Slide Attacks and LC-Weak Keys in T-310

Nicolas T. Courtois[1], Marios Georgiou[1], and Matteo Scarlata[2]

[1]University College London, Gower Street, London, UK
[2]Master student at ETH Zurich

Abstract. T-310 is an important Cold War cipher [Cryptologia 2006]. In a recent article [Cryptologia 2018], researchers show that in spite of specifying numerous very technical requirements, the designers do not protect the cipher against linear cryptanalysis and some 3 % of the keys are very weak. However such a weakness does not necessarily allow to break the cipher, because it is extremely complex and extremely few bits from the internal state are used for the actual encryption. In this article we finally show a method which allows to recover a part of the secret key for about half of such weak keys in a quasi-realistic setting. For this purpose we revisit another recent article from Cryptologia from 2018 and introduce a new peculiar variant of the decryption oracle slide attack with $d = 0$.

Key Words: Cold War, block ciphers, T-310, unbalanced compressing Feistel ciphers, linear cryptanalysis, weak key attacks, slide attacks, decryption oracle, SAT solvers.

1 Introduction

T-310 is an important historical cipher which was used in East Germany during the last period of the Cold War cf. [1, 4, 15] and shortly before the German reunification there were some 3,800 of T-310 cipher machines in active service.

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, is generated at random by the sender and transmitted in clear text. 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 [4]. This key is stored on punch cards.

1.1 Recent Research - Long Term Keys And Security

Eastern German cipher designers have very carefully engineered a complex set of conditions known as KT1, which the LZS must satisfy. A recent article contains a mathematical proof that the KT1 spec implies resistance to a particularly powerful ciphertext-only attack [5]. Does this mean that keys which satisfy the KT1 conditions are secure? Not quite! A recent article yet to appear in Cryptologia in 2018 [6] shows that a proportion of about 3 % of all KT1 keys can exhibit linear properties true with probability 1. However the question HOW at all these properties of [6] can be used in cryptanalysis remained open. This is because the

T-310 encryption mode is extremely strong: only up to 1 bit of the cipher state for every 127 rounds of the block cipher is used for the actual encryption. In this article we will show that for a good proportion of these 3 % of KT1 keys there is a way to exploit them in key recovery attacks. We are going in fact to propose a new simple variant of a decryption oracle slide attack such as recently described in [3] and this allows eventually to exploit some of the weak LZS for the purpose of recovering some part of the 240-bit encryption key.

2 Encryption with T-310

The T-310 has a block cipher which is not used directly to encrypt the data, but it is iterated a large number of times in a stream encryption mode with a low data rate. Some $13 \cdot 127 = 1651$ block cipher rounds 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. Section 2.2.

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 [14] 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 is a source of numerous self-similarity attacks [7, 9, 10].

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 [11]. Then East German cipher designers had already in 1970s mandated a substantially more complex structure [1]. The actual connections depend on the LZS (cf. Section 1.1).

2.1 Block Cipher Inside T-310

Following [15] we denote by $u_{m,1-36}$ the 36-bit state of the cipher at moment $m = 0, 1, \ldots$. We start with $u_{0,1\ldots36}$ =0xC5A13E396. We denote by $\phi : \{0,1\}^3 \times \{0,1\}^{36} \rightarrow \{0,1\}^{36}$ the function of one round. We have

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

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. $u_{m+1,i+1} = u_{m,i}$ for any $i \neq 4k$, $k \in \mathbb{N}$, i.e. for any i not being a multiple of 4.

