function is bijective cf. [7].

Here are the interesting correlations for these 2 keys:

TABLE 1. Some one-bit invariant correlations in T-310.

LZS nb	Rounds	Input → Output	Bias	Prop./Keys
701	7	[30] → [30]	$2^{-11.2}$	0.2
741	7	[29] → [29]	$2^{-4.4}$	TBC
741	7	[30] → [30]	$2^{-4.4}$	TBC
741	7	[31] → [31]	$2^{-4.4}$	TBC
741	7	[32] → [32]	$2^{-4.4}$	TBC

3.1. A short explanation for key 741

Here is a short explanation why key 741 has the properties stated above. First we observe that [29] → [30] → [31] → [32]. Then we are going to show that:

TABLE 2. A detailed explanation for key 741.

LZS nb	Rounds	Input → Output	Bias	Prop./Keys
741	3	[29] → [32]	$2^{-1.0}$	1.0
741	1	[32] → [10,17,25]	$2^{-3.0}$	1.0
741	3	[10,17,25] → [29]	$2^{-2.4}$	1.0

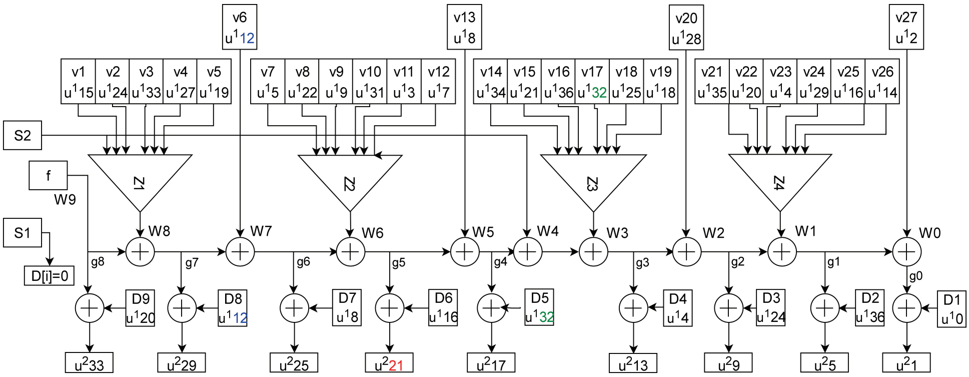

FIGURE 5. One round of T-310 for key 741.

(1) Let $X^{(j)}$ denote values inside round j.

(2) We observe that $P(13) = D(7) = 8$, therefore, $v13 = u_8^{(1)} = u_{D(7)}$. Then $D(5) = 32$. We have

$$u_{25}^{(2)} \oplus u_8^{(1)} \oplus Z2^{(1)}(v7 - v12) \oplus u_8^{(1)} \oplus u_{32}^{(1)} = u_{17}^{(2)}$$

here $u_8^{(1)}$ appears twice and is eliminated, and we have

$$Z2^{(1)}(v7 - v12) = u_{25}^{(2)} \oplus u_{32}^{(1)} \oplus u_{17}^{(2)}.$$

Now we add $u_9^{(1)}$ on both sides

$$Z2^{(1)}(v7 - v12) \oplus u_9^{(1)} = u_{25}^{(2)} \oplus u_{32}^{(1)} \oplus u_{17}^{(2)} \oplus u_9^{(1)}$$

and observe that this bit becomes number 10 in the next round

$$Z2^{(1)}(v7 - v12) \oplus u_9^{(1)} = u_{25}^{(2)} \oplus u_{32}^{(1)} \oplus u_{17}^{(2)} \oplus u_{10}^{(2)}.$$

Finally, we observe that $Z2$ is correlated to $u_9^{(1)}$ which is one of its inputs. Therefore, the following expression is biased

$$u_{32}^{(1)} \oplus u_{10}^{(2)} \oplus u_{25}^{(2)} \oplus u_{17}^{(2)}.$$

(3) Thus we have shown that we have $[32] \to [10, 17, 25]$ in one round.

(4) It remains to see that $[10, 17, 25] \to [29]$ in 3 rounds.

(5) After first 2 rounds bits $u_{10}^{(1)}, u_{17}^{(1)}, u_{25}^{(1)}$ become $u_{12}^{(3)}, u_{19}^{(3)}, u_{27}^{(3)}$ which are $v6, v5, v4$ inside 3rd round. Furthermore,

$$D(8) = 12 = P(6).$$

The output of $Z1^{(3)}$ is correlated to XOR of 2 of its inputs $u_{19}^{(3)} \oplus u_{27}^{(3)}$.

(6) Moreover, $f^{(3)} \oplus Z1^{(3)} \oplus u_{12}^{(3)} = u_{29}^{(4)}$. Thus we have

$$Z1^{(3)} \oplus u_{19}^{(3)} \oplus u_{27}^{(3)} = u_{29}^{(4)} \oplus f^{(3)}$$

and if the left hand side is biased, the right hand side is also biased.

