Linear cryptanalysis and block cipher design in East Germany in the 1970s

Nicolas T. Courtois[1], Maria-Bristena Oprisanu[1], and Klaus Schmeh[2]

[1] University College London, Gower Street, London, UK

[2] cryptovision, Gelsenkirchen, Germany

Abstract. Linear Cryptanalysis (LC) is an important code-breaking method which has become popular in the 1990s and has roots in earlier research [Shamir,Davies] in the 1980s. In this article we show evidence that Linear Cryptanalysis is even older. According to documents from the former Eastern German cipher authority ZCO, systematic study of linear characteristics for non-linear Boolean functions was routinely performed already in the 1970s. At the same period Eastern German cryptologists have produced an excessively complex set of requirements known as KT1, which the long term keys are required to satisfy and keys of this type were in widespread use to encrypt communications in the 1980s. An interesting question is then, to see if KT1 keys offer some level of protection against linear cryptanalysis. In this article we demonstrate that (strangely) not really. This is demonstrated by constructing specific counter-examples of pathologically weak keys which satisfy all the requirements of KT1.
However, as T-310 is used in a stream cipher mode that uses only a tiny part of the internal state for actual encryption, it remains unclear whether this type of weak keys could lead to key recovery attacks on T-310.

Key Words: Cold War, block ciphers, Linear Cryptanalysis, Boolean functions, ANF, T-310, SKS V/1, weak keys, backdoors.

Acknowledgments. The authors would like to thank Jörg Drobick, Bernd Lippmann and Jens Raeder for their help and support.

1 Introduction

This article is about what we can learn about design and analysis of ciphers in the Eastern block during the Cold War based on original documents found in Eastern German state security archives. We focus on low level cryptanalysis questions such as how bit-level linearity and non-linearity shape the security of larger components. It is widely known that Differential Cryptanalysis was known under the name of "tickle attack" in the 1970s, two decades before it was studied in open academic community [12, 19]. In contrast not much is known about the history of Linear Cryptanalysis. We have the early works of Davies [3] and Shamir [29] from the 1980s, which are very incomplete and later works which put earlier attacks in a new light [4, 1, 5] and show that all these facts are very closely related to (nowadays standard) Linear Cryptanalysis [LC]. In this article we show evidence that the study of linear characteristics was part of a routine set of properties which were already carefully studied in the 1970s in Eastern Germany [26] more than a decade before it was studied in the academia [29, 23, 20, 21]. At the same time we will show that the T-310 cipher can nevertheless be extremely weak w.r.t. LC.

This article is organized as follows. In next Section 2 we outline the history of East German cipher machines from 1970-1990. In Section 3 we show that analysis of ciphers in terms [non-]linearity is indeed quite old. In Section 4 we study the T-310 cipher in full detail and in Section 5 we study the constraints which the cipher long-term setup was mandated to satisfy. In Section 6 we show that the cipher can nevertheless be made very weak. In Section 7 we consider a question of existence of a more general non-linear backdoor-like property. Finally in Section 8 and in Conclusion section we discuss the potential implications of our weak-key attacks.

2 History of SKS V/1 and T-310

SKS V/1 is an Eastern German electronic encryption device for teletype communication by radio and wire, mainly used in the late 1970s and 1980s, cf. [16, 17] and `scz.bplaced.net/old.html`. All functions are implemented in hardware by means of logic gates and flipflops. Other communist countries, namely the Soviet Union, Bulgaria, Poland, Czechoslovakia, and Hungary, made use of the SKS V/1, as well. The development of the SKS V/1 started in the early 1970s. The SKS V/1 was developed by the Eastern German authority of cipher affairs, Zentrales Chiffrierorgan (ZCO), which contributed the cryptologic expertise, and the Institut für Regelungstechnik (IfR). Both organizations were located in East Berlin. The development included a comprehensive security analysis of the cipher algorithm used by the SKS V/1, which took place from 1973 to 1974. The SKS V/1 seems to be an Eastern German development. The records contain references to several consultation meetings with Soviet specialists.

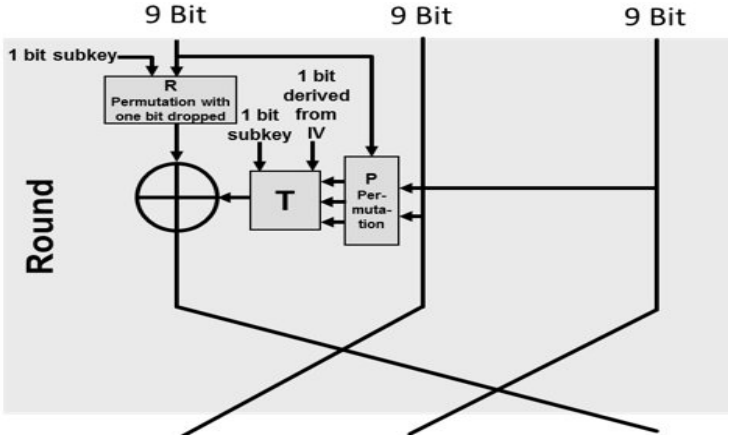

Fig. 1. The main component of SKS V/1 cipher: a block cipher with 27-bit blocks.

After the IfR had built a number of prototypes, the serial production of the SKS V/1 took place at VEB Steremat "Hermann Schlimme" in East Berlin. The first device was shipped in 1977. Five years later in 1982, a T-310 machine which was the successor of the SKS V/1, was in serial production. Nevertheless, an improved version of the SKS V/1, the SKS V/2 DISKRETA, was developed

starting in 1987. Usage of the SKS V/1 in Eastern Germany (and the development of the SKS V/2 DISKRETA) probably ended in 1990 with the German reunification and the merger between the Eastern German ZCO with its western counterpart, the Zentralstelle für Informationssicherheit (ZfI) in Bonn. It is not known, until when the SKS V/1 was used in other communist countries.

The SKS V/1 is not a single device, but a system consisting of numerous components encased in solid metallic boxes which have different names such as CE, DE2 or PG2 and which realize the whole handling of messages including entering, encryption, transmission by cable or radio, receiving, decryption and print. The cleartext is entered with a typewriter keyboard. The long-term key consists of 32 hand-wired circuit boards. The short term key has 208 bits and is entered via a punch card.

The T-310 is another Eastern German encryption machine and the successor of the SKS V/1. T-310 is a complex electronic encryption machine built around another block cipher with 36-bit blocks. Inside we find the exact same component $T()$ cf. Fig. 1 and later Fig. 2 and Fig. 4. It has a long-term key (a.k.a. LZS) configured via printed circuit boards. The short-term key has 240 bits and is entered via a punch card.

T-310 was used to encrypt teletype communications (by radio and wire) during the last period of the Cold War. The T-310 is considered the most important Eastern German cipher machine of its time. It was designed by ZCO crypto experts in the 1970s. Like the SKS V/1, the T-310 is an Eastern German development with Soviet specialists being involved for analysis. It became known to a larger English-speaking public since a paper published in Cryptologia in 2006 [28]. The T-310 was used by the Ministry of State Security (also known as "Stasi"), the Ministry of National Defense, the Council of Ministers, the police, the youth organization FDJ, the trades union organization FDGB, and the Central Committee of the SED (the SED was the leading political party). In 1989 there were some 3,800 copies in active service. There is no evidence that the T-310 was used in countries other than Eastern Germany.