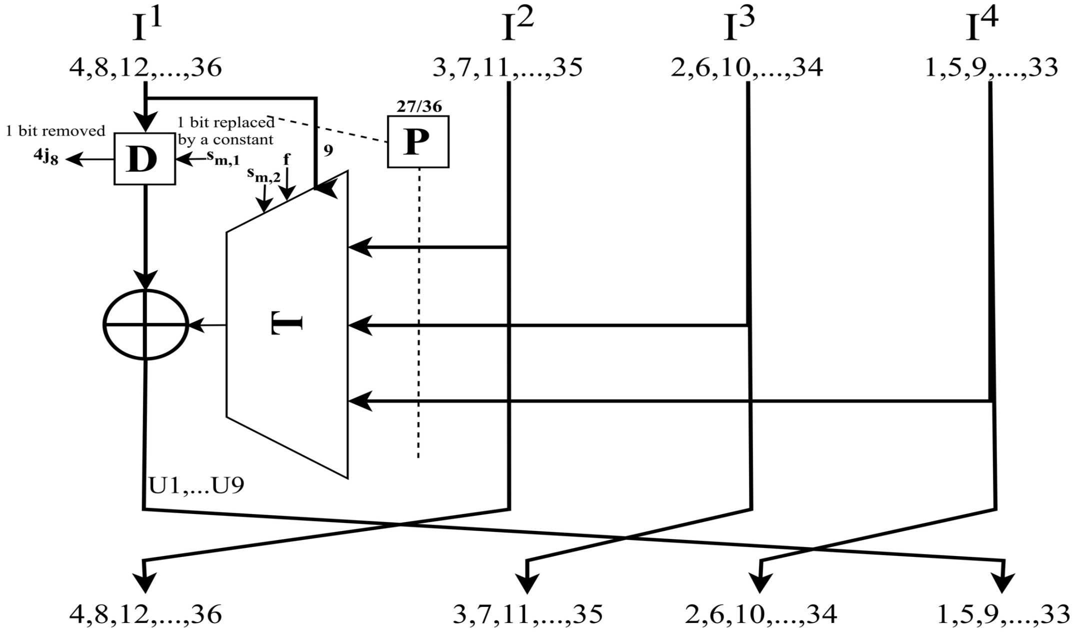

Fig. 1. T-310 mandates a very peculiar variant of a Feistel cipher with 4 branches with further particularities such as replacing one bit by a key-dependent constant $s1$ when we use a long-term key of type KT1.

It remains to specify how the U_{1-9} are computed inside one round. In a typical KT1 case cf. [6] we have $D(i) = 0$ and we assign input $u_{m,0} \overset{def}{=} s_{m+1,1}, \quad m \geq 0$ which is part of the 240-bit secret key and a constant for any given round.

Overall for all KT1 keys we have the following equations (1-9):

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

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

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

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

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

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

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

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

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

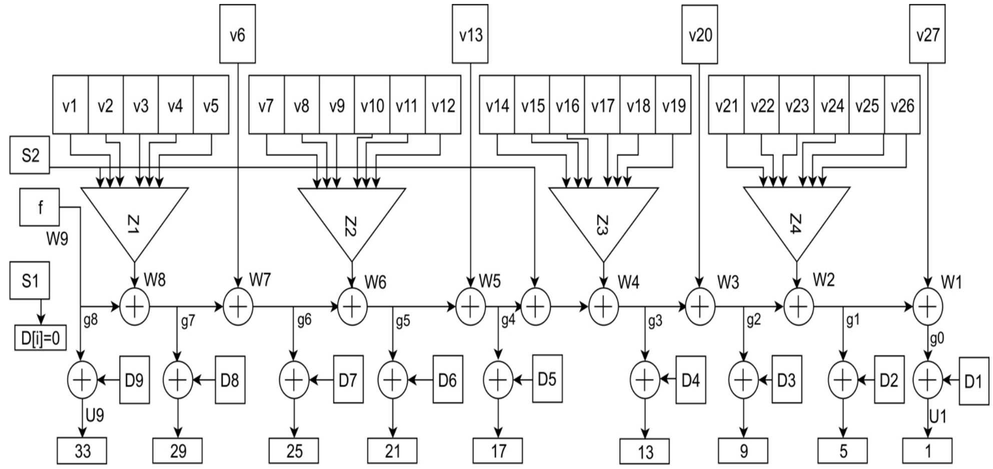

Fig. 2. Internal structure of one round of T-310. Input vi will be connected to bit $P(i)$.

Finally, in the above, $Z1 - Z4$ are what could be called "the T-310 S-boxes", which however have only 1 output bit, and are four identical copies of the following Boolean function Z:

