Use of T-310 Encryption During German Reunification 1990

Winfried Stephan
Mathematician, Retired
wstephan@mein.gmx

Abstract

One of the well-kept political secrets in the few months between the peaceful revolution in the GDR and the reunification of the two German states was the use of GDR cryptological equipment to secure communications between the western FRG and the eastern GDR. The T-310 cipher device, which was approved for state secrets, was selected for secure transmission on teletype links.

During this transitional period the interior ministries of the two German states had to coordinate their interaction. The use of the GDR's T-310 cipher machine for the secure message connection of the teletype networks between the two interior ministries was prepared and carried out by intelligence units of the two German states. The secured connections were operated by the cipher services, which worked in the top-secret facilities of the two government bunkers.

As part of the politically necessary cooperation, the best-kept secrets of the GDR's state cryptology were handed over to the former "class enemy" along with information about the T-310 cipher algorithm.

The following statements are largely based on interviews with people acting at the time. Some of this information is summarized and published here for the first time.

1 About the Cipher T-310

The T-310 device was the most widely used teletype cipher in the German Democratic Republic (GDR).

The cipher T-310 was developed by the Central Cipher Authority ("Zentrales Chiffrierorgan", ZCO) of the GDR in the 1970s. It was used in the cipher procedures ARGON with the cipher machine T-310/50 and SAGA with the cipher machine T-310/51. The ARGON was approved for encryption of teletype communication up to Security Level Secret ("Geheime Verschlusssache"). From 1983 to 1990 there were as many as 3.835 cipher machines T-310/50 in active service by the GDR government, army, security services and political organizations. However, since it was never used within the communication of the various member states of the Warsaw Treaty Organization, it was not a product of the Cold War.

The high number of almost 3.900 devices corresponded to the security needs of the GDR. At the border-line between NATO and the Warsaw Treaty, it was a matter of protection against telecommunications reconnaissance by the German Federal Republic (FRG), the USA, and other countries. Telecommunications reconnaissance against the GDR is documented in the literature (Müller 2017).

In 1990 employees who had previously been trained to protect highly classified information, i. e. state secrets by encryption, were ordered to hand over this information to representatives of the FRG.

This initial situation was aptly summarized by Dr. Otto Leiberich (2001): "Only superficially are codemakers fighting codebreakers. In reality, a scientific war is taking place between the states."

2 First Business Trip to the Class Enemy in June

Let us start with the description of a business trip of three employees of the GDR Ministry of the Interior. Participants were VP-Rat Dr. Klaus

of encryption schemes, ZCO cryptologists used group-theoretic approaches that we in the West were unfamiliar with. That's where the Soviet school obviously made itself felt."

The properties of the ciphering method or the ciphering device and the ciphering algorithm class ALPHA presented at that time are detailed described in the literature (Killmann and Stephan 2021). Alternatively, the historical source is also interesting (Referat 11, 1980). The first publication on the subject outside ZCO is by Schmeh (2006).

A simple functional model of the T-310/50 can be found at CrypTool 2.1 (https://www.cryptool.org/de/ requested 2022-03-24). Ciphering devices used in the GDR are on display in an army museum in Harnekop near Berlin (https://www.nva-harnekop.de/chiffrier-technik.html requested 2022-03-24). Among them are several functioning T-310 devices.

It is not the aim of the article to explain in detail the device and its properties. In the following, a special feature is presented, the function of the long-term key, which became interesting for the application on the line BMI - MdI. It was also a topic in the discussions in Bonn.

6 The Function of the Long-Term Key

The hardware realization of the algorithm had a special feature. Part of the logic was outsourced to a very simple printed circuit board that contained no components but only wiring, the so-called long-term key (LZS). By changing the wirings, on the one hand a whole family of different expressions of the same cryptosystem was created, on the other hand certain cryptological properties had to be proved for each LZS, i.e. for each wiring.

Fig. 6 represents the circuit board, which realized a part of the Complication Unit (see Fig. 7). On the left side you can see the special board with the LZS. As it can be seen, the LZS can be changed very quickly by changing the board. In this way, secured teletype networks could be separated. This option was used, for example, for the four T-310s in the bunkers. They had their own LZS. The LZS 31 came into use. The mathematical-cryptological properties of the algorithm with this LZS and the protocol of its testing were submitted to ZSI in a letter dated July 19, 1990 (ZCO 1990).

