The History of the Development and the Analysis of the Cipher Machine T-310/50 and the Procedure ARGON by the ZCO

Wolfgang Killmann
Neuenhagen, Germany
wkillmann@gmx.de

Abstract

This paper describes important aspects of the 10 years of development and the 18 years of security analysis of the cipher machine T-310/50 and the procedure ARGON by the Central Cipher Authority of the GDR. The threat model of the analysis is pictured. Examples of the security analysis of the cipher algorithm, machine, procedure and key management are provided. The focus is on the analysis of the operating functions of the T-310/50 (operating analysis), including the analysis of operating errors, as well as the analysis of the instruction manual for the cipher procedure ARGON. The possibilities of obtaining information by an attacker from traffic reconnaissance in general and decryption attacks in particular are assessed.

1 Introduction

The cipher T-310 was developed by the Central Cipher Authority ("Zentrales Chiffrierorgan", ZCO) of the German Democratic Republic (GDR) in the 1970s. It was used widely for the protection of teletype communication up to security level secret ("Geheime Verschlusssache") in the 1980s.[1] By the end of the GDR almost all cipher machines T-310/50 were destroyed in 1990. The last use case of the cipher T-310 was for secure governmental communication between GDR and German Federal Republic (Stephan, 2022). The cipher T-310 was kept secret until October 2003.

The development and the analysis of all components and procedures were closely linked together in order to ensure the security of the cipher T-310. The ZCO developed the algorithm together with all long-term keys and the guidance documentation. It also produced the short-term keys for the distribution by the cipher services and their specialists analyzed the cipher and the operational usage of the cipher T-310 over its whole life time. The industry produced the T-310/50 machine.

Today, everyone can see what the T-310 looks like and how it works. It is now on display at the museums, e.g. NVA Museum Harnekop and the Deutsches Museum München. A software simulation of the T-310/50 is available on http://scz.bplaced.net/freeware.html. The algorithm T-310 is demonstrated by the open-source software CrypTool 2 available on https://www.cryptool.org/en/ct2/downloads.

To understand the reasons and details why it works this paper highlights important aspects of the ten years development and the eighteen years of security analysis by the ZCO. Section 2 provides a short historical overview of the development of cipher T-310. Section 3 describes the general threat model used for the security analysis of the T-310. The algorithm (Section 4), the machine (Section 5), and the procedure (Section 6) build together with the overlapping key management (Section 7) bottom-up the cipher.

They are addressed by separated, but dependent hierarchical aspects of the security analysis. The structure of this paper follows this layered approach.

We describe the cipher model of T-310 for the systematic of the security analysis. The *cipher* comprises all regulations and means for the encryption and the corresponding security functions including the key management. The *keys* are variable parts of the cipher. The cipher T-310 uses long-term keys implemented by circuit boards in the machine and short-term keys on punch cards. The *algorithm* is the mathematical model of the encryption and the data authentication. The algorithm T-310 is implemented in hardware and pro-

[1] There were four security level: This is the second hightest.

vides only the encryption (Section 4). The *cryptographic module* implements the algorithms and possibly other security functions (e.g. generation of random numbers) in hardware or software as part of a dedicated *cipher machine*, in our case the T-310/50. The *cipher material* comprises cipher machine and the key material. The *cipher procedure* defines how to use the cipher material by an human operator or by other devices. The T-310 cipher procedure is named ARGON (Section 6). The cipher includes also the *key management*, i.e. the generation of keys, the production and the distribution of key materials (not shown in Figure 1) and the key handling by the crypto officer in the exclusion zone.

2 Time Line of T-310 Development

The ZCO was built in 1951. It developed manual ciphers in the 1950s and cipher machines with the VERNAM cipher in the 1960s. The GDR cipher services used Soviet cipher machines with internal keys, i.e. the key is shorter than all the text encrypted withthis key. In the 1970s the ZCO developed their first own ciphers with internal keys: the cipher SKS for the signal command system SKS V/1 and the teletype cipher T-310.

The first version of the teletype cipher T-310 (code name PUMA) was developed by ZCO from 1973 to 1975. It was designed for encryption of texts on five-hole and eight-hole punched tapes. In 1974 two ZCO cryptographers developed two new algorithms: a linear recursion for the initial vector with prime length of the period and a substitution algorithm for five bit and eight bit codes. In addition, a new technical base was available (e.g. new TTL chips; 1 bit updated to 4 bit). This allowed for cryptographic improvements (e.g. longer short-term key, bigger internal state). The development of the cipher T-310 started with the tactical-technical requirements for a machine T-310 in 1974. The machine shall work with teleprinter and data communication devices in stationary and mobile stations. In 1977 the A-phase of the development ("A" stands for "applied research") was finished and an A-prototype was available for trials. It comes out that the functionality and the complexity of the machine must be reduced (e.g. only five-bit code encryption, doubling of the complication unit on three plates instead of four) in 1978. The algorithm of the machine was fixed in 1979. A cryptographic analysis of T-310/50 was produced in 1980 (ZCO, 1980). It followed extensive trials of the procedure ARGON with the K5-prototypes of machine T-310/50 ("K" stands for "development and launch of products"). The modified 50 K5-prototypes were used as T-310/51 with procedure SAGA for transmission of tactical reconnaissance data by the GDR navy. The use of ARGON with mass-produced T-310/50 began in 1982. There were as many as $3,835$ cipher machines T-310 in active service by the GDR government, army, security services and political organizations.