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

2.2 How Encryption is Performed - Double One-Time Pad

From our iterated block cipher we extract just 1 bit per 127 rounds. Traditionally in numerous ciphers a one time-pad is applied, where the plaintext would be XORed with the keystream. Here the process is more complex and an additional matrix multiplication is used. We have a sort of "double one-time pad" where the plaintext bits are actually "masked" twice, presumably aiming at improved security. More precisely, let $a_i \overset{def}{=} u_{127i,\alpha}$ for any i. Out of these bits, for every 13 bits we discard 3 and use only 5+5 bits to encrypt one character of the plaintext as follows:

$$C_j = (P_j \oplus B_j) \cdot M^{r_j},$$

where P_j/C_j is the plaintext/ciphertext character on 5 bits, respectively, then $B_j = (a_{7+13(j-1)}, \ldots, a_{11+13(j-1)})$ are 5 consecutive bits out of the 13 above, and r_j is are derived from another subset of consecutive 5 bits as follows:

$$r_j = \begin{cases} 0 & \text{if} \quad R_j = (0,0,0,0,0) \\ 0 & \text{if} \quad R_j = (1,1,1,1,1) \\ 31 - r & \text{if}\ R_j \cdot M^r = (1,1,1,1,1) \end{cases}$$

where $R_j \overset{def}{=} (a_{1+13(j-1)}, \ldots, a_{5+13(j-1)})$ and

$$M = \begin{pmatrix} 0\,0\,0\,0\,1 \\ 1\,0\,0\,0\,0 \\ 0\,1\,0\,0\,1 \\ 0\,0\,1\,0\,0 \\ 0\,0\,0\,1\,0 \end{pmatrix}, \quad \text{which is such that} \quad M^{31} = Id.$$

2.3 Decryption Oracle Attacks

Given a decryption oracle the attacker can send any IV of his choice and the ciphertext, and obtain the plaintext. We assume that the encrypted text has k characters (which are on 5 bits each). For the j-th character we have:

$$C_j = P_j \cdot M^{r_j} \oplus B_j \cdot M^{r_j}$$

In particular he can decrypt two different ciphertexts under the same setting with the same r_j and B_j, i.e.

$$C_j \oplus C'_j = (P_j \oplus P'_j) \cdot M^{r_j} \quad \text{for all} \;\; 0 \leq j < k.$$

From this we recover M^{r_j} uniquely almost always (avoiding the ambiguity between $R_j = (0,0,0,0,0)$ and $R_j = (1,1,1,1,1)$) and then determine also B_j. More precisely:

Theorem 2.3.1 (Simple Decryption Oracle Attack). For every IV chosen by the attacker, and for every $k \geq 1$, the attacker can obtain a proportion of about 73 % of the internal keystream bits a_i with a tiny computation cost and with only 2 “Chosen IV and Chosen Ciphertext” decryption queries.
Proof: As above or see Thm. 3.0.1. page 197 in [3].

3 A New Simplified Slide Attack on T-310

A recent article [3] describes a decryption oracle slide attack on T-310 which works basically as follows:

Sa The attacker is able to inject any ciphertexts and any 61-bit IV and obtain the corresponding plaintext.

Sb The attacker produces numerous ciphertexts with different IV which differ by clocking the IV LFSR by $120 \cdot s$ steps for a certain integer s.

Sc From decryptions of multiple ciphertexts under a single key and IV the attacker recovers the bits $a_i \overset{def}{=} u_{127i,\alpha}$ which are used for encryption [only for certain integers i actually used], cf. Thm. 2.3.1 or Thm 3.0.1. in [3].

Sd Then the attacker hopes that in the two encryptions he has created the internal block cipher states will become identical (this can only happen essentially at random with probability 2^{-36}) at exact places where the IVs become aligned after $120s$ steps.

Se Then the attacker uses a correlation attack in order to confirm in each cases the internal states are identical.

Sf Finally the attacker uses a SAT solver to recover the key on 240 bits.

There are several serious problems in this attack approach of [3]:

1. The article [3] does NOT show that this attack is feasible for any even remotely realistic setup. This is essentially due to Step Se: only one LZS named 701 is shown to exhibit a suitable correlation. And key 701 does not have a bijective round ϕ and therefore it is expected to be broken by a substantially better attack of [5].
2. Due to Step Sf, in [3] we have a key recovery attack on $120s$ rounds, and then $s = 1$ seems obligatory for such an attack to succeed in practice. Breaking a large multiple of 120 rounds in this way seems completely unrealistic.
3. In order for the step Sf to work and for the key to be uniquely defined, at least 8 slide pairs such as obtained in previous steps were needed in [3].