Summary. We have shown that there exist KT1 keys with $\alpha \to \alpha$ correlations suitable for the attack described in [2]. Therefore this attack is not only theoretical.

4. On LC-weak keys

There exist numerous distinct classes of keys which are weak w.r.t Linear Cryptanalysis.

Definition 4.0.1 (LC-weak keys)**.** We say that a long-term key LZS is **LC-weak** if it exhibits at least one invariant linear characteristics true with probability 1.

An interesting question is whether keys which are compliant with KT1 specification can also be weak. We found that the answer is yes. There exist numerous classes of weak keys which we need to study one by one. Some examples are given in [8]. As a proof of concept two classes of such keys are detailed below.

4.1. A detailed example of how T-310 can be weak w.r.t. LC

Theorem 4.1.1 (A class of 2R properties). *For each long term key such that* $D(1) = 0$*,* $D(2) = 4$ *and* $P(27) = 6$ *and for any short term key on 240 bits, and for any initial state on 36 bits, we have the following two linear approximations* $[1, 2, 3] \to [2, 4, 6] \to [1, 2, 3]$ *which are true with probability exactly 1.0 for 2 rounds.*

Proof. We recall the first equation of Section 1.6. We replace U_1 and U_2 by $u_{m+1,1}$ and $u_{m+1,5}$ which is where these bits are connected in the next round

$$u_{m+1,1} = u_{D(1)} \oplus u_{m+1,5} \oplus u_{D(2)} \oplus u_{P(27)}.$$

We have $D(1) = 0$ which makes $u_{m,0} = s_{m+1,1}$ and $D(2) = 4$ and $P(27) = 6$. Therefore, we have

$$u_{m+1,1} = s_{m,1} \oplus u_{m+1,5} \oplus u_{m,4} \oplus u_{m,6},$$

and this leads to the following linear approximation for one round:

$$[4, 6] \to [1, 5] \;\; 1R \;\; P = 1.$$

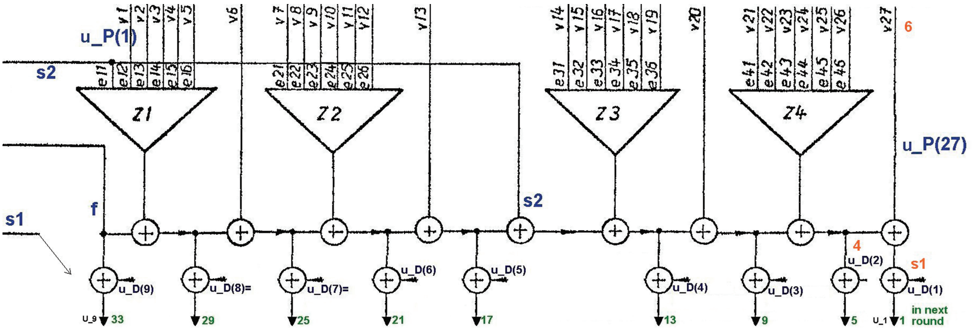

Figure 6. For convenience we show the bits involved here.

Using that fact that bits ≠ $4k$ are just shifted in our Feistel with 4 branches, this can be trivially extended for one earlier round as follows

$$[3, 5] \to [1, 5] \; 2R \; P = 1.$$

Finally, it is trivial to see that [1] → [2] → [3] for two rounds also with certainty, which property can be combined with the previous one and we obtain finally

$$[1,3,5] \to [1,3,5] \ 2R \ P = 1.$$

It follows that the same linear characteristic works for any even number of rounds. It is also easy to see that

$$[2,4,6] \to [2,4,6] \ 2R \ P = 1.$$

□

4.2. A second detailed example for 6 rounds

Here is another more complex result.

Theorem 4.2.1 (A class of 6R properties). *For each long term KT1 key such that $D(7) = 16$, $\{D(3)/D(4), P(20)\} \subset \{4, 8, 36\}$, $P(27) = 10$, and finally, $\{D(2), D(9)\} \subset \{28, 32\}$ and for any short term key on 240 bits, and for any initial state on 36 bits, we have the linear approximation* $[1, 5, 15, 33, s_1^{(6)}, f^{(6)}] \to [1, 5, 15, 33]$ *which is true with probability exactly 1.0 for 6 rounds.*

Proof. We will show that the following holds

Rounds	Input → Output	Probability
2	[1,5,15,33] → [3,7,25,29,35]	1.0
2	[3,7,25,29,35] → [9,13,27,31]	1.0
2	[9,13,27,31] → [1,5,15,33]	1.0

Let $X^{(i)}$ denote values inside round i. We recall a subset of equations from Section 1.6.