The T-310/50 was the last cipher machine made up of small-scale integrated circuits in transistor–transistor logic (TTL). Only the optional code converter of T-310/50 used a microprocessor. The maintenance service used a special computer "Prüfrechner PR310/2" for functional checks of T-310/50 and fault finding in 1985. Telex was the standard form of text communication in governmental networks of the GDR in the 1970s and 1980s. The T-310/50 was used also for slow data transmission with "teletype modems". The next generation of ZCO cipher machines were dedicated for encryption for data storage and transmission (e.g. T-325/POLLUX) including PCM30-base systems for speech (T-311/SELEN) (Drobick, 2023). The new machines used microcomputers at least for the control of the cryptographic module.

The ZCO analyzed the security of the algorithm T-310, the machine T-310/50 and the procedure ARGON until the end of their use in 1990. The ZCO starts the development of the algorithm T-310 with two mathematicians in 1973. The core of algorithm T-310 was derived from the algorithm SKS. The group of cryptologists working on the algorithms T-310 grows to about ten mathematicians in the late 1970s. Additional fifteen cryptologists worked on security analysis of the machines T-310/50 and T-310/51, the procedures and the oversee of the technical development. The analysts were supported by two programmers, engineers, technicians and other staff members of the ZCO building and running special programs and devices, providing literature and other services.

3 General Security Model

The starting point of the security analysis is the security model. The security model describes the threats to the assets (threat model) to be mitigated

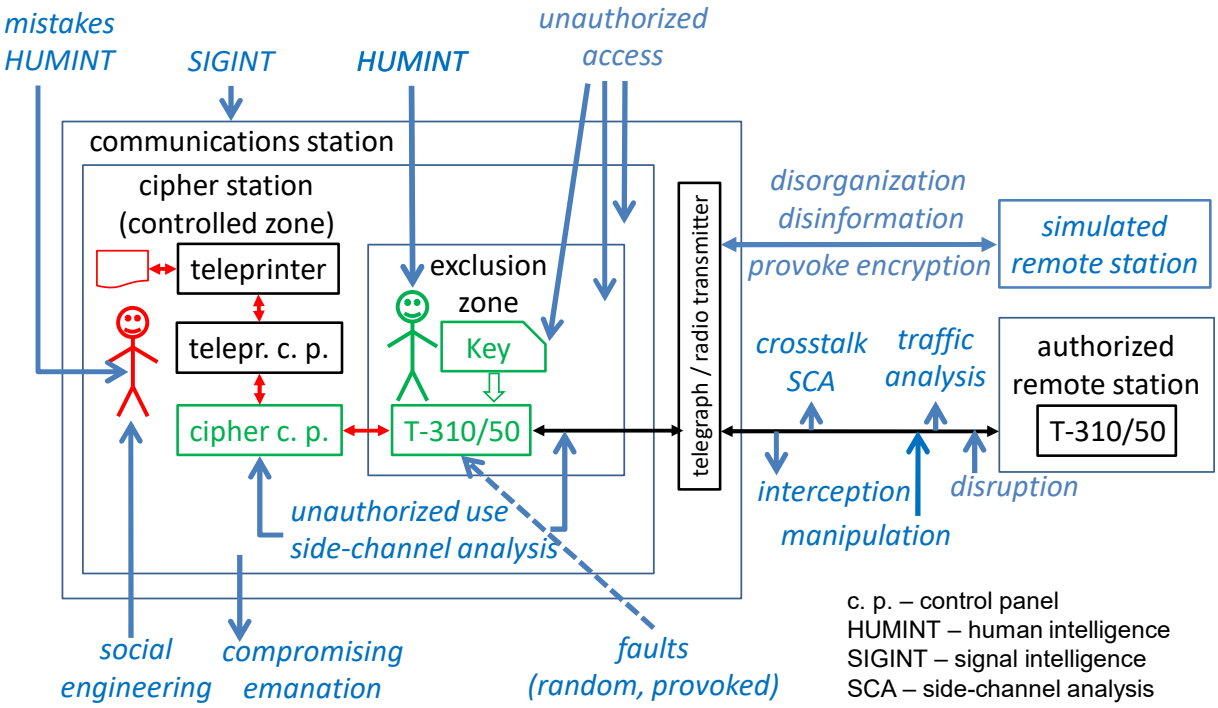

Figure 1: Threat model for the cipher machine T-310/50

by the security measures (cipher model) according to the enforced security policy. The security analysis needs a comprehensive and detailed understanding of the threats in order assess the effectiveness and the security of the cipher and if necessary of the additional countermeasures.