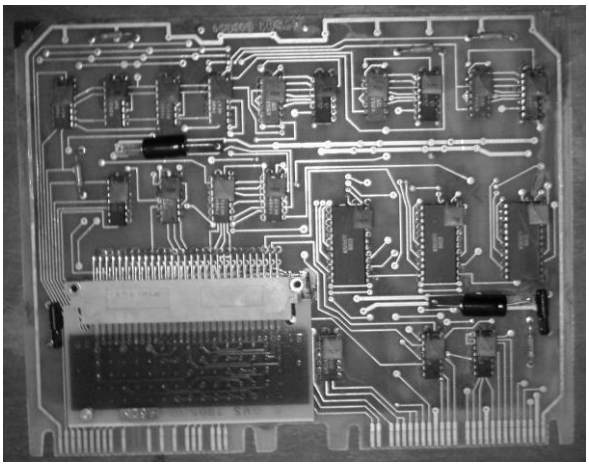

Figure 6: The circuit boards.

Thus, the devices were cryptologically separated from all other T-310s in service. Due to this measure, it was also not possible to decrypt active secured connections in the GDR with the help of the devices.

This design idea had several advantages:

- If the wiring is unknown, then the internal processing of the secret short-time keys (ZS) is unknown and it must be reconstructed. Therefore, the LZS circuit boards were manufactured completely independently from the production sites of the T-310 devices and later inserted into the devices in specially secured environments. This simplified secrecy during production and installation. If an LZS was compromised, it could be replaced with a new one relatively easily. During production, a test LZS was used that did not meet cryptological requirements and thus served as a means of concealment.
- The decision for a specific LZS had to be made only shortly before the delivery of

the devices. Thus, their production was still possible until shortly before delivery. The use of LZS created about five years of additional time for analytical work.

- An operationally deployed LZS had to meet criteria specified in an LZS technology (Referat 11 1980).

- The LZS serves to create a cryptological reserve. If, during the control analyses carried out up to 1989, vulnerabilities had been found concerning an LZS, there should still be those without these cryptological vulnerabilities to be found in the set of LZSs.

The last thought clearly states that the cryptological analysis of the T-310 was not completed. An analysis of ciphering procedures must be carried out over the entire period of use, as potential weaknesses could be found as a result of newer theoretical findings but also the use of more powerful IT etc. The analysis must be carried out on a regular basis. On this basis, it is always necessary to assess how long the procedure can still be used securely in practice and how long the information encrypted with it will remain secure.

Following this reasoning, Courtois' recent publications are of interest. As an example consider (Courtois, 2018). He studies the algorithm using new methods. In his work, he constructs his own LZS that have certain invariance properties and are in some sense singular. The LZS constructed in this way do not meet the criteria of LZS technology. They would thus be explicitly excluded from use (Killmann 2022).

7 The Encryption Machine

The high-level overview shows the division of the Chiffrator into function blocks.

The concept of LZS gave rise to a whole family of stream cipher algorithms of various specifications, the ALPHA class of algorithms. The common basis for their description is an automaton with 2^{36} states, which gets the short-term key and a 61 bit initialization vector as input. It derives the *s*-sequence from the key and the *f*-sequence from the initialization vector controlling the state transition in the Complication Unit. The Complication Unit output a single bit of the *a*-sequence for the Encryption Unit after every 127 clocks (figure 7). The period length of the *a*-sequence is as multiple of $2^{61} - 1$ very large. Each segment of 13 bits of the *a*-sequence selects the substitution applied to the plaintext respective ciphertext character.

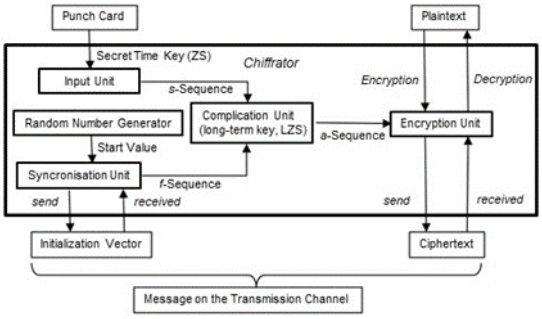

Figure 7: Chiffrator, high-level overview.

More details can be found in section 9. For the technical realization of the machine, proven components from GDR production had to be used, with which the usual teletype transmission rates of 50 to 100 baud could be achieved without any problems.

Each short-time key generated eight transformations of the states in each internal clock, one of which was selected by a control stream of bit triples and used for the next state transition.

We now focus on the description of two important properties of the algorithm that were new to the colleagues from ZSI.

8 Keyspace

The space of the secret short-time key caused astonishment at that time. In 1990, a keyspace of 2^{80} was discussed for public cryptography,

because a keyspace of 2^{56} as with DES was foreseeably no longer sufficient against brute force attacks. However, in government cryptography larger keyspaces were used already at that time.

The secret short-time key in the T-310 device, consisting of two binary vectors each with a length of 120 bits, results in a key pool of 2^{230} short-time keys, taking into account the integrated parity bits.