$$U_1 \oplus s_1 = U_2 \oplus u_{D(2)} \oplus u_{P(27)}, \quad (1)$$

$$U_3 \oplus u_{D(3)} = U_4 \oplus u_{D(4)} \oplus u_{P(20)}, \quad (3)$$

$$U_7 \oplus u_{D(7)} = U_8 \oplus u_{D(8)} \oplus u_{P(6)}, \quad (7)$$

$$U_9 \oplus u_{D(9)} = f. \quad (9)$$

First of all, we observe that [1] → [3], [5] → [7] and [33] → [35] for 2 rounds. We also see that [15] → [16] for 1 round. So

$$u_1^{(1)} = u_3^{(3)}, \quad u_5^{(1)} = u_7^{(3)}, \quad u_{33}^{(1)} = u_{35}^{(3)} \quad \text{and} \quad u_{15}^{(1)} = u_{16}^{(2)}.$$

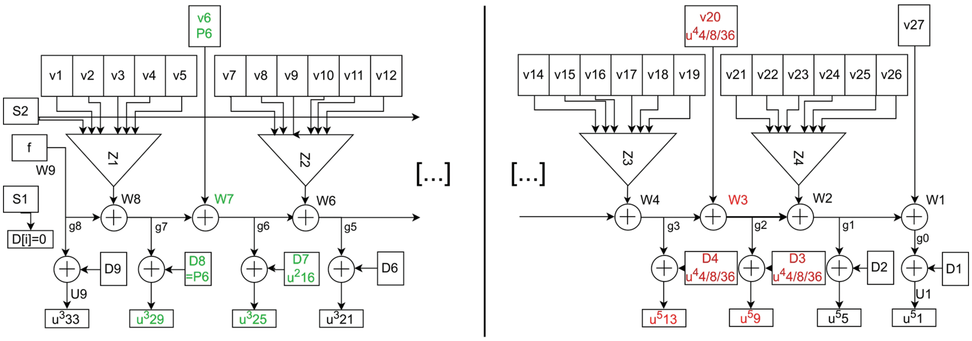

FIGURE 7. Explanations for our proof for key 706.

From the KT1 properties in [9], we know that for all KT1 keys $P(6) = D(8)$. We also assumed $D(7) = 16$. Hence, equation (7) becomes

$$u_{25}^{(3)} \oplus u_{29}^{(3)} = u_{16}^{(2)}.$$

Thus, we have $[16] \rightarrow [25, 29]$ for 1 round and, combining all the linear properties discussed so far,

$$[1, 5, 15, 33] \rightarrow [3, 7, 25, 29, 35] \qquad \text{for 2 rounds.}$$

Then we observe that

$$u_{25}^{(3)} = u_{27}^{(5)}, \quad u_{29}^{(3)} = u_{31}^{(5)}, \quad u_{3}^{(3)} = u_{4}^{(4)}, \quad u_{7}^{(3)} = u_{8}^{(4)} \quad \text{and} \quad u_{35}^{(3)} = u_{36}^{(4)}.$$

We assumed $\{D(3)/D(4), P(20)\} \subset \{4, 8, 36\}$. Therefore, equation (3) becomes

$$u_{4}^{(4)} \oplus u_{8}^{(4)} \oplus u_{36}^{(4)} = u_{9}^{(5)} \oplus u_{13}^{(5)}.$$

Thus, we have shown that

$$[3, 7, 25, 29, 35] \rightarrow [9, 13, 27, 31] \qquad \text{for 2 rounds.}$$

We recall that our goal is to show the following sequence of linear equalities:

$$[1, 5, 15, 33]s1f \rightarrow [2, 6, 16, 34] \rightarrow [3, 7, 25, 29, 35] \rightarrow$$
$$[4, 8, 26, 30, 36] \rightarrow [9, 13, 27, 31] \rightarrow$$
$$[10, 14, 28, 32] \rightarrow [1, 5, 15, 33].$$

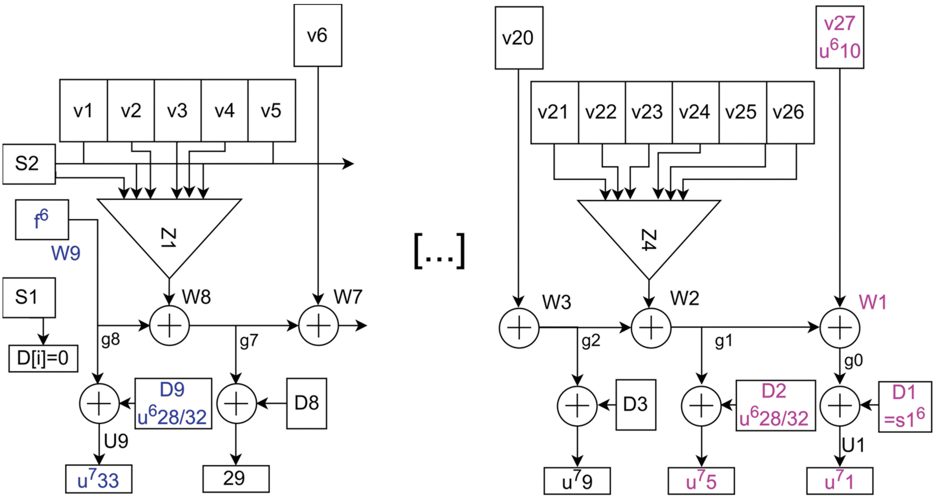

FIGURE 8. Further illustration for our proof.