Figure 1 illustrates the threat model used for the cipher T-310. The primary asset to be protected are the state secrets represented in the plaintexts. The security policy requires the protection of the secrecy, integrity and availability of the state secrets. The cipher T-310 (drawn in green) was designed to ensure the secrecy of plaintexts (drawn in red) by encryption into ciphertext (drawn in black).

The operator transmits and receives non-classified and classified texts by teleprinter using cipher machine T-310/50 and the cipher procedure ARGON. In case of encryption the knowledge of the ciphertexts gained by interception of the communication line is always assumed. The adversary may also disrupt or interfere with communication and even imitate authorized communication.

The key has the same value for the adversary as all plaintexts encrypted with this key. Therefore, the cryptanalysis and the countermeasures distinguish between attacks on the plaintexts and on the keys (Section 4). Any information about the keys, the plaintexts or the internal processes of the cipher machine support the cryptanalysis. Therefore, the attacker analyzes not only the intercepted ciphertext but also the compromising emanation, the transmitted signal, the traffic, and so forth (Section 5.3). In case of state secrets any information about the transmission is of interest as well, e.g. the direction, the time and the priority of the transmission, the length of the plaintexts etc. Because of the general rules of telex and the combination of plaintext and ciphertext in the message the T-310 cannot prevent traffic analysis. But the T-310 must not provide additional marks supporting the traffic analysis (Section 5.1).

As a rule, the cipher is applied correctly. Any aberrance by technical fault in the machine or by mistake by applying the procedure may result in weak encryption and may enable attacks. The analysis of the security impact of every possible aberrance is not traceable. Any aberrance shall be avoided as potential vulnerability. Section 5.2 describes self-protection against technical faults. Section 6.2 discusses the robustness of the procedures and some security measures against operational errors.

In case of state secrets the security analysis shall identify possibilities and indication of covert adversary actions by operators or other persons despite of the personnel and organizational security measures. Section 6.2 provides an example.

The security analysis of the cipher may start with the algorithm but shall comprise all components up to the cipher network.

4 The Cipher Algorithm T-310

The strength of the cipher algorithm is the absolute necessary condition for the strength of the cipher (but as we see later not the only one). The cipher algorithm T-310 is defined in (Killmann and Stephan, 2021; Killmann, 2023). The T-310 is a stream cipher as a symmetric encryption system combining a sequence of teletype characters with the keystream by one character at a time, using a invertible function (like XOR). The structure of the cryptographic module is depicted in Figure 2 (Killmann and Stephan, 2021).

The short-time key of 240 bits (including 10 parity bits) is stored on a punch card. The input unit repeats cyclically the key components $S1$ and $S2$ building the s-sequences (Figure 3). The initial vector of 61 bits is randomly generated for encryption and derived from the message for decryption. The synchronization unit generates with the initial vector the linear shift register sequence f with period length $2^{61}-1$ (which is a prime number). The complication unit generates the keystream a controlling the substitution. For each teletype character 10 out of 13 bits of the a-sequence are used. The substitution combines each teletype character of five bits with ten bits of the keystream a. The mappings of the substitution algorithm build a double transitive permutation group of the teletype characters.

The complication unit is the core of the algorithm T-310. It implements a nonlinear shift register with the transition function φ of the states U as depicted in Figure 3 (Killmann and Stephan, 2021).

The sequences s and f act as parameters of φ. The long-term key defines the structure of the mapping φ. It defines the selection and the permutation of the 27 bits of the internal state U as inputs of the Boolean functions, the 9 bits XORed to the feedback and the place of the output bit α of the register U. After 127 internal clocks one output bit is read for the a-sequence.

The cryptographic strength of the complication unit is crucial against attacks on the short-term keys. It comes out that the long-term key is critical for cryptographic strength of the cipher. Although kept secret the long-term keys are assumed fixed and potentially known to the attacker (Section 7). The specialists of the ZCO analyzed deeply the function φ depending on the long-term keys. The ZCO applied a procedure for the approval of long-term keys intended for application in the field (Killmann and Stephan, 2021; Killmann, 2023). These carefully selected long-term keys allowed to prove important security features of the cipher. If the parameters of φ are freely chosen, then the bijective φ generates a permutation group over the set of internal states U. The cryptologists proved that this group is transitive in the late 1970s. In the early 1980s they ensured that the group is the alternating group. These features prevent some simplified models of the complication unit. In the mid 1980s a new quality of results were reached in case the parameters of φ are deterministic sequences derived from the short-term key and the initial vector. The period of the a-sequence controlling the substitution is with high probability a multiple of the period of the f-sequence (i. e. $2.3 \cdot 10^{18}$). The specialists estimated the cardinality of equivalent keys as sufficient small depending on the long-term key.

The cryptologists of ZCO provided manual paper-and-pencil proofs and used computer programs for calculating specific long-term keys. They built special devices connected to a computer for time-consuming calculation. The special device T-032 were used for the calculation of cycles of the permutation φ since 1980. The special device T-037 generated internal sequences for statistical tests since 1982.

