Development of the Block Cipher LAMBDA1 in 1990

The Block Ciphers DES, GOST and LAMBDA1

Winfried Stephan
Mathematician, Retired
wstephan@mein.gmx

Abstract

In 1990, it became apparent that the German Democratic Republic (GDR) would leave the socialist community of states. This involved the gradual reduction of cooperation between the cipher services of these countries and the separation of cipher connections.

LAMBDA1 is a block cipher developed in East Germany in 1990. It was designed for a cipher device for which a Soviet algorithm was originally intended. The plan was to use a predecessor of the Soviet block cipher algorithm, called GOST. This now had to be replaced. The aim was to provide a cipher algorithm that could not be easily decrypted by either the Warsaw Treaty countries states or the NATO countries.

The background to these considerations was the assumption that the GDR would confirm to exist as an independent state for an extended period in a kind of transitional phase.

The article describes the circumstances under which the LAMBDA1 algorithm was developed in just one month. It was based on the results of previous projects and was then intensively analyzed.

The project was only abandoned when it became clear that the unification of the two German countries would take place at short notice and was imminent.

The algorithm below is described only to the extent necessary to understand the development process.

1 Publications on LAMBDA1 and T-316 after 1990

Like all state secrets of the German Democratic Republic, information about cipher algorithms and cipher machines was kept secret until 1992. With the dissolution of the GDR, the Stasi Record Archive (BStU) received all existing documents on the cipher service, with a few exceptions. They were registered there and only gradually made available to the public. Since then, this office has been integrated into the Federal Archives (Bundesarchiv).

The publication of the LAMBDA1 algorithm and the T-316 GO cipher device was made possible in particular by Jörg Drobick's many years of research into the cipher services of the GDR.

Programs to implement the algorithm are publically available, as well as a video tutorial showing encryption and decryption using the T-316 GO cipher device (Drobick 1989). Additionally, two more implementations are available: (CrypTool 2) and (github.com).

A bachelor thesis was written based on this material (Altenhuber 2018).

So while the technical details of LAMBDA1 have already been published, this paper explains the reasons and historical circumstances under which the algorithm was developed.

2 The Situation in 1990

Elections to the People's Chamber of the GDR were held on March 18, 1990. The majority of the newly elected parliamentarians voted in favour of unification of the GDR with the German Federal Republic (FRG). This marked the beginning of the unification process, although the timeframe was initially open. A

transition period of about two to four years was generally assumed.

It was therefore clear that the GDR would withdraw from international relations, in particular from the Council for Mutual Economic Assistance and the Warsaw Treaty.

It should also be noted that according to the regulations in force in the FRG, communications could not be secured using NATO procedures, as the GDR was still a member of the Warsaw Treaty. NATO technology was not allowed to be used in these countries.

3 Tasks of the Cipher Services

In the GDR, the Central Cipher Authority (ZCO) was responsible for the technical management and control of the ciphering facilities (CW). Until 1989, this was a department of the Ministry for State Security (MfS). It was then assigned to the GDR Ministry of the Interior in January 1990. After reunification, work continued on its dissolution. The ZCO remained under the control of the Ministry of the Interior of the Federal Republic of Germany until its final dissolution on December 31, 1990.

The tasks of the ZCO included the development, production and provision of new ciphering techniques and other cryptological procedures, means and methods for encrypting messages, in addition to providing guidance to the operational services.

Let's take a closer look at a development project that has been underway since the mid-1980s:

At that time the hardware basis for cryptographic machines was changing. Mainframe computers were used in computer centers and machines with CPU-based cipher implementations were developed. In addition, a corresponding algorithm was needed for commercial applications. New algorithms were needed for this and an analogue to the American block cipher algorithm (FIPS77) was already under development in the Soviet Union (GOST89).

As a general rule, the methods and algorithms used at the level of state secrets should not be used on a large scale in the commercial sector. As in the USA there should be a separation between encryption methods used in the government or military sector and those used in the commercial sector.

The predecessor of the new cipher was developed by the Russian State Security Committee (KGB) in the 1970s. As early as spring 1984, Soviet cryptologists informed the GDR about their work on this block cipher algorithm in two lectures: "Properties of the Data Cipher Algorithm (DCA)" (1986) and (1987) (Killmann W., Stephan W. 2024 Appendix A). It is the forerunner of the algorithm which is now known as GOST No. 28147-89 (GOST89)[1].

It should be used as a block cipher algorithm in the socialist countries. In the GDR, it was therefore assumed that in the future the Soviet standard would be used if necessary. The algorithm was still classified as "Top Secret" until 1990.

The use of DCA or GOST would have required the permission of the Soviet Union. However, this was no longer to be expected due to the political situation.

The process of unbundling between the socialist states also included the disentangling of relations between the encryption services of these countries.

For example, all cipher machines used by the armies of the Warsaw Treaty had to be handed over by the GDR army to the Soviet army. This also concerned confidential documents on cooperation with the Soviet cipher services, encryption algorithms and encryption devices that were in use or under development at the time. This also included all existing documents relating to the DCA and GOST.