The first specification of the tactical and technical requirements for the T-310 was available in 1973. "Quasi-absolute security" was stated as a requirement. In 1974 the design of the cryptographic algorithm (in some documents named ARGON) began. Two cryptologists (both mathematicians) were commissioned for one year. The development of the device began in 1976 at the IfR with first prototypes being available in 1978. In 1980 cryptologists of the ZCO and from the Soviet Union conducted an investigation of the security of the encryption process. Two years later the T-310/50 model of T-310 was put into serial production at VEB Steremat "Hermann Schlimme". In August 1990, shortly before the German reunification, the ZCO handed over a T-310 device to their Western German colleagues from the Zentralstelle für Informationssicherheit (ZfI), which was later renamed to Bundesamt für Sicherheit in der Informationstechnik (BSI). With the reunification, the usage of the T-310 terminated. The BSI later analyzed the encryption algorithm of the T-310. Officially, the BSI was not authorized to say anything about the results, but unofficially, the device was rated extremely secure.

3 Cipher Design, Boolean Functions and Linear Cryptanalysis in the Eastern Bloc

Our study reveals that many fundamental questions related to security of ciphers have a long history.

3.1 Boolean Functions and ANF

A standard way to represent a Boolean function in modern cryptography is to use the Algebraic Normal Form (ANF). According to Wikipedia [31], this method of algebraization of arbitrary Boolean functions was invented by the Soviet mathematician Zhegalkin in 1927 [31]. ANFs or Zhegalkin polynomials are simply "polynomials of ordinary high school algebra" which when interpreted over the integers mod 2 become remarkably simple: "requiring neither coefficients nor exponents", cf. [31]. Interestingly, it took nearly a decade for Western

mathematicians to also use this tool, and initially mathematicians proposed unnecessarily complicated methods to "arithmetize" the Boolean algebra. Only in 1936 the U.S. mathematician Marshall Stone has reflected on the not quite "loose analogy" between Boolean algebras and rings which has led to wider adoption of ANF representations of Boolean functions cf. [31]. Not surprisingly we found that the ANF (or Zhegalkin polynomials) is the default and routine tool consistently used across numerous Eastern German cryptography documents we have studied.

3.2 The Boolean Function in SKS V/1 and T-310 Ciphers

The principal cipher used in Eastern-German cryptography during the Cold War is T-310 cf. [28]. The primary non-linear component of this cipher is a Boolean function $Z : \mathbb{F}_2^6 \to \mathbb{F}_2$. This function was in fact designed in the 1970s for SKS V/1 cipher, the predecessor of T-310 [30, 27]. An exact specification of Z can be found in [27] page 113 [27] and in page 39 of [30]. We have verified that both Boolean functions are identical.

$$\begin{aligned} Z(e_1, e_2, e_3, e_4, e_5, e_6) = 1 \oplus e_1 \oplus e_5 \oplus e_6 \oplus e_1e_4 \oplus e_2e_3 \oplus e_2e_5 \oplus e_4e_5 \oplus e_5e_6 \oplus \\ e_1e_3e_4 \oplus e_1e_3e_6 \oplus e_1e_4e_5 \oplus e_2e_3e_6 \oplus e_2e_4e_6 \oplus e_3e_5e_6 \oplus \\ e_1e_2e_3e_4 \oplus e_1e_2e_3e_5 \oplus e_1e_2e_5e_6 \oplus e_2e_3e_4e_6 \oplus e_1e_2e_3e_4e_5 \oplus e_1e_3e_4e_5e_6 \end{aligned}$$

In this article $\oplus$ denotes an XOR (addition modulo 2).

3.3 Design Criteria for the Boolean Function Z from 1973

We found a list of original design criteria which were mandated by Eastern-German cryptologists in 1973 [25] for the (same) Boolean function $Z()$ of the earlier SKS V/1 cipher. They are listed on page 53 of [25] as follows:

(1) $$|\{X = (X_1, X_2, \ldots, X_6) \in \{0,1\}^6 | Z(X) = 0\}| = 2^5$$

(2) $$|\{X \in \{0,1\}^6 | Z(X) = 0, HW(X) = r\}| \approx \tbinom{6}{r} \cdot \tfrac{1}{2}, \qquad r = 0..6$$

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

(4) Z is not symmetric

It is noteworthy that the criterion (3) is related to Differential Cryptanalysis which was only officially studied in 1990s and these criteria are very old: they come from the same period of time when DES was designed in the U.S. [5, 12].

3.4 Another Important Set of Requirements from 1976

We found another important document from 1976, which gives a different set of points to study and requirements or criteria which the Boolean function Z should satisfy, cf. page 30 in [15]. It also clearly states that these properties were specified one year earlier and that they are studied in full detail in [26]. We provide a translation below:

1. All derivations of Z were computed as Zhegalkin polynomials[1] and as value tables.
2. Frequency of the function result being '1' with k fixed values was computed for $(k = 1, 2, 3)$.
3. The *statistic structure* of the Boolean function was computed.
4. Z is not symmetric. This means that the function value changes if the arguments are permuted, if one or several arguments are negated, if the function is negated or if a combination of these three changes is applied.

The meaning of *statistic structure*. An examination of pages 17 and 18 in [26] makes it crystal clear that term *statistic structure* refers exactly to computing a full set of linear characteristics for this Boolean function Z cf. our Table 1 page 8 below.

Further statements. The original document [15] contains further precisions. It says that 1. and 2. are important requirements for further examination. Then it expands on 3. which again is precisely about Linear Cryptanalysis approximations cf. Section 3.5 and our Table 1 below, a.k.a. *statistic structure* (of Z). It says that it did not reveal any cryptographic "advantages" resulting from an approximation of the function Z via Boolean functions. Finally it explains

[1] Again this is the same as Algebraic Normal Form (ANF), cf. Section 3.1] and [31].

(in relation to 4.) that due to the asymmetry (property demonstrated on pages 19-20 in [26]) of Z the equivalence of long-term keys will be limited.

3.5 Linear Characteristics of Z

In this article we show that Linear Cryptanalysis was studied in a systematic way in the 1970s. A complete study of all possible 2^6 linear characteristics of Z is done on pages 17-18 of [26] under the name of "Statistische Struktur" (statistical structure) of the Boolean function Z.

Table 1. Fragment of Table 3.1-2 in page 18 of [26] dated 1976 which contains a complete set of linear characteristics of Z. In this table L denotes 1.