In this article we show that for a proportion of LZS keys we can have large s and step Sf will not be necessary. The fundamental equation in [3] is:

$$120 \cdot s = 127 \cdot t + d$$

where the attacker produces two IVs being $120 \cdot s$ steps away and hopes that d is small and that suitable correlations exit to make Step Sf work. Now if we are only allowed to have $s = 1$ we get $d = -7$ which leads to Step Sf using correlations on the cipher state 7 steps away and we found that extremely few such correlations exist in T-310. In this article we consider $s = 120$ exactly and this gives $d = 0$. Here there is no need for correlations (at least if we can recover the keystream cf. Step Sc). The keystream bits will be identical IF the two states on 36 bits are identical. The attacker is able to identify "slid pairs" - technical term for 2 identical encryptions with identical states which carries on and on forever, and at no cost whatsoever.

Remark. The reason why the case $d = 0$ was not exploited in [3] is that all that the attacker gets are P/C pairs for a blockcipher with at least $120 \cdot 127$

rounds and 240-bit key. This has seemed extremely difficult to attack so far. In this article we will show that this can in fact be attacked and that key bits [or rather their linear combinations] can be recovered by the attacker. This is essentially due to the power of LC-weak keys: linear properties in question are true with probability 1 and propagate for an arbitrarily large number of rounds.

4 A Key Recovery Attack On Vulnerable LZS

The main claim in this article is that:

Theorem 4.0.1 (Slide Attack with LC-weak Keys). If an LZS is subject to an LC invariant property which involves some s1 key bits, and some f/IV bits, then the attacker can recover from an access to a decryption oracle at least one linear equation on a subset of 240 the key bits which is guaranteed to be correct.

Proof: To make this argument more concrete and compelling we are going to assume that our LZS has the following property which for example[1] occurs for key 706:

```
706: P=8,2,33,4,13,20,5,14,9,22,30,31,16,19,21,32,3,25,28,36,
27,11,23,29,12,24,10 D=0,28,8,4,24,12,16,20,32
[1,5,15,33]-s1f->[2,6,16,34]->[3,7,25,29,35]->[4,8,26,30,36]->
      [9,13,27,31]->[10,14,28,32]->[1,5,15,33]
```

The attacker proceeds as follows:

Sab Again the attacker produces numerous ciphertexts with one IV chosen at random and IV' which differs by clocking the IV LFSR backwards by $120 \cdot s$ steps for $s = 127$. He obtains the corresponding plaintexts [from the printer for example].

Sc1 This is done 2+2 times, 2 times for IV and 2 times for IV'. Due Thm. 2.3.1 the attacker can determine about 73 % of the potential keystream bits $u_{\alpha \cdot i}$ for IV, and also about 73 % of the $u'_{\alpha \cdot i}$ for IV'.

Sc2 We assume that the ciphertexts used with IV have 5 characters, and those used with IV' have about 1205 characters so that after $120 \cdot 127$ steps of the cipher with IV' consuming less than $120 \cdot 10 \cdot 13$ to process 1200 characters, we have still at least 5 characters which will have at least $5 \cdot 13 = 65$ bits of type $u_{\alpha \cdot i}$ in the overlapping part where the cipher key, IV and offsets of bits used for encryption overlap perfectly.

Sc3 Overall for each pair IV, IV' the attacker recovers two sequences of some 65 bits out of which there will be about $35 \approx 65 * 0.73 * 0.73$ locations where the bit $u_{\alpha \cdot i}$ and the same $u'_{\alpha \cdot i}$ is known for both IV and IV'.

Sc4 If on this subset of 35 locations i out of 65, all bits are identical i.e. $u_{\alpha \cdot i} = u'_{\alpha \cdot i}$, the attacker will conclude that the state $u'_{120 \cdot 127,1-36}$ of the cipher is identical to $u_{0,1-36}$ =0xC5A13E396.

[1] In Thm. A.0.1 in Appendix we show that same happens for many other keys.

Sc5 In order for such an event to actually happen, the attacker tries some 2^{36} different pairs of IV, IV' and obtains $(2+2) \cdot 2^{36} = 2^{38}$ decrypted ciphertexts.

Sd Overall the attacker tries about 2^{36} different pairs IV, IV' until the 35 bits are identical and he can conclude that $u'_{120 \cdot 127, 1-36}$ =0xC5A13E396 with probability at least 50 %.

Se' Here we do not follow the previous attack anymore. Now using the property of key 706 that [1,5,15,33]→[1,5,15,33] for 6 rounds, and 5 other related properties of type [2,6,16,34]→[2,6,16,34] etc, the attacker computes 6 parity equations on the key bits S1.