The substitution played a special role in protection of the plaintexts and the short-term keys too. If the keystream of a stream cipher with a simple invertible function is used more than once then the keystream may be withdrawn. Such attacks are well known for the VERNAM cipher and constitute a potential vulnerability of stream ciphers. If two ciphertexts are encrypted with the same keys and initial vector (disregarding of equivalences) the a-sequence can be determined by guessing the corresponding plaintexts. The a-sequence is the (necessary) base for attacks on the short-term key. It can also be used for encryption of another text imitating an authorized cipher station. If three such ciphertexts are intercepted and two corresponding plaintexts are known (or guessed) then the third plaintext may be determined independent on the strength of the keys and the complica-

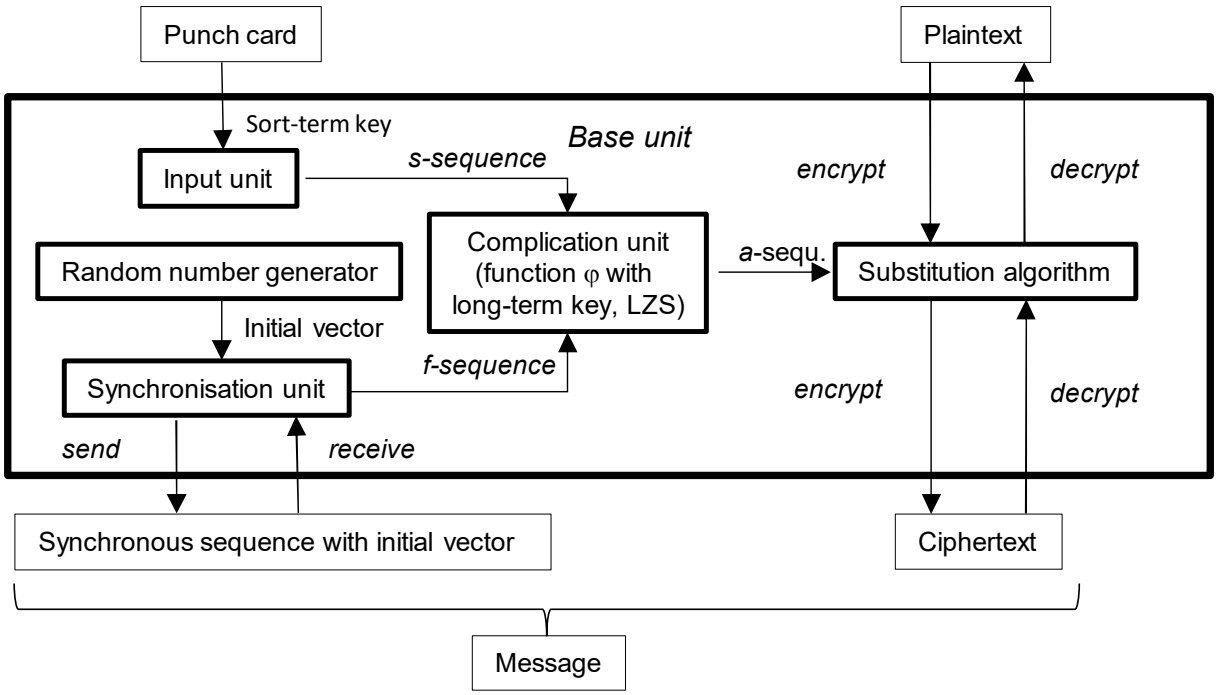

Figure 2: The cryptographic module

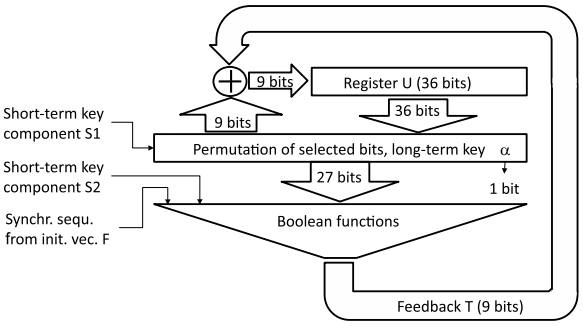

Figure 3: Structure of the complication unit

tion unit (Killmann and Stephan, 2021; Stephan, 2022). The countermeasures against such attacks are (1) the generation of the initial vector by means of strong random number generators (Section 5.1), and (2) the robust cipher procedure preventing the encryption with an untrustworthy initial vector (Section 6.2).

The cryptologists of ZCO assessed the algorithm with approved long-term keys as secure and appropriate for encryption of state secrets.

According to Crypto Museum homepage[2], the US Army and the NATO widely used the SAVILLE cryptographic algorithm in high-level encryption devices including for teleprinter in the 1980s. SAVILLE is a stream cipher based on a nonlinear finite state machine, that has an internal cycle of several tens of iterations per output bit. The short-term keys consists of 128 bit key including 8 bit checksum (2^{120} keys), which is much less than T-310 short-term keys. The SAVILLE cryptographic algorithm is still secret. Thus, we cannot compare SAVILLE and T-310 in details. Some cryptologists are still interested in the strength of the algorithm T-310, even the machine T-310/50 has historical value only. The currently published attacks do not break the algorithm with approved long-term keys (Killmann, 2023).