Tabelle 3.1-2

α	Δ_α^Z	t	α	Δ_α^Z	t
000000	32 0	32	L00000	0	32
00000L	2	34	L0000L	6	38
0000L0	-4	28	L000L0	0	32
0000LL	6	38	L000LL	6	38
000L00	-4	28	L00L00	-4	28
000L0L	-2	30	L00L0L	2	34
000LL0	0	32	L00LL0	4	36
000LLL	2	34	L00LLL	2	34

On page 17 a suitable definition is provided: the goal is to compute Δ_α^Z for any[2] $\alpha \in \{0,1\}^6$, which function is defined precisely as:

$$\Delta_\alpha^Z = 2^{6-1} - ||Z(x) - \sum_{i=1}^{6} \alpha_i x_i||$$

where $||g(x)||$ is the number of times $g(x) = 1$. We can also remark that

[2] Here $\alpha \in \{0,1\}^6$ and should not be confused with the notation $\alpha \in \{1,\ldots,36\}$ which is used to specify a part of the T-310 long-term key in [28, 13].

$$\Delta_{\alpha}^{Z} = t - 2^{6-1}$$

where t is the number of times $g(x) = 0$ with $g(x) = Z(x) - \sum_{i=1}^{6} \alpha_i x_i$ as above (and where sign '$-$' is the same as '$+$' modulo 2).

Observations. This table suggests that systematic computation of linear characteristics was already a routine task for cipher designers in 1976, a decade before [29, 23]. The presence of sign '$-$' suggests that similar or more general definitions in fields or rings other than $GF(2)$ were studied. Moreover, in [26] it is clearly indicated that this definition comes from a yet earlier source. Namely the authors say that the definition comes from Section 2 inside Chapter 2 "Boolean Functions" from classified lecture notes on cryptography delivered by Soviet specialists, known under reference number 2243 and not dated.

On Modern Notion of Non-Linearity. From here standard cryptographic literature would define the nonlinearity of the Boolean function Z as the Hamming distance from the set of all affine functions which in this case will be equal to:

$$\mathcal{N}(Z) = Min\,(\; Min_{\alpha}(||g(x)||)\;,\; Min_{\alpha}(t)\;)$$

The earliest reference in the open academic literature which contains this definition is Pieprzyk and Finkelstein, cf. Def. 7 page 326 in [23] from 1987/88 which cites an earlier paper from 1985 by the first author published in a more obscure publication in Poland.

4 The T-310 Cipher

T-310 or T-310/50 is a cipher machine which was the primary encryption method used in East Germany throughout the 1980s [16, 28]. The encryption method it uses is a peculiar form of a synchronous stream cipher which is also a mode of operation of a block cipher. A keystream is derived from the internal state obtained by iteration of a quite complex block cipher which we call "the T-310 block cipher". This should be compared to the original method of encryption invented by Feistel around 1971 [18], where the cipher state is divided in two "branches". Eastern block cipher designers had already in the 1970s [25, 28] mandated substantially more complex ciphers. SKS V/1 and T-310 can be seen as particular variants of the concept of "Contracting Unbalanced Feistel cipher" [22] with 3 and 4 branches respectively, cf. Fig. 1 and 2.

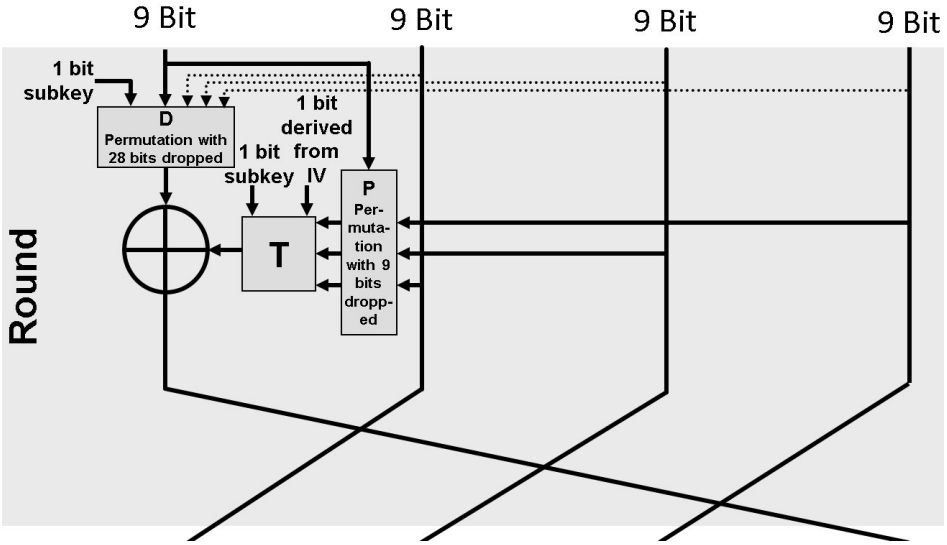

Fig. 2. Outline of one round of T-310.

This block cipher has a 240-bit secret key and the block size is 36 bits. It also takes an Initialization Vector (IV) of 61 bits which are generated at random by the sender and sent in cleartext (and which will be different for each transmission).

The encryption method used is in fact highly non-standard cf. [28]. The block cipher is basically never used directly to encrypt, and it is iterated a large number of times depending on the length of the data to be encrypted. Some $13 \cdot 127 = 1651$ block cipher rounds are performed in order to extract as few as 10 bits from the block cipher state, which will then be used to encrypt just one 5-bit character of the plaintext, cf. [28, 13, 14] for more details.

The secret key is $s_{1-120,1-2}$ which is 240 bits. The two key bits used in different encryption rounds m are $s_{m,1-2}$, $m \geq 1$ which repeat every 120 steps:

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

In contrast the IV bits are expanded in a less regular way, not periodic. The expansion is based on the following LFSR which produces a sequence with a very large prime [27] 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 or KeeLoq, which is a source of numerous self-similarity attacks [8, 10]. A detailed description of T-310 can be found in [13].

4.1 The Long-Term Keys

As in previous works the vulnerability of the cipher against attacks [13, 14] will strongly depend on the so-called long-term key, in German *Langzeitschlüssel*, a.k.a LZS. This LZS is defined by two mappings D, P which $D : \{1 - 9\} \rightarrow \{0 - 36\}$ and $P : \{1 - 27\} \rightarrow \{1 - 36\}$ which define the internal connections of the cipher and it also comprises a constant $\alpha \in 1 - 36$, the index at which data may be extracted for encryption. The long-term key LZS is precisely which defines how much the actual structure will diverge from a simple "Contracting Unbalanced" scheme with 4 branches, cf. [22] and Fig. 5. The designers of T-310 mandated numerous technical conditions which the LZS should satisfy, cf. Section 5 below.