The complexity of our attack is about 2^{38} decryption queries and running time is roughly also proportional to 2^{38}. The data complexity is large and probably can be substantially reduced for certain LZS where the attacker would submit queries with well chosen IVs such that both IV and IV' would be valid simultaneously in several different cases saving the time spent finding suitable pairs. This point would depend on additional fine details about the weak LZS in question.

5 Attack Summary and Discussion of Vulnerable Keys

Our main result is that if the long term key has a linear property for K rounds and if this property involves S1 and f bits, then K linear combination of secret key bits can be recovered by the attacker. Importantly, the complex specification KT1 which was enacted by the designers of T-310 in 1970s [14, 4] does NOT protect against this attack and up to $K = 6$ key bits can be recovered for example with key 706, and countless other KT1 keys with added the exact conditions of our Thm. A.0.1 in Appendix A. With these conditions we can define a class of keys which will be fully compliant with KT1 spec and therefore could have been approved and used to encrypt real-life communications, yet the attacker with access to a decryption oracle can recover a number of key bits.

5.1 More Vulnerable Keys within KT1 Space

Furthermore it is possible to show that keys which are “like” 706, cf. Thm. A.0.1, are a small proportion inside a vast space of other types of long-term keys vulnerable to our attack. To show this we have conducted a series of computer simulations and have identified numerous distinct classes of LZS vulnerable to our attack. Below we give some concrete examples with $K = 3, 5, 6$ and 8 rounds.

```
3R [1-6,33-36+1S1F+2S1F+3S1F] D=0,36,24,32,8,28,20,12,4, P=
36,8,33,24,17,12,5,4,9,26,23,31,20,2,21,1,3,25,22,16,28,13,35,29,18,32,6
6R [10,14,20,24+1S1F] D=0,24,36,4,32,12,16,28,20 P=
32,20,33,4,36,28,5,13,9,26,22,10,16,18,21,27,24,25,1,8,23,12,2,29,7,11,30
5R [1-10,13-16,25-36+1S1F+2S1F+3S1F+4S1F+5S1F] D=0,32,36,4,24,12,16,20,28
P=11,36,33,1,7,20,5,23,9,28,13,27,16,12,21,17,15,25,34,8,32,2,4,29,24,14,10
8R [1,3,5,17,21+3F+5F+7S1] D=0,36,16,32,24,8,20,28,4
P=36,4,33,16,30,28,5,17,9,19,11,23,20,26,21,24,22,25,1,12,35,8,31,29,32,7,6
```

Here the notation XS1+YF means that the property uses simultaneously bit $s1$ of the key at round X and f bit of IV at round Y. Overall we found countless distinct cases with smaller $K = 1, 2, \ldots$ which also have linear properties involving $s1$ and f and in a computer simulation we found that for about 53 % of all KT1 keys with linear properties, these properties contain both f and $s1$ parts for some K. Knowing that it was estimated that about 3 % of all KT1 keys have some linear properties cf. [6], we see that overall about 1.5 % of all KT1 keys are vulnerable to the attack described in this article.

Table 1. Fraction of LC-weak keys and the highest possible K value such that they exhibit a linear property for K rounds containing simultaneously $s1$ and f.

$K = 1$	$K = 2$	$K = 3$	$K = 4$	$K = 5$	$K = 6$	$K \geq 7$	total
0.000	0.46	0.06	0.003	0.001	0.001	0.0001	0.53

In our simulations 46 % of weak KT1 keys have $K = 2$ and we have never seen a property with $K = 1$ s.t. another better property with $K \geq 2$ would not exist.

Remark. For some other keys, which are no longer of type KT1, we can have higher $K = 12$ cf. Appendix B.

6 Conclusion

T-310 is an important Cold War cipher. It is essentially a block cipher from which we extract extremely few bits for the actual encryption. This property and its incredibly large gate complexity, cf. [1], makes that T-310 looks substantially stronger than any other cipher from the same historical period such as DES or RC2. Cryptanalytic literature knows extremely few examples of key recovery attacks under such difficult circumstances, cf. [4, 8]. Our main result is to show how to recover a part of the 240-bit key of T-310 when the long term keys LZS are somewhat weak[2], in a somewhat realistic decryption oracle attack scenario. This article combines two different attacks recently published on T-310: a linear attack and a slide attack. None of these attacks was able to recover any key bits so far and even less so, if the keys are expected to follow all the strict KT1 rules mandated by the designers. This ambitious goal we eventually achieved here. For a substantial fraction of about 1.5 % of all possible KT1 keys, cf. Section 5.1, yet none[3] of the actual historical keys, we are able to recover up to 8 bits of the secret key. For some other keys we can recover up to 12 bits, cf. Appendix B.