5 The Cipher Machine T-310/50

The cipher machines T-310/50 were developed by the “Institut für Regelungstechnik” (IfR) and the ”VEB Steremat Berlin Hermann Schlimme“, and they were produced by the ”VEB Steremat Strausberg“. The ZCO as contracting authority defined the tactical-technical requirements, affirmed the specifications and the results of the development steps A and K, and the serial production of T-310/50. The developers provided a complete documentation (seven books from technical descriptions, circuit diagrams up to engineering drawings), A-prototypes, K-prototypes and serial-product machines. The T-310/50 consists of (1) the cipher control panel (green box in Figure 1) for the operator, (2) the basic unit implementing the encryption, (3) the power supply unit, and (4)

[2]https://www.cryptomuseum.com/crypto/usa/saville.htm

the cables connecting the panel and the units. It is connected between the teleprinter control panel ("Fernschaltgerät") and the communication line.

The cipher machine is much more complex than the abstract cipher algorithm. It shall implement the security functionality for encryption and decryption and may provide intended but security irrelevant functionality (like encoding the binary ciphertext to numbers). An (often hidden) functionality or feature of the cipher machine could also build a security vulnerability. The ZCO analyzed deeply the correctness and the security of the T-310/50. The following three examples illustrate the security analysis of the cipher machine T-310/50 performed by ZCO.

5.1 Random Number Generator

The generation of the initial vectors is an important aspect of the stream cipher T-310. From the pure algorithmic point of view the initial vectors must be different for all texts encrypted with the same short-term key (disregarding of equivalences). At first glance a deterministic generation of initial vectors would be possible e.g. by a linear shift register with a long period. But this approach requires random start vectors. The generation of initial vectors at random is an appropriate solution. The random number generator (RNG) is a non-algorithmic part of the cipher at the boundary between mathematics and engineering.

The RNG shall produce initial vectors of 61 bits for each message to be encrypted. The cipher machine of SKS V/1 implemented a physical random number generator. The A-protoype of T-310 used external input for the initial vector from teleprinter or punch cards in 1977. For the sake of reduction of the required punch cards and simplification of the machine the T-310/50 K-prototype used a non-physical true RNG[3] called System-RNG in 1978. The System-RNG used as noise sources (1) the clock for reading the punch card with the short-term key, (2) the time of the third step of the prophylactic check (Section 5.2), and (3) the telex characters read from the local and line interfaces. The System-RNG was analyzed by means of a comprehensive stochastic model and tests with special devices built by ZCO. Unfortunately the stochastic model could not be substantiated by sufficient amount of test data (e.g. reading of thousand punch cards). It was found that the evidence for the security of the System-RNG is sufficient for the procedure SAGA, but not for the procedure ARGON (ZCO, 1982). SAGA was used for only 50 clients and unilateral encryption from surveillance stations to the center. The System-RNG was secure for SAGA. In case of ARGON up to 150 client may communicate to each other sharing the same short-term key and generating initial vectors for each message. Therefore, the decision was made to equip the serial-production T-310/50 with a physically true RNG based on a transistor noise source in 1983. The final security analysis assessed the final RNG as secure in 1984.

The self-test of T-310/50 includes a health test of the physical RNG apparent during the prophylactic checks. The noise source is tested by counting the occurrences of a fixed pattern of six bits in its output. The health test is performed by the crypto officer when the punch card reader is switched on for input of the short-term key. When the pattern is detected 16 times then the H-OFF miniature lamp of the control panel is switched on or off. The decision can be made on the health of the noise source: (1) if the H-OFF does not blink then the noise source is broken and the machine is blocked (or the machine is T-310/51), (2) if the H-OFF blinks then the noise source is working, and (3) if the H-OFF blinks between 43 and 50 times in one minute then the noise source is working well (ZCO, 1983a).

Modern cipher machines implement physical RNG for the generation of keys and initial vectors. Standards exist only for deterministic RNG, which shall be used in combination with physical RNG. The stochastic model of the noise source is still a necessary but difficult part of the security analysis of physical RNG (BSI, 2013b).

5.2 Self-Protection against Technical Failure

Technical faults of a cipher machine may result in weak encryption of the secrets (Figure 1). The self-protection of T-310/50 shall detect every security critical single technical fault and prevent adverse aftermath by blocking the output. The security analysis of the self-protection required a detailed analysis of the implementation up to the level of the electric scheme.

The T-310/50 consists of

- twice the complication unit (their output are compared by a control unit),
- the control units for security critical internal

[3] (BSI, 2013b) for definition.

sequences,

- the control units of the module connecting the peripheral devices and the line,
- the blocking unit which blocks the output when faults were detected, and
- the prophylactic checks of the control units and blocking.

The two complication units are implemented on three identical plates with two types of small plates implementing the long-term key. One of these plates implements function for both duplicating each other complication units. The ZCO specialists detected that a single fault on this plate may cause the same undetected deviation from the algorithm. Therefore, the plates were reworked. Finally the analysis found the self-protection effective (ZCO, 1983c).