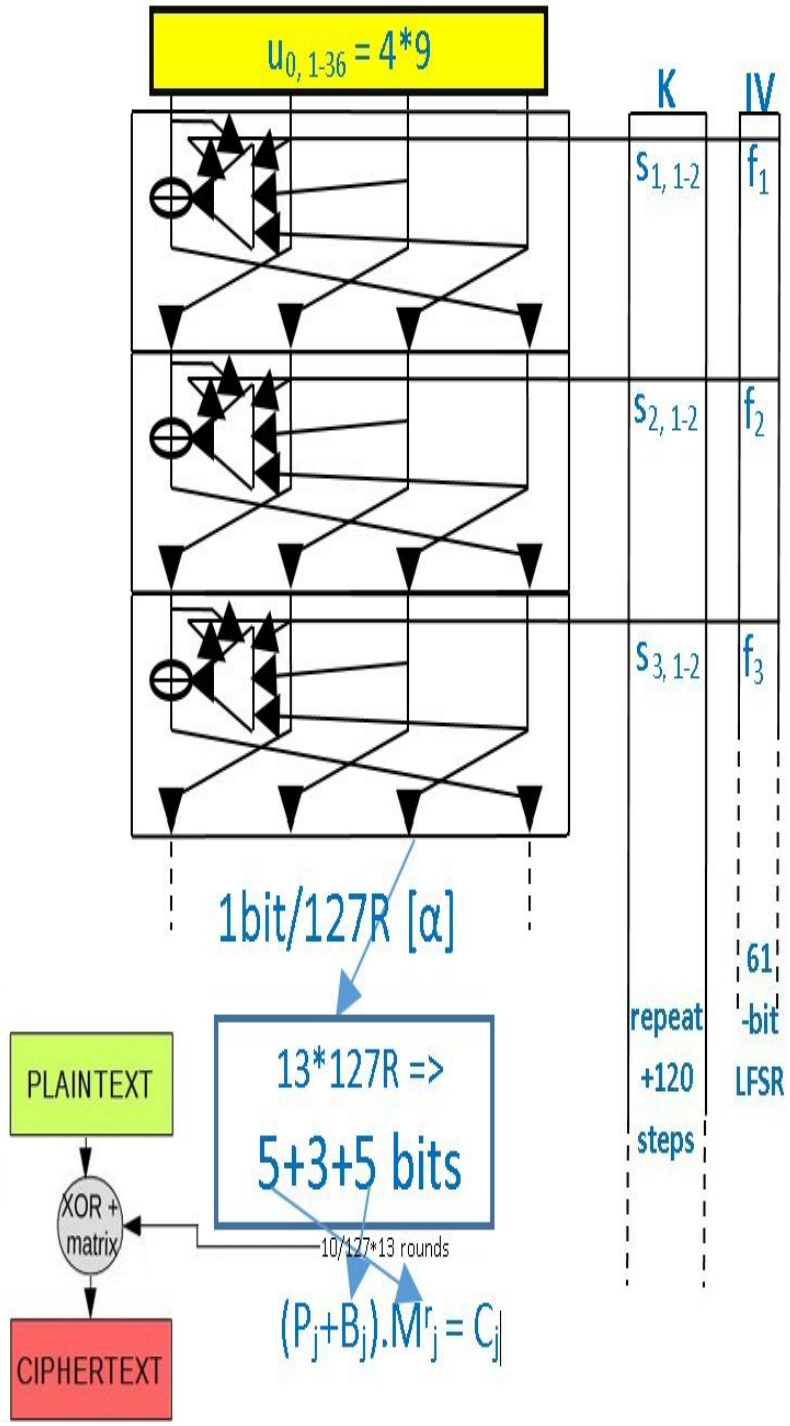

Fig. 3. T-310 Cipher.

Following [28] we denote by $u_{m,1-36}$ the 36-bit state of the cipher at moment $m = 0, 1, \ldots$. 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 of the other bits get shifted by one position i.e. $u_{m+1,i+1} = u_{m,i}$ for any $i \neq 4k$. Let U_{1-9} be the 9 newly created bits. By definition after one round we have

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

4.2 One Block Cipher Round

It remains to specify how the U_{1-9} are computed inside one round. The traditional method to define the round function is to first define a compression component $T : \mathbb{F}_2^{2+27} \to \mathbb{F}_2^9$ cf. Fig. 2 and [27, 28]. Then the 9 outputs are XORed with 9 bits specified by $D()$. In this article we adopt a particularly compact way to describe the whole round which is composed of $T()$ and final XORs directly. We present a series of formulas which allow to compute the U_i directly in order $u_0, U_9, \ldots, U_1$ which is computed last. This is also illustrated in Fig. 4 below and on Fig. 6 page 20. These compact notations require a special convention such that if $D(i) = 0$ for one of the i, we put $u_{m+1,0} \stackrel{def}{=} s_{m,1}, \quad m \geq 0$, which is part of the secret key and a constant for any given round. The Boolean $Z : \mathbb{F}_2^6 \to \mathbb{F}_2$ was specified in earlier Section 3.2.

$$\begin{aligned}
u_0 &\stackrel{def}{=} s_1 \\
U_9 &= u_{D(9)} \oplus f \\
U_8 &= u_{D(8)} \oplus U_9 \oplus u_{D(9)} \oplus Z(s_2, u_{P(1-5)}) \\
U_7 &= u_{D(7)} \oplus U_8 \oplus u_{D(8)} \oplus u_{P(6)} \\
U_6 &= u_{D(6)} \oplus U_7 \oplus u_{D(7)} \oplus Z(u_{P(7-12)}) \\
U_5 &= u_{D(5)} \oplus U_6 \oplus u_{D(6)} \oplus u_{P(13)} \\
U_4 &= u_{D(4)} \oplus U_5 \oplus u_{D(5)} \oplus Z(u_{P(14-19)}) \oplus s_2 \\
U_3 &= u_{D(3)} \oplus U_4 \oplus u_{D(4)} \oplus u_{P(20)} \\
U_2 &= u_{D(2)} \oplus U_3 \oplus u_{D(3)} \oplus Z(u_{P(21-26)}) \\
U_1 &= u_{D(1)} \oplus U_2 \oplus u_{D(2)} \oplus u_{P(27)}
\end{aligned}$$

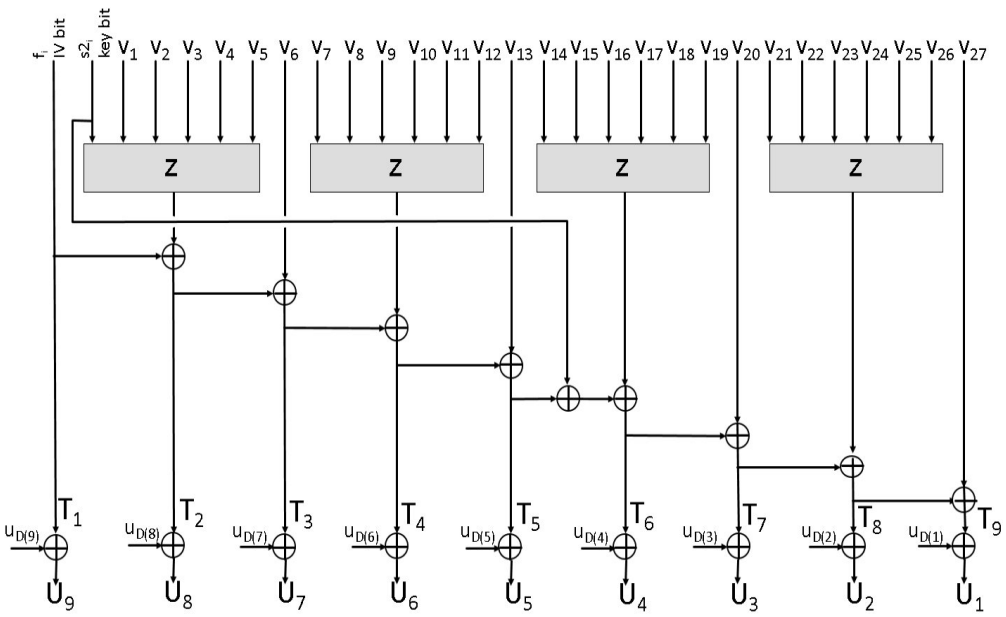

Fig. 4. Internal structure and T inside one round of T-310.