6.1 Further Research - Combination Attacks

It is easy to see that the attack described in this paper can be further combined with the previous slide-correlation attacks with $d > 0$ in [3]. It is easy to see that many of the weak keys studied in this article allow to easily improve the previous slide attacks in [3], by making it easier for the attacker to know when 2 states in 2 different encryptions are likely to be identical. In this type of attack scenarios the attacker should in fact prefer another (disjoint) set of weak LZS, those which do not use $s1$. A wider variety of examples of weak keys can be found in [4].

[2] Weak keys in cryptanalysis do not matter in general, **except** if their relative frequency is quite large. In such cases, which is the case here and also in [9, 10], it is important to see the complexity of the best single key attack will not be an (even remotely) accurate method to evaluate the security of the cipher.

[3] Unfortunately 1.5 % is not yet that large, or we are not lucky, and following [6] neither our attack, nor another strong linear property, do not work for any actual Cold War LZS.

6.2 Recovering More Key Bits and Non-Linear Invariant Attacks

At this moment we have an academic key recovery attack on T-310 which is only able to recover a part of the secret key. It remains an open problem if any further key bits or linear combinations could also be obtained and if any further than 1.5 % of all KT1 keys could also be weak. In particular until now we have no attack able to recover any bits from the other half s2 whatsoever. We conjecture that this will not work with the simple linear invariant attacks such as studied in this article. The answer to all these questions lies in non-linear invariant attacks which are a highly non-trivial generalization of linear attacks we study suggested in Section 7 of [6]. However no truly relevant and realistic example of such attack was yet found. A recent article shows that such invariants do exist and shows how they can be constructed and made to work for T-310. A nice proof of concept example which shows that invariants using $S2$ very specifically are actually possible is the key 771 in Section 8.3. in [2]. This example is directly applicable to our attacks. Non-linear invariants are very likely to improve on our 1.5 % of vulnerable KT1 keys. However constructing solutions with specific features or even checking if such solutions do at all exist remains difficult and requires more research. In addition the solution 771 of [2] is not yet quite satisfactory. It only works when the Boolean function Z is modified.

Overall recovering more than 6 bits of the key in our linear attacks or more advanced non-linear invariant attacks, and/or for a larger proportion of LZS, and/or in realistic attack scenarios (with the original Boolean function) remains an open problem.

References

1. 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.
2. Nicolas T. Courtois: *On the Existence of Non-Linear Invariants and Algebraic Polynomial Constructive Approach to Backdoors in Block Ciphers,* `https://eprint.iacr.org/2018/807.pdf`, received 1 Sep 2018, last revised 3 Dec 2018.
3. Nicolas T. Courtois: *Decryption oracle slide attacks on T-310,* In Cryptologia, vol. 42, Iss. 3, 2018, pp. 191-204. `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1362062`
4. 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://eprint.iacr.org/2017/440.pdf`
5. 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`.
6. Nicolas Courtois, Maria-Bristena Oprisanu and Klaus Schmeh: *Linear cryptanalysis and block cipher design in East Germany in the 1970s,* will appear in Cryptologia in 2018.
7. Nicolas Courtois: *Security Evaluation of GOST 28147-89 In View Of International Standardisation,* in Cryptologia, volume 36, issue 1, pp. 2-13, 2012.
8. Nicolas T. Courtois: *The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime,* In SECRYPT 2009 – International Conference on Security and Cryptography: pp. 331-338. INSTICC Press 2009, ISBN 978-989-674-005-4.
9. Nicolas Courtois: *Algebraic Complexity Reduction and Cryptanalysis of GOST,* Monograph study on GOST cipher, 2010-2014, 224 pages, available at `http://eprint.iacr.org/2011/626`.
10. Nicolas Courtois: *On Multiple Symmetric Fixed Points in GOST,* in Cryptologia, Iss. 4, vol 39, 2015, pp. 322-334.
11. 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.
12. Mitsuru Matsui: *Linear Cryptanalysis Method for DES Cipher,* Eurocrypt'93, LNCS 765, Springer, pp. 386-397, 1993.
13. Jacques Patarin, Valérie Nachef, Côme Berbain: *Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions,* in Asiacrypt 2006, pp. 396-411, LNCS 4284, Springer 2006.
14. 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.*
15. *Klaus Schmeh: The East German Encryption Machine T-310 and the Algorithm It Used,* In Cryptologia, vol. 30, iss. 3, pp. 251 – 257, 2006.