It is clear that

$$u_{13}^{(5)} = u_{15}^{(7)}, \quad u_9^{(5)} = u_{10}^{(6)}, \quad u_{27}^{(5)} = u_{28}^{(6)}, \quad \text{and} \quad u_{31}^{(5)} = u_{32}^{(6)}.$$

The remaining conditions from the theorem 4.2.1 hypothesis are

$$P(27) = 10 \quad \text{and} \quad \{D(2), D(9)\} \subset \{28, 32\}.$$

Hence, equation (1) becomes

$$u_{10}^{(6)} \oplus s_1^{(6)} \oplus u_{D(2)}^{(6)} = u_1^{(7)} \oplus u_5^{(7)}$$

and equation (9) becomes $u_{D(9)}^{(6)} \oplus u_{33}^{(7)} = f^{(6)}.$

Finally,

$$u_{10}^{(6)} \oplus u_{D(2)}^{(6)} \oplus u_{D(9)}^{(6)} \oplus s_1^{(6)} \oplus f^{(6)} = u_1^{(7)} \oplus u_5^{(7)} \oplus u_{33}^{(7)}.$$

It follows that if

$$\{D(2), D(9)\} \subset \{28, 32\},$$

we have

$[10, 28, 32, s_1^{(6)}, f^{(6)}] \rightarrow [\,1,\ 5,\ 33\,]$ for 1 round.

Finally, we have also shown that

$[9, 13, 27, 31] \rightarrow [1, 5, 15, 33]$ for 2 rounds.

This ends the proof that if the conditions of the theorem are satisfied, we have

$[1, 5, 15, 33, s_1^{(6)}, f^{(6)}] \rightarrow [1, 5, 15, 33]$ for 6 rounds. □

4.3. How to use LC-weak keys in cryptanalysis?

For a long time an open problem was whether LC-weak keys can be used in cryptanalysis. One solution to this problem is presented in a new paper [6]. Not all key bits can yet be recovered by this method, therefore the question is not completely settled yet.

4.4. On frequency of LC-vulnerable KT1 keys

We have approximately $2^{83.2}$KT1 keys total, cf. Section 8.6. of [9] and [8]. Our computer simulations on generating and testing vast quantities of KT1 keys at high speed indicate that about 3.0 % of all KT1 keys are LC-weak. Some 10% or 0.3 % of the total are those of Section 4.1 In addition we found by a computer simulation that overall there exist many other similar classes of keys for a total of 3.0 % of all KT1 keys. We refer to another recent paper on this question which in particular shows that Linear Cryptanalysis was known and studied by the designers of T-310 in the 1970s, [8].

4.5. What about the other 97.0 % and non-linear invariants

We have seen that union of a number of results such as our Thm. 4.1.1 and Thm. 4.2.1 above leads overall to 3.0 % of all KT1 keys which are LC-weak and have linear invariant properties true with probability 1. An open important problem is to find an attack on any of the 97.0 % of KT1 keys resistant to Linear Cryptanalysis. We need to look at the question of **non-linear invariants** or Generalised Linear Cryptanalysis (GLC) [3, 11]. In a recent paper [4] we show that it IS possible to construct some non-trivial non-linear invariants for T-310.

4.6. A proof of concept - an example of a non-linear invariant

There are several very serious problems in constructing non-linear invariants and in the last 20 years in most cases research has failed to find suitable non-linear invariants, and it is not clear if they exist or not. We give one example of a non-linear invariant which is a proof of concept for GLC in T-310 setting. We consider the following polynomial invariant

$$\mathcal{P} = efg + efh + egh + fgh + fg.$$

It is possible to verify, cf. [4], that this invariant works when $F = 0$, $S1 = 0$ and $S2 = 0$ in one round and if we use the following long-term key :

```
317: P =  27,29,31,21,33,19,26,25,22,32,23,17,24,
          16,18,9,5,10,35,13,36,30,34,11,2,28,14.
     D =  17,25,26,35,18,34,30,32,28.
```

In addition, this works only for a special (weak) Boolean function

$$Z(a, b, c, d, e, f) = 1 + a + c + d.$$

and only for such quite weak Boolean functions.

An open important problem is to construct non-linear invariants which would be also resistant to Linear Cryptanalysis (which the example above already does) AND which would work not only when key and IV bits $F, S1, S2$ are fixed to 0, some solutions are provided in [4]. An open problem is to further do the same for either of any LZS which is of the form KT1 or when the round function is a bijection on 36 bits. None of these is true with 317 above but is possible in other cases, see our tutorial paper on this topic [4]. It remains an open problem to find a non-linear invariant attack on a real-life historical key. Another open problem is to find an invariant attack on any LZS which would have non-linear invariants and which would work with the original Boolean function, and which would have no simpler linear invariants such as linear invariants. One example of an attack where the Boolean function differs from the original by only one linear term we found after this paper had been written and can be found in [5].