The prophylactic checks are enforced after input of the short-term key. The crypto officer shall run the prophylactic checks step-by-step (ZCO, 1983a). Each step simulates a fault that shall be detected by the control unit and cause indicated blocking of the output.

The analysis of ciphertexts in case of technical faults is a standard method called failure analysis. Today, the self-protection functionality must (or at least should) be a standard countermeasure against breaches of security caused by technical faults. The fault resistance of the hardware must be accompanied by software robustness, which is even more important and difficult to achieve for computers today.

5.3 Protection against Side-channel

The terminology document of ZCO (ZCO, 1971) states that emanation of electromagnetic, acoustic or other forms of energy by cipher machines, teleprinters, typewriters etc. may compromise secret information which are helpful for cryptanalytic attacks. Therefore, compromising emanation was an important topic of the security analysis not only of the cipher machine itself but also in combination with the teleprinter.

One of the vulnerabilities to mitigate was the crosstalk of secret plaintext from peripheral devices to the line. Figure 4 illustrates the problem. The teleprinter caused sharp edges of the plaintext signal on its output interface. The teleprinter control panel did not prevent crosstalk during local operation, e.g. preparing tapes with secret plaintext (upper picture). The operational manual of ARGON (ZCO, 1983a) prohibits the use of local mode using the teleprinter control panel. The T-310/50 implements a secure local mode of operation separating securely the local connection and the termination of the teletype line (middle picture). T-310/50 prevents also crosstalk of the plaintext on the local interface to the line interface during online encryption (bottom picture).

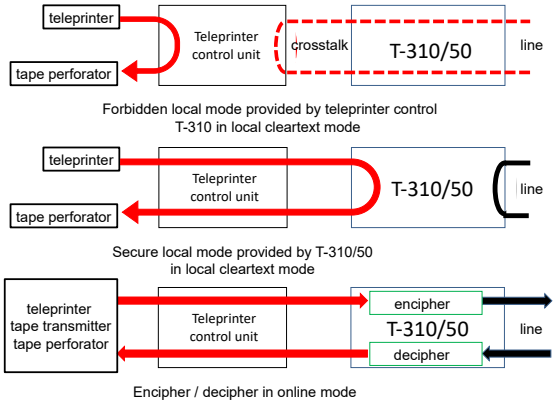

Figure 4: Forbidden and secure local mode

The T-310/50 mitigates crosstalk by means of an “active electronic suppression” (“Aktive elektronische Entstörung (AES)”).

The AES was effective for electro-mechanical teleprinters (mass-produced machines since 1984, other machines were reconditioned). Electronic teleprinters like F1000 caused even sharper signals of the plaintext. Thus the T-310/50 cannot prevent crosstalk in this case. The use of T-310/50 with electronic teleprinter (e.g. F1300, F2000) protected against emanation and crosstalk was investigated and planed. That is why the installation manual (ZCO, 1986) allowed the use only of T-310/50 with modified electro-mechanical teleprinters T51 and T63 with attached tape punch T52, tape transmitter T53/x, $x = 3,4,5,6$, and the line switch T 57/4 of T 57/8. A exhibition of T-310 with electro-mechanical teleprinter is historical correct although the reason of the lack of electronic teleprinter is not obvious.

The emanation security and side channel protection were intensive investigated for cipher machines and communication technique by the ZCO. The analysis and the assessment followed a Soviet standard which was similar to American TEMPEST documents. The analysis of side channels and emanation are hot topics even today. The German Bundesamt für Sicherheit in der Information-

stechnik published corresponding guidance (BSI, 2013a; BSI, 2008).

6 The Cipher Procedure ARGON

The cipher procedure ARGON defines how the operator and the crypto officer shall securely use both the cipher machine T-310/50 and the teleprinter. General security regulations and the technical provisions prescribed the organizational, personnel, physical and technical security measures for the premises, the installation and the operation for the use of ciphers in stationary and mobile stations. Based on this the ZCO specified the manuals for the installation of the T-310/50 and of the procedure ARGON as mandatory guidance documentation. The ZCO performed the trial of the prototypes and the procedures. It guided the training of the crypto officers and the operators. The ZCO and the cipher services inspected the application of ARGON in real life.

ARGON regulates the use of the T-310/50, the key material, the texts, the teletype components and the security measures. ARGON and SAGA are two different procedures for the very similar machines T-310/50 and T-310/51.

6.1 The Installation Manual of T-310/50

The installation manual (ZCO, 1986; ZCO, 1983b) defines the technical security measures for the installation of the T-310/50 and teleprinter components. The teleprinter components are connected to the cipher control panel. An additional teleprinter may be connected trough an additional control unit and the first control unit to the base unit. The control units may be installed in distance of up to 100 m from the base unit.

The basic unit and the power supply were located in an exclusion zone ("Sperrzone") surrounding the base and power supply units of at least 0.5 m. The exclusion zone may access only explicitly authorized person e.g. the crypto officer for key management or the service personnel for maintenance of the machine. The controlled zone ("kontrollierte Zone") surrounded the exclusion zone, all components of T-310/50 and the teleprinter components of at least 10 m. The plaintexts are input into and output from the T-310/50 within the controlled zone. The controlled zone prevents sojourn of vehicles, unauthorized persons or interception devices near to the devices and cables transmitting or operating secret information.