During the design phase of development around 1980, the following considerations were made in this regard:

1. A brute force attack is basically impossible with the intended quantity, even with the means available today.

2. If there are any hidden weaknesses in the algorithm that allow the keyspace to be sampled, then this reduced short-time key set should be smaller than about 2^{80}. This would mean that a very large number of keys, on average about 2^{150} each, would produce the same control *a*-sequences for encryption. The ZCO cryptographers were optimistic that such a vulnerability was detectable in the analysis and avoidable by choosing the LZS appropriately.

3. The selected key length was also technically suitable, because the 240 bits fit exactly on a punch card. This meant that the available technical possibilities were used effectively (Fig. 8).

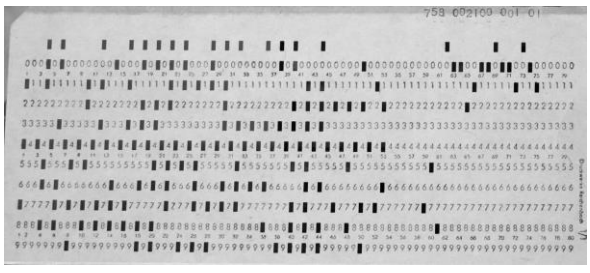

Fig 8: short-time key punch card.

9 Encryption Unit

Symmetric encryption is implemented in the encryption unit (Fig. 9). The selection of the cipher transformation is controlled by the *a*-sequence, which is calculated beforehand in the complication unit (Fig. 7).

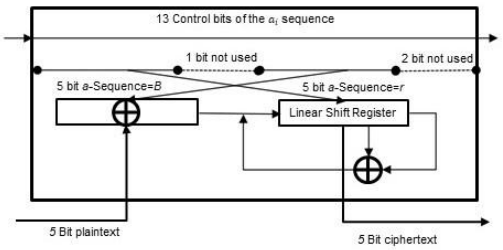

Figure 9: Encryption Unit.

The *a*-sequence then controls the selection of the substitution for the cipher. This approach is unusual; usually an XOR operation is used for stream ciphers.

To encrypt a given letter of plaintext we have 32x31=992 possibilities for substitution.

In practice for attackers it has the following impact:

- A ciphertext only attack needs three ciphertexts encrypted using the same *a*-sequence.
- A known plaintext attack requires two text pairs in order to determine parts of the *a*-sequence and to obtain information about the keys used.
- If the ciphertext character is zero then the plaintext character is equal to the five bits of the *a*-sequence used for the XOR (Figure 9). This happens with probability 1/32 per character.

The probability that these situations occur in practice is very low. Thus, the possibility to get sufficient bits of the *a*-sequence for reconstruction of the short-term key via this way is practically almost excluded.

In general, it could be estimated during the consultation at ZSI that no methods are known that would allow a decrypter to reconstruct the secret short-time key even if, according to

Kerckhoffs' principle, all information about the cipher algorithm or method including the LZS and any number of texts are known to him.

This assessment seems to be correct even from today's point of view.

10 Further Use of the T-310 Device for the Two Ministries for Defense

Another use of the T-310 unit was to secure communications between the Ministry for Disarmament and Defense of the GDR (MfAV) in Strausberg and the Federal Ministry of Defense (BMVg) in Bonn. The connection existed from 6 September to 6 October 1990 (http://www.hptnzmfnv.homepage.t-online.de /bonn.htm requested 2022-03-24). According to the source mentioned, only one T-310 unit was installed on September 6th. Rheinbach near Bonn's Hardthöhe, the headquarters of the BMVg, is mentioned as the place of installation.

11 Third Business Trip to Bonn in August

A presumably last mission on questions of the use of the T-310 took place on 16 and 17 August 1990.

Participants were Dr. Nickel and Mr. Wiemann from the ZCO, Mr. Peters, Mr. Ahlbrecht, Mr. Neles and Mr. Müller from the ZSI and temporarily Mr. Weber from the BMI, division Dr. Werthebach.

The report on the business trip shows that further technology and documentation was handed over. The ZSI employees were instructed in the operation of this technology. In an additionally handed over overview document ”Compilation of information on the T-310/50 equipment system and its use“, statements on tempest safety, operational service and maintenance can be found in addition to technical details on the equipment and the coupling options to the periphery (Drobick 2020).

There is much to suggest that at this time preparations were still being made for a longer deployment of the T-310 in the transition phase.

However, rapid political developments quickly rendered these activities obsolete.