In spite of all these, the very existence of non-linear invariants is an important discovery for T-310 which answers an open problem from Section 7 of [8]. They are subject to the exactly same methodology as in the present paper: with the right pre-conditions such as Thm. 4.1.1, the existence of the invariant can be guaranteed. One simple example of a pre-condition in the GLC case can be found in Section 7.6 in [4] showing that a specific weak key 827 does in fact lead to a larger class of weak keys, which is systematically the case.

We conjecture that up to 100 % of all KT1 keys will be vulnerable to non-linear invariants when the degree and complexity of these invariants increase. The number of non-linear invariants grows double-exponentially and a systematic exploration is not possible. Even for quadratic invariant the space of GLC attacks cannot be explored systematically: we have $2^{\binom{36}{2}} \approx 2^{600}$ possible invariants $\mathcal{P}$ to try. This is why at this moment extremely few working examples of non-linear invariants are known.

5. On collisions on the cipher state in T-310

A recent paper shows that if the round function ϕ is not bijective, the cipher can be broken in ciphertext-only scenario, cf. [7]. In this paper, we will only look at the hard case: when ϕ is bijective. We recall from [7, 9] that from a pure functional/encryption point of view, **nothing** forces ϕ to be invertible. Being able to compute the previous states of our T-310 generalized Feistel cipher variant, is **not** needed in the normal operation of the cipher. Bijectivity is a feature which makes the cipher substantially more secure cf. [7]. Mathematical proofs that the two main historical key classes KT1 and KT2 have bijective round functions are given in [8].

5.1. Vanishing differential attacks

One reason for ϕ to be bijective is that it prevents some quite strong attacks not only on T-310 cf. [7,9] but also on block ciphers at large. Most modern block ciphers have been built to specifically **avoid** such attacks and they are known under different names such as vanishing differentials, all-zero output difference attacks, cf. slide 253 in [1] and [3], a.k.a. collision attacks. In this paper, we consider one extension of the concept of vanishing collision attacks, where the attacker is in presence of [or can provoke] also some localised flips on the key bits. This implies that there are either some electrical faults inside the machine or that the attack is able to produce such faults, for example, by manipulating the power supply or injecting short electrical glitches at some wires which are accessible to him such as wires connecting the command unit with the cipher machine unit. It remains however an open problem how to exploit such events in cryptanalysis: if and how such keys could be used to recover the secret key.

5.2. Related key collision attacks

The following result - or requirement - is expected to hold for all good[3] long-term keys for T-310, cf. page 49 in [16].

Theorem 5.2.1 (Local injectivity result for ϕ^4)**.** *For four rounds ϕ^4 if we fix the block input u on 36 bits, and vary the 12 of the key and IV bits, we obtain 2^{12} pairwise distinct $\phi(u)$ values on 36 bits.*

A similar result also holds for 1,2 and 3 rounds of T-310, with 2^{3n} images cf. page 49 in [16]. Then it does NOT hold for 5 rounds, and we show here some counter-examples. We have found the following KT1 key which we will call 716 and another similar key 722:

```
716: P = 16,6,33,11,20,24,5,13,9,7,31,19,36,12,
         21,30,34,25,17,32,23,28,4,29,26,8,3.
     D = 0,4,16,28,12,20,36,24,8.

722: P = 15,11,33,28,27,8,5,30,9,24,35,22,16,34,
         21,18,7,25,12,36,14,20,4,29,32,1,17.
     D = 0,4,28,32,12,20,16,8,24.
```

For these keys there exist differentials on the key only, which can be annihilated leading to no difference on the full 36-bit state of the cipher, this for only 5 rounds. This is closely related to the notion of "missing bits" in T-310, studied in [9]. We observe that several bits of the state are not equal to any

[3] It is not entirely clear if these statements and many other found in Chapter III in [16] are **actual** properties (claims/lemmas) or just **desirable** properties (e.g., security requirements). There is no justification (or mathematical proofs) provided, and it is not clear which exact long-term keys are concerned by this property.

of the $P(j)$ and these bits are inevitably **not used** in the round function inside next round of T-310. This allows certain differentials to remain constrained and to "propagate" more easily which makes related-key differential attacks somewhat easier than expected, cf. [9].

TABLE 3. Missing bits for some keys vulnerable to related-key differential attacks.

LZS nb	Bits which are not used in $P(j)$
716	1, 2, 10, 14, 15, 18, 22, 27, 35
722	2, 3, 6, 10, 13, 19, 23, 26, 31

Notation. In this paper, we use very compact notations in order to represent our related-key collision events. For example, the notation $1, 2 > 3$ means that a differential at a certain round i occurs only on bits $1, 2$ out of 1-36 possible, and in the next round only on bit 3. All the other bits are unchanged. Furthermore we can extent this notation with key bits, for example, $s1 > 1$ indicates that a difference on a secret key bit $s1$ inside one round (there is only one such bit per round) provokes a difference on the cipher state entering the next round at bit 1. If both events occur in the same round we use commas like $2 > 3, s1 > 4$ meaning that in the middle round both keys and the cipher states are not identical in two encryptions.