Example. For example $P(27) = 1$ means that we connect rightmost output U_1 (or state bit u_1 or 1 in green from I^4 on Fig. 5) to input v_{27} in the next round cf. Fig. 4. Then $D(9) = 4$ means that first bit u_4 from I^1 on Fig. 5 was XORed to the state when computing U_9, which U_9 becomes bit 33 of I^4 in the next round.

4.3 Design Criteria for the Round Function

We denote by S1 any of 120 key bits $s_{m,1}$, $m \geq 1$ and S2 any of the $s_{m,2}$. We observe that only S2 bits are used as input to $Z()$. cf. Fig. 4. We found a document [25] which explains the origin why S2 is used twice inside this component cf. Fig. 4. More precisely on page 54 of [25] from 1973 we discovered an earlier (weaker) design for the component $T()$ where $S2$ is used only once, cf. Fig. 4. The authors report that for exactly half of the inputs of the round function ϕ, the 9-bit output would be independent of the key input $S2$ which is avoided in SKS V/1 and T-310 ciphers.

4.4 On Weakness of the T-310 Round Function

A comparison between the structure of $T()$ and many modern block ciphers suggests that it is potentially weaker. Informally, the non-linear functions on Fig. 4 do not "mask" the input bits completely. Even though, none of 27 inputs v_i are copied directly at the output, they somewhat pass through and we can fear that the apparent complexity of $T()$ cf. Fig. 4 can potentially be undone or reduced by elimination.

One type of interesting fact is that for example $T_1 \oplus T_2$ reveals the output of first $Z()$ which could be biased under some conditions and reveal some information to the attacker. Our research shows that correlation attacks are quite well defended against in T-310 by mandating a bijective round function cf. [13, 14].

Another type of property of interest is that for example $T_2 \oplus T_3$ reveals the input v_6, and similarly $T_8 \oplus T_9$ reveals the input v_{27}. This property will be exacerbated by the fact that the KT1 keys which we will study in Section 5 below, do specifically allow a large number of outputs of D to be identical to outputs of P, which is forbidden for KT2 keys cf. [14]. Therefore additional cancellations can be imagined as the T_i are later XORed to some of the $v_{D(i)}$ and cancellations are permitted cf. round function formulas and Fig. 4. In this article we are going to show that this indeed is a problem and that KT1 keys can be indeed very weak, cf. Lemma 6.0.1 page 19.

5 On KT1 Keys and Their Security

The original documentation of T-310 specifies some 20 or more very technical conditions which the T-310 keys should satisfy, cf. [27] and [14]. We focus on the KT1 class of keys which was the primary type of keys used in actual historical communications in 1979-1990 (cf. Def. 5.0.1 below and [28, 17, 14]).

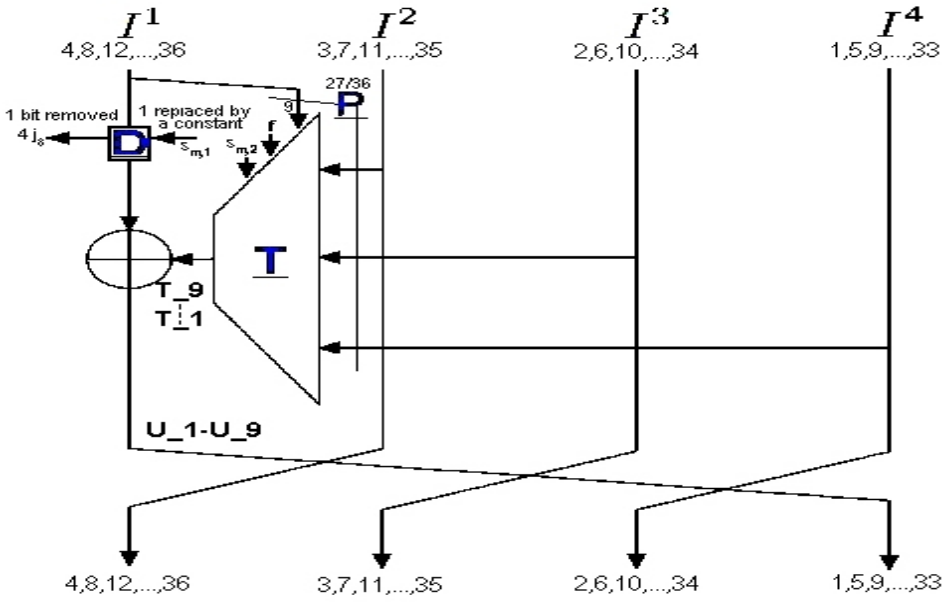

Fig. 5. With KT1 keys D uses 8 bits from the left branch I^1, one is dropped and replaced by one of the key bits $s_{m,1}$. P can take extra bits from I^1.

Definition 5.0.1 (KT1 key). We say that a triple D, P, α belongs to KT1 class of keys if all the following conditions are simultaneously satisfied:

D and P are injective, $P(3) = 33, P(7) = 5, P(9) = 9, P(15) = 21, P(18) = 25,$
$P(24) = 29,$ Let $W = \{5, 9, 21, 25, 29, 33\} \forall_{1 \geq i \geq 9}$ $D(i) \notin W$ and $\alpha \notin W$ and,
Let $T = (\{0, 1, \ldots, 12\} \backslash W) \cap (\{P(1), P(2), \ldots, P(24)\} \cup \{D(4), D(5), \ldots, D(9)\} \cup \{\alpha\})$
Let $U = (\{13, \ldots, 36\} \backslash W) \cap (\{P(26), P(27)\} \cup \{D(1), D(2), D(3)\})$ then we require
that: $|T \backslash \{P(25)\}| + |U \backslash \{P(25)\}| \leq 12, D(1) = 0$ and, there exist $\{j_1, j_2, \ldots, j_7, j_8\}$
a permutation of $\{2, 3, \ldots, 9\}$ which defines $D(i)$ for every $i \in \{2, 3, \ldots, 9\}$
as follows: $D(j_1) = 4, D(j_2) = 4j_1, D(j_3) = 4j_2, \ldots, D(j_8) = 4j_7$ and $P(20) = 4j_8$
$(D(5), D(6)) \in \{8, 12, 16\} \times \{20, 28, 32\} \cup \{24, 28, 32\} \times \{8, 12, 16\}$ and,
$P(6) = D(8), P(13) = D(7), P(27) \neq 0 \bmod 4, \forall_{1 \geq l \geq 9} \exists_{1 \geq i \geq 26} P(i) = 4 \cdot l$
$D(3) \in \{P(1), P(2), P(4), P(5)\}$ and $D(4) \notin \{P(14), P(16), P(17), P(19)\}$
$\{P(8), P(10), P(11), P(12)\} \cap \{D(4), D(5), D(6)\} = \emptyset$

5.1 Examination of Real-Life Keys

In [17] we find 7 keys from the period of 1979-1990 numbered 14,21,26,30,31,32,33. We have verified that these 7 keys satisfy all the conditions of Def. 5.0.1.