The installation manuals consider the results of the analysis of the emanation security and the physical protection of the T-310/50. The exclusion zone and the controlled zone are standard security measures protecting state secrets.

6.2 The Operational Manual of ARGON

The operational manual of ARGON shall ensure the general rules for the protection of state secrets by means of telex communication with T-310/50. The specialists of the ZCO performed a detailed analysis (ZCO, 1985) of every elementary reaction on any interaction through all interfaces of T-310/50 up to complex processes of cipher operation and network analysis. The machine allows for (1) the *transparent mode* (like in absence of the cipher machine), (2) the local and online *cipher mode* (encryption resp. decryption depending on the direction of the transmission), and (3) the local (offline) and online *monitoring mode* (entering decryption after receiving a synchronization sequence) (ZCO, 1983a). The T-310/50 implements some automatic processes e.g. the encryption of four fixed characters "Maschinenbefehlsfolge 2" BU, CR, LF, LF in front of the provided plaintext.

It followed that ARGON shall cope with two major issues: (1) the switchover between transparent, monitoring and cipher mode of operation, and (2) the change between sending/encryption and receiving/decryption of text without new synchronization in the cipher mode. These vulnerabilities must be mitigated by organizational countermeasures.

The operator may send by mistake secret plaintext in transparent and monitoring mode of operation. The analysts of ZCO found a precaution against unintended sending of plaintext if the T-310/50 is in monitoring online mode. The T-310/50 starts encryption by sending a "Maschinenbefehlsfolge 1" *bbbb* and the synchronization sequence containing the initial vector. When receiving this prefix at the peripheral interface or line interface in monitoring online mode the T-310/50 expects the synchronization sequence at the line interface and blocks any input at the peripheral interface. Therefore, the analysts suggested to add the prefix *bbbb* at the beginning of secret plaintext, e.g. on the punched tape prepared for sending by online encryption. In case of unintended transmission of the punched tape in monitoring mode the transmission will be stopped. The

suggestion was followed in the operational manual (ZCO, 1983a, sec. 5). The input of secret plaintext with prepared punch tapes was mandatory if the ciphertext was send by radio transmission.

The T-310/50 being in cipher mode changes between encryption and decryption depending on the interface receiving the characters, i.e. encrypt characters input on the peripheral interface and decrypt characters input on line interface. This feature enables an encrypted dialog between the cipher stations. But this feature might be misused to provoke ciphertexts encrypted with the same short-term key and initial vector. Suppose the following scenario: An attacker *Eve* intercepts a message containing probably an interesting encrypted plaintext with short-term key K and a synchronization sequence with the initial vector V. *Eve* assumes that a cipher station operates a T-310/50 with the same short-term key K in monitoring online mode, but unwatched by the operator *Alice*. *Eve* establishes a connection with this T-310/50, imitates a legitimate cipher station, synchronizes the T-310/50 with V and waits for receiving a ciphertext from *Alice*. *Alice* sees the T-310/50 in cipher mode without any expected text. If *Alice* asks for clarification in cipher mode then *Alice* provides *Eve* a ciphertext encrypted with the same K and V. If *Eve* repeats successfully this procedure twice and can guess the plaintext sent by *Alice* and *Eve* can guess the corresponding plaintext *Alice*, then *Eve* may decipher the intercepted ciphertext. Such attacks are known for a long time and called nowadays social engineering.

The described scenario maybe used also as deliberate attack of an fraudulent operator compromising a specific plaintext. Instead of direct decryption of this plaintext the operator does not know the compromised plaintext and there is no evidence of the treason except the encryption of arbitrary text. Thus such actions must be explicitly forbidden in order to make the operator accountable for the adverse action.

In order to mitigate such attacks the operational manual of ARGON requires (1) the station dialing to the remote station must initiate the cipher mode, and stop any communication if the dialed in remote station starts synchronization, (2) watch the behavior of the machine during establishment of the cipher connection and the indication “C” of the cipher mode on the control unit during the encrypted communication, (3) enforce the required exchange the names of the station by the answerback unit, and other required information, (4) to enter the transparent mode when leaving the T-310/50 unwatched (ZCO, 1983a, sec. 13).

The guidance for the training addressed the security requirements and regulations identified by the security analysis (ZCO, 1984). The analysts got feedback from the supervision of the application of the T-310/50 and ARGON by the cipher services.

The procedure ARGON may be demonstrated partly (local mode) if at least one T-310/50 is operational. Only two operational T-310/50 allows for detailed demonstration of ARGON and the potential problems as discussed above. Security problems of the operation may be solved by robust procedures reducing the probability and the affect of mistakes. Computers allow better ease of use, but the complex applications make analysis much more difficult.