Observations on key 716. With these notations, the exact form of internal differential that is eventually annihilated by some differences on key bits during the two encryptions is $1 > 2 > 3 > 4$. For example, we have observed the following types of events with key 716: we have $s1 > 1 > 2 > 3, s1 > 4, s1$. Overall the two states become identical after only 5 rounds. This is quite unusual and 716 is an example of an exceptionally weak KT1 key. This sort of properties were a subject of considerable care by the designers of T-310, see Thm. 5.2.1 which states that the same result should not hold for 4 rounds.

5.3. A detailed example

More precisely, we have the following sequence of events for 5 rounds:

1) In the 1st round, the difference on key bit $s1$ becomes a difference on $U_1 = u_1$, cf. Fig. 9 page 79. A formal explanation is as follows. We have

$$U_1 = u_{D(1)} \oplus U_2 \oplus u_{D(2)} \oplus u_{P(27)}$$

following the first equation (1) in Section 1.6. Then we have

$$s1 = u_0 \quad \text{and} \quad D(1) = 0$$

and we obtain

$$U_1 \oplus s_1 = U_2 \oplus u_{D(2)} \oplus u_{P(27)}.$$

The right hand side does not change and a flip on key bit $s1$ in round 1 will affect bit u_1 at the input of the second round. Accordingly bit 1 and only this bit is flipped after the first round.

2) Then inside round 2, according to Table. 3 this input bit 1 is NOT used, it does NOT enter the round function, and it simply becomes bit 2 [this is, a substantial weakness]. Thus only bit 2 is flipped after the 2nd round.

3) Then in round 3, according to Table. 3 this bit 2 is still NOT used otherwise than it becomes bit 3. Thus only bit 3 is flipped after the 3rd round. We have the following differential characteristic $s1 > 1 > 2 > 3$.

4a) Then in round 4, we have $P(27) = 3$ and bit 3 is used. Again we have $U_1 \oplus s_1 = U_2 \oplus u_{D(2)} \oplus u_{P(27)}$ so the only thing a difference 1 on bit 3 would do is to flip the bit $T_9 = U_2 \oplus u_{D(2)} \oplus u_{P(27)}$ which will be annihilated by a flip in bit $s1$ inside the same round and overall the bit u_1 is not flipped after round 4. We have $s1 > 1 > 2 > 3, s1$.

4b) At the same time, the flip will still be copied from wire u_3 which becomes u_4 now. We have $s1 > 1 > 2 > 3, s1 > 4$.

5a) Then in round 5, we have a difference on the entering bit 4. The construction of T-310 prevents this from being cancelled too easily. We have $P(23) = 4$ which is one of the inputs s_4 of Z_4 in 4th round. A detailed examination of the truth table of $Z()$ shows that the difference on bit s_2 is cancelled with probability close to 1/2 **no matter what all the other 5 input bits are** in each case, systematically and uniformly[4] over such choices.

5b) At the same time we have $D(2) = 4$. In the fifth round the bit 4 has another effect: it would normally flip u_1, except for that we have again $U_1 \oplus s_1 = U_2 \oplus u_{D(2)} \oplus u_{P(27)}$, and this modification can be cancelled by flipping bit $s1$ inside the 5th round.

!!) Overall our differential is extinguished with probability 1/2 over 5 rounds as follows: $s1 > 1 > 2 > 3, s1 > 4, s1$.

[4] This is quite surprising, and due to the requirement (3) listed on page 53 of [15], and in Section 3.3. of [8] which is as follows:

$$|\{X \in \{0,1\}^6 | Z(X_1, \dots, X_i, \dots, X_6) = Z(X_1, \dots, X_i \oplus 1, \dots, X_6)\}| \approx 2^5, \quad i = 1, \dots, 6. \tag{3}$$