A Appendix - A Detailed Result for 6 Rounds of T-310

The key 706 is not the only key which exhibits an invariant property for 6 rounds with probability 1 and which depends on s1 part of key bits. The same happens for all keys which satisfy a number of conditions as follows:

Theorem A.0.1 (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 2.1:

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

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

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

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

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

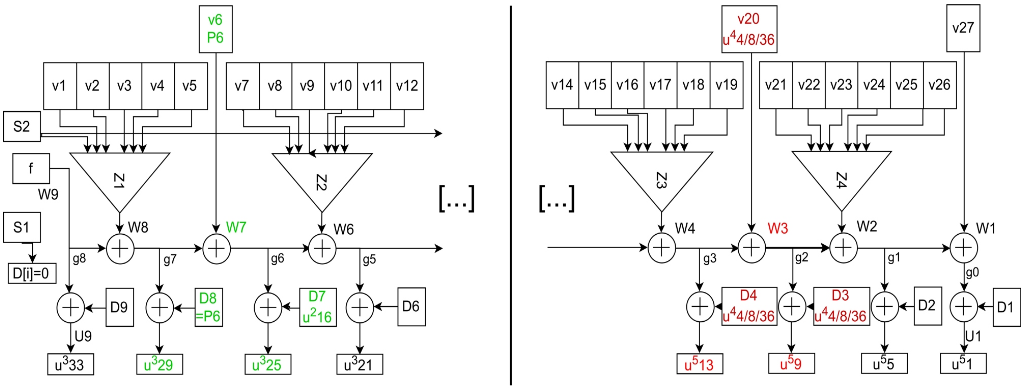

Fig. 3. Explanations for our proof for key 706.

From the KT1 properties in [4], 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] → [25, 29] for 1 round and, combining all the linear properties discussed so far, [1, 5, 15, 33] → [3, 7, 25, 29, 35] for 2 rounds.

Then we observe that $u^{(3)}_{25} = u^{(5)}_{27}$, $u^{(3)}_{29} = u^{(5)}_{31}$, $u^{(3)}_{3} = u^{(4)}_{4}$, $u^{(3)}_{7} = u^{(4)}_{8}$ and $u^{(3)}_{35} = u^{(4)}_{36}$. We assumed $\{D(3)/D(4), P(20)\} \subset \{4, 8, 36\}$. Therefore, equation (3) becomes

$$u^{(4)}_{4} \oplus u^{(4)}_{8} \oplus u^{(4)}_{36} = u^{(5)}_{9} \oplus u^{(5)}_{13} \tag{10}$$

Thus, we have shown that [3, 7, 25, 29, 35] → [9, 13, 27, 31] for 2 rounds.

We recall that our goal is to show the following sequence of linear equalities:
[1,5,15,33]s1f→[2,6,16,34]→[3,7,25,29,35]→
[4,8,26,30,36]→ [9,13,27,31]→[10,14,28,32]→[1,5,15,33]