7 Key Management

The cryptographic role of the long-term keys comprises the secrecy of the algorithm, the cryptographic reserve for strength, and the separation of networks (Stephan, 2022). The ZCO approved six long-term keys, but only three of them were implemented in hardware for ARGON and SAGA. The production of the plates with the long-term-key was controlled by the ZCO. The change of the long-term key for mass-produced T-310/50 would be difficult because many machines needed to work together. Thus the long-term keys were never changed in the field.

The ZCO produced all the short-term key material for distribution by the cipher services. The short-term keys were changed every week. The manufacturing of the short-term keys was developed, build, run, and continuously checked by the ZCO. The packets of punch cards were distributed over secure channels of the cipher services and stored in safes of the cipher stations. The packaging of the punch cards provided only a known limited physical security. The number of clients sharing the same short-time key was limited to 150 in order to reduce the security impact in case of compromise. The short-term key were put into the base unit by crypto officers. The operator of the teleprinter does not need to know the short-term key. But the operator shall destroy the short-term key stored electronically in the basic unit by push-

ing a button “GG AUS” on his cipher control panel in case of emergency.

One should have these circumstances in mind when examining an exhibited punch card package or watching the key import in a museum. The key-distribution method was specific and appropriate for the cipher services. The cryptologists of ZCO knew the public-key methods. But public-key cryptography was not needed for the key management of the cipher services at the time of ZCO, because all cipher stations were under sole control of cipher services, including the distribution of the cipher machines and the key material.

8 Conclusion

The machine T-310/50 and the procedure ARGON are historical objects. Their development and the analysis provided a lot of insight for the cryptologists of ZCO. The cryptologists used their experience for the next generation of ciphers in the 1980s. The strength of the algorithm T-310 is still of interest, even the machine T-310/50 has historical value only. The security analysis of the machine T-310/50 and the procedure ARGON then provided by the ZCO is comparable to the modern Common Criteria evaluation on EAL 4 augmented with vulnerability analysis against high attack potential (AVA_VAN.5) (https://www.commoncriteriaportal.org/).

Acknowledgments

The author thanks Winfried Stephan and Franz-Peter Heider for the fruitful discussions and Nils Kopal and Bernhard Esslinger for proofreading. The author would also like to thank Jörg Drobick publishing additional information about the cipher service of GDR on his website http://scz.bplaced.net/.

References

BSI. 2008. *TR-03209: Elektromagnetische Schirmung von Gebäuden, Theoretische Grundlagen*. Technical report, BSI.

BSI. 2013a. *AIS 46*. Technical report, BSI.

BSI. 2013b. *Evaluation of random number generators*. Technical report, BSI.

Jörg Drobick. 2023. *Homepage Der SAS- und Chiffrierdienst*.

Killmann and Stephan. 2021. *Das DDR-Chiffriergerät T-310*. Springer Spektrum, Berlin. 978-3-662-61896-7.

W. Killmann. 2023. *On security aspects of the ciphers T-310 and SKS with approved long-term keys*. *Cryptologia*, pages 1–33.

W. Stephan. 2022. *Use of T-310 Encryption During German Reunification 1990*. In *Proceedings of the 5th International Conference on Historical Cryptology HistoCrypt 2022*, Linköping Electronic Conference Proceedings 188.

ZCO. 1971. *Fachbegriffe des Chiffrierwesens*. VVS - ZCO/407/71.

ZCO. 1980. *Kryptologische Analyse des Chiffriergeräts T-310/50*. Technical Report GVS ZCO Nr. 402/80, ZCO. BStU Archiv der Zentralstelle MfS - Abt. XI, Nr. AR3 594.

ZCO. 1982. *Das Auftreten gleicher Spruchschlüssel bei Geräten T 310/50*. Technical Report VVS-o020 MfS XI/393/82, ZCO. BStU Archiv der Zentralstelle MfS - Abt. XI, Nr. 596.

ZCO. 1983a. *Gebrauchsanweisung ARGON T-310/50*. Technical Report GVS B 434-081/83, ZCO. Harnekop NVA Museum.

ZCO. 1983b. *Gerätesystem T310/50 Installationsvorschrift (1. Ergänzung – Zentrale Chiffrierstellen)*. Technical Report VVS B 434-065/83, ZCO. Harnekop NVA Museum.

ZCO. 1983c. *Technische Analyse des PBS des Chiffrators des Geräts T 310/50*. Technical Report GVS-o020 MfS XI/356/83, ZCO. BStU Archiv der Zentralstelle MfS - Abt. XI, Nr. 596.

ZCO. 1984. *Schulungsanleitung Verfahren ARGON (T 310/50)*. Technical Report VVS B 434-416/84, ZCO. Harnekop NVA Museum.

ZCO. 1985. *Analyse der Bedienhandlungen am Gerätesystem T 310/50 und deren Konsequenzen für die Gewährleistung der Sicherheit der zu übertragenden Informationen*. Technical Report GVS MfS-Nr. XI/113/85, ZCO. BStU Archiv der Zentralstelle MfS Abt. XI, Nr. 665.

ZCO. 1986. *Gerätesystem T-310/50 Installationsvorschrift*. Technical Report VVS B 434-143/86, ZCO. Harnekop NVA Museum.