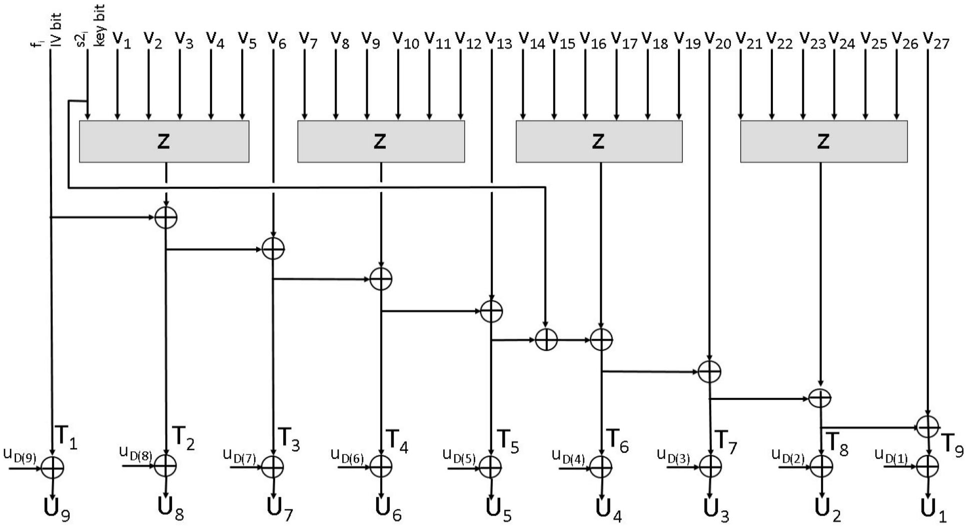
f_i
IV bit
$s2_i$
key bit
V_1 V_2 V_3 V_4 V_5 V_6 V_7 V_8 V_9 V_{10} V_{11} V_{12} V_{13} V_{14} V_{15} V_{16} V_{17} V_{18} V_{19} V_{20} V_{21} V_{22} V_{23} V_{24} V_{25} V_{26} V_{27}
Z
Z
Z
Z
T_1 T_2 T_3 T_4 T_5 T_6 T_7 T_8 T_9
$u_{D(9)}$ $u_{D(8)}$ $u_{D(7)}$ $u_{D(6)}$ $u_{D(5)}$ $u_{D(4)}$ $u_{D(3)}$ $u_{D(2)}$ $u_{D(1)}$
U_9 U_8 U_7 U_6 U_5 U_4 U_3 U_2 U_1

FIGURE 9. The internal structure of $T()$ inside one round of T-310.

5.4. A general result

From the above we see immediately that

THEOREM 5.4.1 (A 5-round related-key differential). *The extinguishing related-key differential property $s1 > 1 > 2 > 3, s\,1 > 4, s1$ works for each long term key such that $D(1) = 0$, $D(2) = 4$, $P(23) = 4$ and such that $\forall_j P(j) \notin \{2, 3\}$. For such LZS, the property is triggered by imposing the $s\,1$ key difference for 5 rounds is 0x19, and for any $s\,2$ key, for any IV, and for any cipher state on 36 bits and the differences are extinguished after 5 rounds with probability almost exactly equal to 1/2, cf. requirement (3) above.*

TABLE 4. Some LZS vulnerable to related-key differential attacks.

LZS nb	Related-key differential trail
716	$1 > 2 > 3 > 4$

Remark. A similar yet weaker result could be obtained for key 722. In this case, the differential property is rather $s1 > 1 > 2 > 3 > 4, s1$ and the difference on $s1$ key bits is $0\,x\,11$ which has only 2 active bits as we do longer need to flip a bit at round 4 as $P(27) \neq 3$ and bit 3 is not used. The propagation probability is 1/4, half of the previous result, due to the fact that in round 2 bit 1 is used as input of Z_4 with $P(26) = 1$, therefore, the property (3) is used twice.

5.5. Weak keys which combine LC-weakness with RKDC

To illustrate this we found that there exist keys which are simultaneously very weak w.r.t. LC and RKDC, for example, key 718.

```
718: P = 3,18,33,12,36,8,5,27,9,19,14,23,20,16,
         21,26,7,25,31,28,32,15,4,29,24,22,6.
     D = 0,4,36,12,24,16,20,8,32.
```

5.6. How many RKDC weak keys exist

We found that this sort of weak keys are almost inevitable. If we increase the number of rounds, the percentage of weak keys increases. At 16 rounds, nearly 100 % of keys are weak including the actual historical keys used in real life.

6. Conclusion

T-310 is an important Cold War cipher. Cryptanalysis of such a cipher can be seen as a combinatorial constraint satisfaction problem: find some constraints or pre-conditions on $D()$ and $P()$ leading to particular weakness and attack which would also be compatible with the KT1 conditions which are required by the designers. This question requires numerous weak key classes to be studied one by one. In this paper, we studied three major classes of weak keys. For each class we attempt to construct also KT1 keys which would be weak. Our first contribution is to show that there exist KT1 keys with 1 bit correlations. Our second contribution is to show that LC-weak keys can be constructed step by step rather than found at random, and that we can compute precise pre-conditions which allow each type of weak keys to exist, cf. Thm. 4.1.1 and Thm. 4.2.1. Our third contribution is a new class of weak keys with related-key differential properties. We found that up to 100 % of T-310 long-term keys are vulnerable w.r.t. this new class of weak keys.

In contrast only 3.0 % of all KT1 keys have linear invariant properties true with probability 1. What about the other 97 % of KT1 keys? A recent paper [4] shows how to construct some non-linear invariants for T-310. In this paper, we provide one example and a proof concept. Most non-linear invariants known at this moment are very far from being relevant or satisfactory. They are just special. An important open problem is to construct non-linear invariants which are of type KT1. If KT1 does not protect against linear invariants, we see no reason why it would protect against their direct generalizations. However this has yet to be demonstrated. We conjecture that the vulnerability of this cipher to non-linear invariants increases as the degree of these invariants increases and we conjecture that possibly it approaches 100 % as the degree of invariants grows. It could however also stagnate somewhere very near the 3 %. We have interesting new open problems to study.