5.2 Key Observation About KT1 Keys

We have discovered the following property:

Theorem 5.2.1 (KT1 Cycling Theorem). For every key in the class KT1 if we replace the first value $d[1] = 0$ by $P(20)$ and we divide all values by 4, we obtain a permutation E of the set $\{1, \ldots, 9\}$ with exactly one cycle.

Proof: Following the definition of KT1, there exist $\{j_1, j_2, \ldots, j_7, j_8\}$ a permutation of $\{2, 3, \ldots, 9\}$ such that $D(j_1) = 4, D(j_2) = 4j_1, D(j_3) = 4j_2, \ldots, D(j_8) = 4j_7$ and $P(20) = 4j_8$ We claim that then, the following permutation E represented as 1 single cycle [in order], is what we are looking for: $1, j_8, j_7, \ldots, j_2, j_1, 1$ which closes the cycle. Indeed 1 is mapped to j_8 due to $P(20) = 4j_8$, then we have $D(j_8) = 4j_7$ which implies that j_7 must follow position j_8 etc, finally j_1 is mapped to 1 due to $D(j_1) = 4$.

Moreover we also have

Theorem 5.2.2 (KT1-D Counting Theorem). There exist exactly $18 \cdot 6!$ valid choices for an injective $D : \{1 - 9\} \to \{0, 4, 8, 12, \ldots, 36\}$ such that $(D(5), D(6)) \in \{8, 12, 16\} \times \{20, 28, 32\} \cup \{24, 28, 32\} \times \{8, 12, 16\}$ and such that a suitable $j[]$ exists.

Proof: In principle there are 9! choices for $D : \{1 - 9\}$. However we have only $18 = 2 \cdot 3^2$ choices which are allowed for $D(5), D(6)$. Then in theory we have $18 \cdot 7!$ possibilities for D left, from which we need however to exclude all those where the one single cycle property of Thm. 5.2.1 is not valid, as this property is required[3]. We need then to see that in every of 18 cases, for example $D(5) = 8 = 4 \cdot 2$ and $D(6) = 20 = 5 \cdot 4$ exactly 1/7 of all possible permutations have one single cycle. We need to count permutations E of $\{1 - 9\}$ such that $E(5) = 2$ and $E(6) = 5$ where $E(x) = D(x)/4$ and such that E has one single cycle. We also

[3] From inspection of KT1 conditions the proof of Thm. 5.2.1 actually uses.

need to check that none of 18 cases allowed for $E(5-6)$ leads to a situation of type $E(x) = y$ and $E(y) = x$. In contrast situations of type $E(6) = 5$ and $E(5) = 2$ which would be consecutive in a cycle are allowed but these do not prevent the complete permutation form having just one cycle. In the case of type $E(6) = 5$ and $E(5) = 2$ we just complete the cycle by deciding $E(5) = x$ out of 6 possibilities, excluding 2,6,5, then $E(x)$ can take 5 values, etc, overall we get 6! way of completing the cycle. In the case of type $E(6) = 7$ and $E(5) = 2$ which is not connected, we have 5 numbers 1-9 not yet used. There are 6 ways to decide how many elements need to be inserted after 7 and before 5, any number between 0 and 5, and then there are 5! ways to place remaining 5 elements then after 7 and after 2 to form a single cycle. Again we have 6! possibilities. This gives the desired result of $18 \cdot 6!$ possibilities for the number of possible D which are allowed by the KT1 rules.

Remark. We have checked by computer simulation that all of $18 \cdot 6!$ possibilities are taken, and each leads to a vast number of actual valid KT1 keys.

5.3 KT1 Key Generation

We provide a simple and efficient method aimed at enumerating KT1 keys without any special properties, approximately uniformly, and at random.

1. We select one of $18 \cdot 6!$ valid choices of $D()$ from Thm. 5.2.1. A full list is pre-computed and stored.
2. We determine $P(20)$ as the only value of type $4k, 0 < k \leq 9$ not taken by $D()$ and we put $P(3) = 33, P(7) = 5, P(9) = 9, P(15) = 21, P(18) = 25, P(24) = 29$ and $P(6) = D(8), P(13) = D(7)$.
3. Now for all value of $P()$ not yet decided, we place $D(3)$ so that $D(3) \in \{P(1), P(2), P(4), P(5)\}$ and also place all multiples of 4 not already taken so that $\forall_{1 \geq l \geq 9} \exists_{1 \geq i \geq 26} P(i) = 4 \cdot l$.
4. Now we generate other values $P(i)$ at random avoiding values already taken to insure injectivity.
5. For all other KT1 conditions we restart all steps until a valid KT1 key is found, which occurs with a relatively large probability of about 0.19.

5.4 KT1 Key Symmetries and Entropy

We now evaluate the size of KT1 long-term key space.

Lemma 5.4.1 (KT1 key size). The size of the space of KT1 keys is approximately $2^{83.2}$ elements.

Justification: The best evaluation previously known was that the key space for D, P only and without α is between 78.1 and 79.7 bits, cf. page 56 in [27]. In addition there are about $\log_2(36 - |W|) \approx 2^{4.9}$ possibilities for α in each case which gives a range of between 83.0 and 84.6 bits total. Can we provide a more precise figure? From the definition of KT1 above, and by careful inspection we observe that if we permute in arbitrary way $\{P(1), P(2), P(4), P(5)\}$ we always get a valid KT1 key as the definition never makes any distinction between these indices. The same applies to $\{P(8), P(10), P(11), P(12)\}$ and also to the pair $\{P(21), P(23)\}$. Given than P is injective, it is therefore sufficient to count KT1 keys in which the values in each of these 4 sets are ordered in an increasing order, and multiply the result by $2(4!)^2 = 2^{10.2}$. This makes our set of keys smaller and easier to study. First we have exactly $18 \cdot 6! \approx 2^{13.7}$ valid choices of $D()$ from Thm. 5.2.1 which always pass step 2, 3, 4 and will enter step 5. Then for each of $2^{13.7}$ cases we know the full d and we need to see how many valid versions of p exist so that their combination is a valid key. Our simulations show that the number of possibilities for $p[1-16]$ is about $2^{30.3}$ and for $p[17-27]$ about $2^{32.1}$. Moreover, we found that the probability that such two halves of the description of p can be combined to form a valid KT1 key is about $2^{-8.0}$. Overall we conclude that the key space of KT1 keys has about $2^{10.2+13.7+30.2+32.1-8.0+4.9} \approx 2^{83.2}$ for complete LZS with D, P, α.