12 Historical Annotation

We recall the political events at that time:

- January 1990, the ZCO is detached from the Office for National Security (AfNS) and attached to the MdI
- March 1990, last Volkskammer election on March 18, dissolution of the AfNS
- July 1990, coming into effect of the monetary, economic and social union between the FRG and the GDR on 1 July
- August 1990, in Berlin's Kronprinzen-palais, Federal Minister of the Interior Schäuble and GDR undersecretary Krause sign the German-German Unification Treaty on August 31
- September 1990, approval by the GDR Volkskammer and the Deutsche Bundestag of the Unification Treaty on September 20
- September 1990, the GDR withdraws from the Warsaw Treaty on September 24
- October 1990, reunification of FRG and GDR on October 3

The very rapid political development towards reunification meant that the framework conditions for establishing a secure link between the two ministries of the interior were also constantly changing.

Ultimately, with the signing of the Unification Treaty in August, it was clear that long-term use of the T-310 would no longer be necessary. This may also explain why the cipher link between the

two government bunkers was discontinued at the end of August.

The ZCO remained in existence after 3 October 1990, with a significantly reduced staff and the addition of "i. L." until December 31, 1990, in order to carry out the specified tasks for liquidation. Among other things, the staff dismantled a large number of T-310s and prepared them for destruction. In that sense, we have come full circle: developers of the T-310 ultimately destroyed it as well.

In accordance with the Unification Treaty, the ZCO was dissolved and its documents and equipment were handed over to the authorities of the FRG. The equipment was almost all destroyed and the documents became part of the holdings of the Stasi Records Agency (BStU).

At the beginning of 1991, ZSI became the new Federal Office for Information Security (BSI).

The role of the T-310 in the reunification process is thus described. And those involved in the process would certainly agree with Brühl (2019) from their own experience:

Cryptography is the most political form of mathematics

Acknowledgments

The author thanks Wolfgang Killmann, Franz-Peter Heider for the fruitful discussion and support, Dr. Nickel and Mr. Schmohl for information about their first business trip based on personal records. The author would like to thank also Jörg Drobick publishing interesting information about the cipher service of GDR on his website http://scz.bplaced.net/.

References

Jens Albes. 2021. *Enigmas Erben – DDR-Verschlüsselungsmaschinen beim Klassenfeind.* https://www.heise.de/news/Enigmas-Erben-DDR-Verschluesselungsmaschinen-beim-Klassenfeind-5048022.html requested 2022-03-24

Johannis Brühl. 2019. *Kryptografie-Geschichte: Der Code der Freiheit* aus der Süddeutschen Zeitung vom 23./24. November 2019

Nicolas T. Courtois. et. al. 2018. *Cryptographic Security Analysis of T-310*. url: https://eprint.iacr.org/ 2017/440.pdf

Jörg Diester and Michaela Karle. 2013. *Plan B.* Verlagsanstalt Handwerk GmbH

Jörg Drobick. 2019 *T310/50 ARGON DOKU*. url: http://scz.bplaced.net/t310.html, requested 2022-03-2l

Wolfgang Killmann and Winfried Stephan. 2021. *Das DDR-Chiffriergerät T-310: Kryptographie und Geschichte*. Springer Verlag, 248 Seiten, ISBN 978-3-662-61896-7

Wolfgang Killmann. 2022. *On security aspects of the ciphers T-310 and SKS with approved long-term keys.* Cryptologia (submitted)

Otto Leiberich. 2001. *Vom diplomatischen Code bis zur Falltürfunktion*. Spektrum der Wissenschaften, Dossier 4, S. 30 - 31.

A. Müller. 2017. *Wellenkrieg. Agentenfunk und Funkaufklärung des Bundesnachrichtendienstes 1945 - 1968.* Veröffentlichungen der Unabhängigen Historikerkommission zur Geschichte der Erforschung des Bundesnachrichtendienstes 1945 - 1968, Band 5. ISBN-978-3-86153-947-6. Ch. Links, Berlin, 2017.

Marcel Rosenbach and Holger Stark. 2010. *Von Mielke zu Merkel.* In: Der Spiegel 39 (2010), S. 30 - 31.

Referat 11. 1980. *Kryptologische Analyse des Chiffriergeräts T-310/50*. Techn. Ber. GVS ZCO Nr. 402/80. BStU Archiv der Zentralstelle MfS - Abt. XI, Nr. AR3 594. ZCO.

Klaus Schmeh. 2006. *The East German Encryption Machine T-310 and the Algorithm It Used*. In: Cryptologia 30.3 (2006), S. 251 - 257.

Klaus Schmeh. 2007. *Die Erben der Enigma*. secunet.

ZCO. 1990 *Chiffrieralgorithmus 310*. Streng geheim T-310/50. BStU Archiv der Zentralstelle MfS - Abt. XI, Nr. 599