Applications. An interesting question is if any of our weak keys can be used in cryptanalysis and how. Very few can, and if this works, not all key bits can be recovered, cf. Section 4.3 and [6,9]. One method to actually break T-310 would be to combine more than one vulnerability in one single long-term key. To illustrate this we show that there exist keys which are simultaneously very weak w.r.t. LC and RKDC, cf. our example in Section 5.5.

REFERENCES

[1] COURTOIS, N. T.: : *Cryptanalysis of GOST*, (a very long extended set of slides about the cryptanalysis of GOST, 2010–2014),
`http://www.nicolascourtois.com/papers/GOST.pdf`; (An earlier and shorter version was presented at 29C3 Conference at 29th Chaos Communication Congress (29C3), December 27–30, 2012, in Hamburg, Germany).

[2] ______ *Decryption oracle slide attacks on T-310*, Cryptologia, **42** (2018), no. 3, 191–204;
`http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1362062`

[3] ______ *Data Encryption Standard (DES)* (slides used in GA03 Introduction to Cryptography and later in GA18 course Cryptanalysis taught at University College London), 2006–2016;
`http://www.nicolascourtois.com/papers/des_course_6.pdf`

[4] ______ *On the Existence of Non-Linear Invariants and Algebraic Polynomial Constructive Approach to Backdoors in Block Ciphers*, Report 2018/807;
`https://eprint.iacr.org/2018/807.pdf`

[5] ______ *Structural Nonlinear Invariant Attacks on T-310: Attacking Arbitrary Boolean Functions*, Cryptology ePrint Archive, Report 2018/1242;
`https://ia.cr/2018/1242`

[6] COURTOIS, N. T.—GEORGIOU, M.—SCARLATA, M.: *Slide attacks and LC-weak keys in T-310*, Cryptologia**43** (2019), no. 3, 175–189.

[7] COURTOIS, N. T.—OPRISANU, M. B.: *Ciphertext-only attacks and weak long-term keys in T-310*, Cryptologia, **42** (2018) no. 4, 316–336;
`http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1362065`

[8] COURTOIS, N. T.—OPRISANU, M. B.—SCHMEH, K.: *Linear cryptanalysis and block cipher design in East Germany in the 1970s*, Cryptologia, December 5, 2018; Published online: `https://www.tandfonline.com/doi/abs/10.1080/01611194.2018.1483981`

[9] COURTOIS, N.T.—SCHMEH, K.—DROBICK, J.—PATARIN, J.—OPRISANU, M.-B.—SCARLATA, M.—BHALLAMUDI, O.: *Cryptographic Security Analysis of T-310*, Monography study on the T-310 block cipher, 132 pages;
`https://eprint.iacr.org/2017/440.pdf`

[10] FEISTEL, H.— NOTZ, W. A.—SMITH, J. L.: *Cryptographic Techniques for Machine to Machine Data Communications*. Report RC-3663, IBM T. J. Watson Research, Yorktown, Heights, N.Y., December 27, 1971.

[11] HARPES, C.—KRAMER, G.—MASSEY, J.: *A generalization of linear cryptanalysis and the applicability of matsui's piling-up lemma*. In: Eurocrypt'95, Lecture Notes in Comput Sci. Vol. 921, Springer-Verlag, Berlin, 1995. pp. 24–38.

[12] MATSUI, M.: *Linear cryptanalysis method for des cipher*. In: Eurocrypt'93, Lecture Notes in Comput Sci. Vol. 765, Springer-Verlag, Berlin, 1993, pp. 386–397.

[13] PATARIN, J.—NACHEF, V.—BERBAIN, B.: *Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions*. In: Asiacrypt 2006, Lecture Notes in Comput Sci. Vol. 4284, Springer-Verlag, Berlin, 2006, pp. 396–411.

[14] SCHMEH, K.: *The East German Encryption Machine T-310 and the Algorithm It Used*, In Cryptologia, vol. 30 (2006), no. 3, 251–257.

[15] *Document MfS-Abt-XI-183*, (a documentation of SKS V/1 contains a selection of pages extracted from a larger document known as MfS-020-Nr. 747/73), 1973.

[16] *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, Berlin, 1980, 123 pages.

Received October 10, 2018

Nicolas T. Courtois
University College London
Gower Street
London
UNITED KINGDOM
E-mail: courtois@minrank.org
n.courtois@bettercrypto.com

Matteo Scarlata
ETH Zurich
Department of Computer Science
Universitätstraße 6
Building CAB
8092 Zürich
SWITZERLAND
E-mail: scmatteo@ethz.ch

Marios Georgiou
4 Miltiadous street
Latsia 2232
CYPRUS
E-mail: co.mariosgeorgiou@gmail.com