6 How to Make T-310 Weak w.r.t. Linear Cryptanalysis

We now present an explicit constructive method to weaken the T-310 cipher.

Lemma 6.0.1 (Weak Setup for T-310). For every long-term key in T-310 such that $D(1) = 0$, $D(2) = 4$ and $P(27) = 6$ the T-310 block cipher has two invariant linear approximations for 2 rounds true with probability 1 which are

$[1,3,5] \to [1,3,5]$ and $[2,4,6] \to [2,4,6]$. Here state bits are numbered $1, 2, \ldots 36$ as in [28, 27] and the notation $[1,3,5]$ means that we XOR bits 1,3 and 5 together.

Proof: We recall the last equation of Section 4.2:

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

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

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

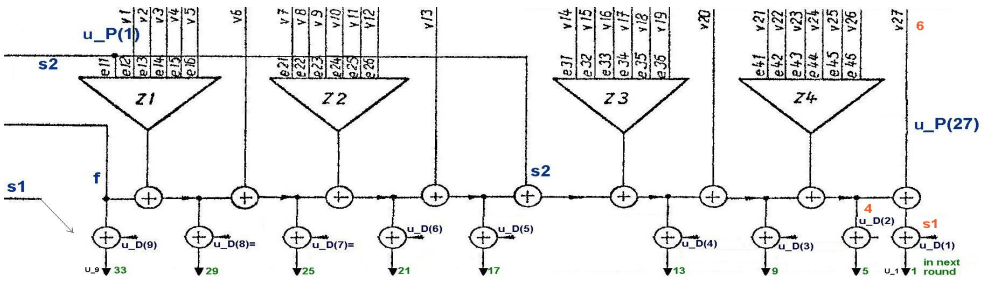

Fig. 6. For convenience we show the bits involved here, cf. also Fig. 4.

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

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

Numerous similar linear approximations exist and in isolation they have very limited value, if they cannot be connected to some other well-chosen approximations. Using that fact that bits $\neq 4k$ are just shifted in our Feistel cipher with 4 branches, this can be trivially extended for one round before as follows:

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

Finally we have $[1] \to [2] \to [3]$ for two rounds also with certainty, which property can be combined with the previous one and we obtain finally that:

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

Similarly we also have

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

Moreover all this can indeed happen for the KT1 keys, see for example our key 783 specified below. We will call such keys "LC-weak" keys:

Definition 6.0.2 (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.

6.1 Vulnerability Assessment of KT1 Keys

How many keys are concerned by this vulnerability? In this article we show:

Lemma 6.1.1 (Weak KT1 key size bound). The probability that a KT1 chosen at random has at least two invariant linear approximations true with probability 1 is at least 0.3%.

Justification: We recall from Section 5 that for the KT1 keys we always have $D(0) = 1$ and $D(j_1) = 4$. Therefore in order to make a KT1 keys satisfy our linear attack of Lemma 6.0.1 we just need to satisfy 2 (and not 3) conditions: $j_1 = 2$ and $P(27) = 6$. Which fraction of $2^{83.2}$ keys of Lemma 5.4.1 satisfy these conditions. The first condition $j_1 = 2$ occurs with probability of about $1/8 \approx 2^{-3}$. The probability that second condition knowing that $j_1 = 2$ is a bit harder to evaluate. Therefore an approximative estimation would be $1/8 \cdot 1/36 \cdot 2^{83.2} \approx 2^{75.0}$ weak KT1 keys or 0.3% of all KT1 keys.

6.2 Weak KT1 Keys with Multiple Linear Invariants

We have tested many other KT1 keys generated essentially at random (cf. Section 5.3) and discovered that some keys are even weaker than what we expect from Lemma 6.0.1. For some KT1 keys the vulnerability is stronger and we get more than two invariant linear approximations true with probability as high as 1, which can propagate for an arbitrary number of rounds. Below we give three examples of vulnerable KT1 keys we discovered.

Currently the most pathological KT1 key known is 784. This key 784 can be characterized in a very simple way as follows. It exhibits simultaneously the same 8-round periodic linear characteristic as key 788 AND exactly the same 2-round periodic linear characteristic as key 783. Moreover these involve two disjoint and linearly independent sets of linear combinations with 10=8+2 total of linear invariant properties, which happen to work with probability 1 for all keys and

Table 2. KT1 keys with multiple invariant linear characteristics for T-310.

LZS nb	D	P	rounds	solutions
783	0,4,8,32,28,16,12,20,24	8,32,33,11,1,20,5,26,9,24,4,7,12,2,21, 34,28,25,3,36,31,13,18,29,19,16,6	2	2
788	0,4,36,32,24,8,12,20,16	26,19,33,36,4,20,5,27,9,17,2,11,12,31, 21,22,1,25,7,28,16,24,32,29,8,30,34	8	8
784	0,4,32,28,24,8,12,20,16	3,1,33,11,32,20,5,26,9,2,4,7,12,24,21, 34,31,25,8,36,28,13,18,29,19,16,6	8	10

IVs. Below we provide full internal details about both periodic properties which are self-explanatory and also show which exact key/IV bits are used:

```
[1,3,5]-s1->[2,4,6]->[1,3,5]
[9,13]->[10,14]->[11,15]->[12,16]->[25,29,33]-f->
                        [26,30,34]->[27,31,35]->[28,32,36]->[9,13]
```

6.3 More Weak KT1 Keys

A more detailed study done by ourselves with help of UCL students doing a COMPGA18 Cryptanalysis project on this topic in 2018, shows that there exist numerous other ways to achieve a similar result. Overall we found that about 3% of all KT1 keys are LC-weak (i.e. they admit linear approximations true with probability 1). This is 10 times more than properties studied in this article cf. Lemma 6.1.1. Extensive computer simulations show that among all possible $8! = 40320$ values for $\{j_1, j_2, \ldots, j_7, j_8\}$ in KT1 keys, some 4549 which is 11.3% are potentially compatible with LC-weak keys.

6.4 On Importance of LC-Weak KT1 Keys

Weak keys do not matter... unless their frequency is quite large, see [10, 11] for specific examples of weak keys which do have an impact on the security evaluation of a cipher because their frequency is sufficiently large. With KT1 keys in T-310 the weak long-term keys are also of concern: 3% chance means that weak keys could have been accidentally generated and used to encrypt government communications. A detailed examination of all real-life keys from [17], shows that this has not happened. This brings a further question whether

our weak-key attack can be generalized to include yet more weak keys, which question we study in Section 7 below.

7 Non-Linear Algebraic Backdoors and Related Research

A natural generalization of the linear invariant properties which are demonstrated to exist for a substantial fraction of KT1 keys in T-310, are higher degree non-linear invariant properties. Current literature on this topic [24, 6, 7] shows several constructions of weak ciphers with multivariate equations of degree 2 [6] or higher. A recent PhD thesis [2] contains a construction of a toy block cipher operating on 6 bits with a non-linear trapdoor due to a hidden vector space law which is not apparent to the attacker and will not be detected by routine Linear Cryptanalysis.