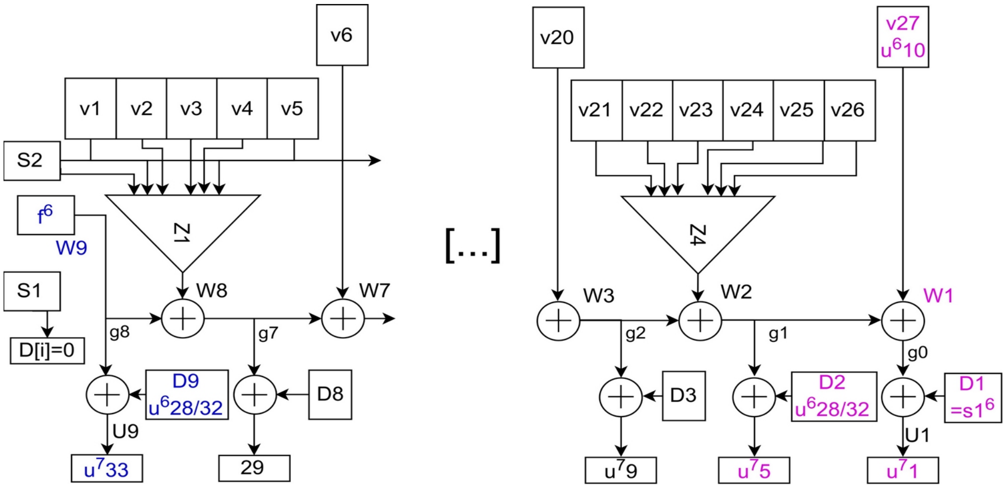

Fig. 4. Further illustration for our proof.

We proceed to the final part of the proof as follows: It is clear that $u^{(5)}_{13} = u^{(7)}_{15}$, $u^{(5)}_{9} = u^{(6)}_{10}$, $u^{(5)}_{27} = u^{(6)}_{28}$, and $u^{(5)}_{31} = u^{(6)}_{32}$. The remaining conditions from the theorem A.0.1 hypothesis are $P(27) = 10$ and $\{D(2), D(9)\} \subset \{28, 32\}$. Hence, equation (1) becomes

$$u^{(6)}_{10} \oplus s^{(6)}_{1} \oplus u^{(6)}_{D(2)} = u^{(7)}_{1} \oplus u^{(7)}_{5}$$

and equation (9) becomes

$$u^{(6)}_{D(9)} \oplus u^{(7)}_{33} = f^{(6)}$$

Finally

$$u^{(6)}_{10} \oplus u^{(6)}_{D(2)} \oplus u^{(6)}_{D(9)} \oplus s^{(6)}_{1} \oplus f^{(6)} = u^{(7)}_{1} \oplus u^{(7)}_{5} \oplus u^{(7)}_{33} \tag{11}$$

It follows that if $\{D(2), D(9)\} \subset \{28, 32\}$ we have $[10, 28, 32, s^{(6)}_{1}, f^{(6)}] \rightarrow [1, 5, 33]$ for 1 round. Finally, we have also shown that [9, 13, 27, 31] → [1, 5, 15, 33] for 2 rounds. This ends the proof that if the conditions of the theorem are satisfied, we have $[1, 5, 15, 33, s^{(6)}_{1}, f^{(6)}] \rightarrow [1, 5, 15, 33]$ for 6 rounds.

B Appendix B - Further Vulnerable Keys Not KT1

In this section we show that if we drop certain requirements of the class KT1 we are able to construct even weaker keys with larger K being up to $K = 13$. Here are two examples of such keys with $K = 12$ and $K = 13$ respectively with full details of the linear properties obtained.

```
712: P=28,26,33,32,30,24,5,15,9,8,22,13,4,6,21,10,20,25,
16,36,11,31,27,29,17,18,12 D=0,16,28,32,12,20,4,24,8
 [1,5,27,31,35]->[2,6,28,32,36]->[3,7,9,13]->[4,8,10,14]->
  [11,15,25,29,33]-f->[12,16,26,30,34]->[1,5,27,31,35]-s1->
   [2,6,28,32,36]->[3,7,9,13]->[4,8,10,14]->[11,15,25,29,33]
    -f->[12,16,26,30,34]->[1,5,27,31,35]
813: P=8,18,17,13,29,33,26,28,12,32,30,19,9,27,10,34,16,5,
35,11,1,6,31,23,14,25,15 D=32,28,4,8,36,12,20,24,16
 [4,8,35]->[9,12-13,36]->[14,17,21]->[15,18,22]->[16,19,23]
  ->[20,24,33]-f->[25,29]->[26,30]->[27,31]->[28,32]
   ->[1,5,16]->[2,6,33]-f->[3,7,34]->[4,8,35]
```

These keys have been generated in 1 hour approximately by our proprietary software which uses a SAT solver in order to generate keys with arbitrary specified characteristics together with a full formal mathematical proof of a linear property. The key 813 is problematic: s1 is not used inside the linear property therefore we do not get a key recovery attack. The key 712 is the strongest example of key which uses s1 and f and therefore the attack of Section 4 can be applied and $K = 12$ linear equations on secret key can be obtained.