We conjecture that it should be possible to embed a non-linear "backdoor" or weakness in T-310 with KT1 keys or similar standard setup. In the current article we achieve this objective for linear equations. More generally we ask the following question: Is it possible to find a non-linear function $f()$ such that the value of $f()$ is an invariant preserved after an arbitrarily large number of rounds of T-310? A non-linear f would allow for a construction of stronger forms of "backdoors" or deliberate weakness in T-310, which could be substantially harder to detect.

8 Is Linear Cryptanalysis Relevant to T-310?

This is an interesting and highly non-trivial question. In this article we ignored the question of how exactly the block cipher inside T-310 is used in encryption. It turns out that Eastern German cryptologists have mandated a specific and remarkably strong encryption operation mode for their block cipher. Extremely few bits from the cipher state are used for encryption: less than 1 bit every 127 rounds, cf. [28, 13, 14]. The cryptanalytic literature knows extremely few attacks which operate under such extremely difficult circumstances cf. Section 2.1. in [13] and [9].

Our linear cryptanalysis weakness we construct in this article can concern linear combinations up to 10 bits out of 36 in each round, yet it does not in the slightest lead to any property involving single bits. For this reason it is not clear how much T-310 is actually weakened by such a modification. Potentially one could prove that no bias exists on individual bits used for encryption and therefore potentially we are not yet able to break T-310 used in encryption in any meaningful way.

9 Conclusion

In this article we show that Linear Cryptanalysis and systematic study of ciphers in terms of non-linearity and Boolean polynomials [a.k.a. ANF] are quite old. We show that a careful systematic study of these properties was a routine task in Eastern Germany in the 1970s. An interesting question is then why the designers of East German T-310 cipher machine has NOT made resistance against linear attacks obligatory for their rather carefully designed class of KT1 keys. In this article we show a specific counter-example: we construct weak keys which are 100% compliant with the KT1 specification. Our Lemma 6.1.1 shows that at least 0.3% out of 2^{83} KT1 keys are weak w.r.t. LC, and further study shows that some 3% are weak. Therefore it is plausible that weak keys could be generated and used in the real life. A careful examination of principal real life keys from 1979-1990 cf. Section 5.1 and [17], shows that none of these keys are vulnerable.

Some of our linear vulnerabilities seem quite strong, up to 10 out of 36 linear combinations of internal state bits can be known to the attacker for any number of rounds. However these still do not really allow to decrypt T-310 communications as far as we can see. This is due to the fact the T-310 uses extremely few bits of the internal state for the actual encryption. It remains an open question if or how such (strong) linear vulnerabilities could (or not) be exploited in order to decrypt T-310 communications. In Section 7 we suggest a higher-degree non-linear generalization of our weak-key attack.

References

1. Eli Biham: *On Matsui's Linear Cryptanalysis,* Eurocrypt'94, LNCS 950, Springer-Verlag pp. 341-355.
2. Marco Calderini: *On Boolean functions, symmetric cryptography and algebraic coding theory,* Ph.D. in Mathematics, Supervisor: Prof. Massimiliano Sala, University of Trento, Italy, April 2015
3. D.W. Davies, *Some Regular Properties of the Data Encryption Standard,* Crypto'82, pp. 89-96, Plenum Press, New-York, 1982.
4. D. Davies and S. Murphy, *Pairs and Triplets of DES S-Boxes,* Journal of Cryptology, vol. 8, Nb. 1, pp. 1-25, 1995.
5. Nicolas Courtois, Guilhem Castagnos and Louis Goubin: *What do DES S-boxes Say to Each Other ?* Available on `eprint.iacr.org/2003/184/`.
6. Nicolas Courtois: *Feistel Schemes and Bi-Linear Cryptanalysis,* in Crypto 2004, LNCS 3152, pp. 23-40, Springer, 2004.
7. 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.
8. Nicolas Courtois: *Security Evaluation of GOST 28147-89 In View Of International Standardisation,* in Cryptologia, volume 36, issue 1, pp. 2-13, 2012.
9. 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.
10. 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`.
11. Nicolas Courtois: *On Multiple Symmetric Fixed Points in GOST,* in Cryptologia, Iss. 4, vol 39, 2015, pp. 322-334.
12. 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.

13. 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
14. Nicolas T. Courtois, Maria-Bristena Oprisanu: *Ciphertext-Only Attacks and Weak Long-Term Keys in T-310,* to appear in Cryptologia in 2017.
15. Arbeitsgebiet 113: *Sachstandbericht zur Arbeit am Chiffrieralgorithmus des Gerätes T 310/50,* MfS-020-XI/674/76, 51 pages, Berlin, 31 December 1976, also known as MfS-Abt-XI-532
16. Jörg Drobick: *T-310/50 ARGON,* a web page about T-310 cipher machines consulted 19 March 2017, http://scz.bplaced.net/t310.html
17. Jörg Drobick: *T-310 Schlüsselunterlagen,* a web page which enumerates several different known long-term keys for T-310 from 1973-1990, consulted 21 January 2017, http://scz.bplaced.net/t310-schluessel.html
18. 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.
19. Horst Feistel: *Cryptography and computer privacy;* Scientific American, vol. 228, No. 5, pp. 15-23, May 1973.
20. Anne Tardy-Corfdir, Henri Gilbert: *A Known Plaintext Attack of FEAL-4 and FEAL-6,* Crypto'91, LNCS 576, Springer, pp. 172-181, 1992.
21. Mitsuru Matsui: *Linear Cryptanalysis Method for DES Cipher,* Eurocrypt'93, LNCS 765, Springer, pp. 386-397, 1993.
22. 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.
23. J. Pieprzyk and G. Finkelstein: *Towards effective nonlinear cryptosystem design,* IEE proceedings E - Computers and Digital Techniques, Vol. 135 Iss. 6, November 1988, pp. 325-335, ISSN 0143-7062.
24. Vincent Rijmen and Bart Preneel, *A family of trapdoor ciphers,* In FSE'97, pp. 139–148, Springer, 1997.
25. Archive document known as MfS-Abt-XI-183, which contains a selection of pages extracted from MfS-020-Nr. 747/73, 1973.
26. ZCO: *Charakterisierung der Booleschen Funktion Z,* handwritten document, MfS-020-XI/493/76, 24 pages, 1976.

27. 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.*
28. *Klaus Schmeh: The East German Encryption Machine T-310 and the Algorithm It Used,* In Cryptologia, 30: 3, pp. 251–257, 2006.
29. Adi Shamir: *On the security of DES,* Crypto'85, LNCS 218, Springer, pages 280-281.
30. VEB Steremat "Hermann Schlimme", *Gerätesystem SKS V/1, Gerät DE1,* Zeichnungs-Nr. 310017, Band 2, also known as MfS-Abt-XI-415, and a.k.a. B 86/1-31/77, Berlin, 1976.
31. Zhegalkin polynomial, Wikipedia entry, `https://en.wikipedia.org/wiki/Zhegalkin_polynomial`