This situation is described below using the development of the T-316 data cipher machine as an example. For this device the use of GOST was intended.

The development of the devices was already well advanced. The T-316 was one of the first encryption devices in the GDR to use a programmable microprocessor system. This made it possible to implement various encryption algorithms, taking into account the technical framework. The T-316 was designed and built

[1] From this point on, GOST will be used as an abbreviation for GOST No. 28147-89.

for both civilian and military use. The civilian version, called the T-316 GO (Figure 1), was fitted in an attaché case and the military version T-316 M in a metal housing.

The development of the T-316 devices must have begun before 1987, because the BStU already possesses a document from 19 August 1987, entitled *"Demand planning for the T-316 and T-314 cipher devices under development"* (ZCO1 1987).

Figure 1: The civilian variant T-316 GO
Source http://scz.bplaced.net/316.html

By 1990, ten T-316 GO units had already been produced. It was also planned to produce another 50 units in 1990 and 850 units in 1991.

In addition, the Czechoslovakia was to receive a loaner device for testing, which indicates that it was intended to provide T-316 to other socialist countries (Drobick 1990).

In this situation, an encryption algorithm other than DCA or GOST had to be found for the T-316 GO in a very short period of time. (Drobick 1989). This explains the time pressure under which the LAMBDA1 algorithm was developed.

It is noteworthy that in the BStU documents analyzed so far, GOST or its predecessor DCA do not appear as the algorithm actually intended for the T-316 device. It seems that the secrecy of these facts has been maintained until today. Therefore, this information is new and comes from the developers and the author of this paper.

4 DES as Candidate for Replacement

The first candidate for replacement was the internationally renowned American DES.

The American data encryption standard DES (FIPS 77) was the most widely used standard for non-classified data encryption at the time.

However, since its publication, there have been concerns about its security. The ZCO has been monitoring and analyzing publications on DES since at least the early 1980s.

Let us recall some of the design features of this block cipher.

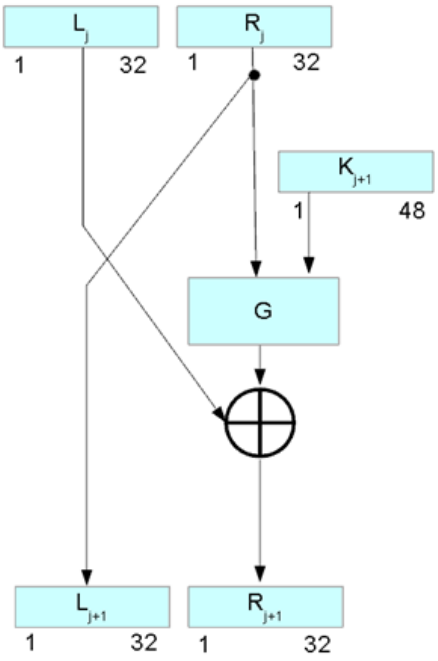

Figure 2: The round function of a Feistel cipher

Figure 2 outlines the basic principle of a round of a Feistel cipher. The DES algorithm performs 16 of these rounds.

An important component of the round function is the so-called Feistel function *G*. The construction of this function corresponds to the principle of diffusion and confusion established by Claude Shannon (Figure 3).

In an assessment *Possibilities and dangers of using the DES* (ZCO2.1990) the following three potential weaknesses were highlighted:

• 56 bits for the key are already in 1990 not enough. It is conceivable that the most powerful decryption services, using all the possibilities of science and technology (special hardware, parallelization, etc.), will realize the TPM (total trial method - brute force) with an effort that goes to the limits of their capacity.

• It is unknown whether decryption services are aware of the laws of DES (trapdoors), which – under any real assumptions – require much less effort than trying out 2^{56} variants.

• In the DES literature in 1990, it was speculated that the S-boxes and key scheduling might contain trapdoors.

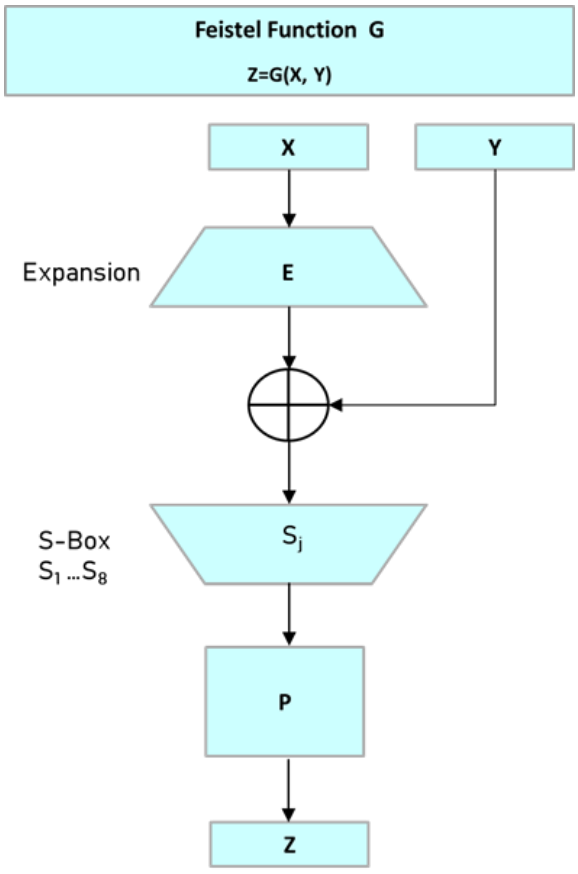

Figure 3: The Feistel function *G* for the DES

The following conclusions were drawn from this:

The possibility of using the DES as an alternative to GOST was considered for applications with lower security requirements. For state secrets in particular, it was ruled out on the basis of the assessments made, in particular because of the small size of the key. A potential decryption – by whomever – must be ruled out.

There was also no other acceptable, rapidly deployable method for this area, especially as it was difficult to assess whether other services could decrypt such an alternative algorithm. The FEAL and MASSEY algorithms were discussed. They were still quite new at the time and there were only a few publications on their cryptanalysis.

The way out was to develop them in-house, officially based on DES, unofficially using the knowledge of the GOST. The starting point was a Feistel cipher, which was the common basis for both block algorithms.

Only the structure of the round function, the S-boxes, the expansion function and the number of 16 rounds were taken over from the DES.

5 GOST as Source for LAMBDA1

As early as 1984, East German cryptologists performed a control evaluation of the Soviet block cipher algorithm. It was based on a comparison with the published articles on DES. The knowledge gained was very useful in 1990 when an own algorithm had to be constructed.

Official sources on the DCA have not yet been found. However, there are no significant cryptographically relevant differences between the GOST algorithm and its predecessor.

Only features of the GOST that were used in the design of LAMBDA1 are listed here. The full description of GOST can be found on the website cited in the source (ZCO3).

The cipher standardized under GOST 28147-89 is a Feistel cipher with a key length of 256 bits, which corresponds to 32 8-bit characters. It is the Soviet counterpart to the Data Encryption Standard (DES).

The block length was also equal to 64 bits. At 32, the number of rounds was twice that of DES.

The key space is much larger and therefore the use of TPM (total trial method - brute force) is practically impossible.

Key scheduling is solved differently for GOST than for DES:

The first eight 32-bit round keys K_i are obtained from the key K dividing them into eight blocks, i.e. $K = (K_8, K_7, K_6, K_5, K_4, K_3, K_2, K_1)$, the round keys K_9 to K_{16} and K_{17} to K_{24} correspond again to the keys K_1 to K_8, the last eight round keys K_{25} to K_{32} are the first round keys in reverse order. All in all, we get the key order K_1, ... , K_8, K_1, ... , K_8, K_1, ... , K_8, K_8, ... , K_1.

The analogues to the S-boxes in the DES were eight interchangeable permutations P, each of which was used to realize four bit substitutions. They could also be used as secret key elements (long-term keys).

Instead of the bitwise addition of the binary vectors in the individual rounds in the DES, the addition *mod* 2^{32} was used.

6 LAMBDA1 Key Space and used Round Keys

The exact definition of the LAMBDA1 algorithm can be found in (ZCO3). A brief overview of this description is given in the chapters 6 to 9.

The key space for LAMBDA1 and the round key generation is borrowed from DCA/GOST. This was obvious as they also use 256 bits and the T-316 was already prepared for this key size. The key consists of 32 characters (S) of eight bits each (B):

$$S=(S1,S2,\ldots,S32)=(B_1,B_2,\ldots,B_{256})$$

The function T^{11} is a cyclic shift of a 48-bit vector. In the 16 round keys, only 192 bits are used. Accordingly, they are cyclically shifted by 11 bits each (see equations below). The keys K_{17} and K_{18} are used only once in the middle of the calculation in round 8. They are only 32 bits long.

The bits are assigned to the rounds according to the following rule:

$$K_1 := (B_1, \ldots B_{48})$$
$$K_2 := (B_{49}; \ldots B_{96})$$
$$K_3 := (B_{97}, \ldots B_{144})$$
$$K_4 := (B_{145}, \ldots B_{192})$$
$$\forall j \in 5,12: \quad K_j := T^{11}(K_{j-4}) \ldots$$
$$\forall j \in 13,16: \quad K_j := T^{11}(K_{25-j}) \ldots$$
$$K_{17} := (B_{193}, \ldots B_{224})$$
$$K_{18} := (B_{225}, \ldots B_{256})$$

The key S should be used as a time key and be valid for 7 days.

7 LAMBDA1 The modified Feistel Function

Until 1990, it was always assumed that trapdoors were hidden in the DES due to the design of the round function in conjunction with key scheduling. These would have led to a reduction in decryption effort. For this reason, the Feistel function for LAMBDA1 was modified. Only the expansion function and S-boxes are adopted from the Feistel function of the DES.

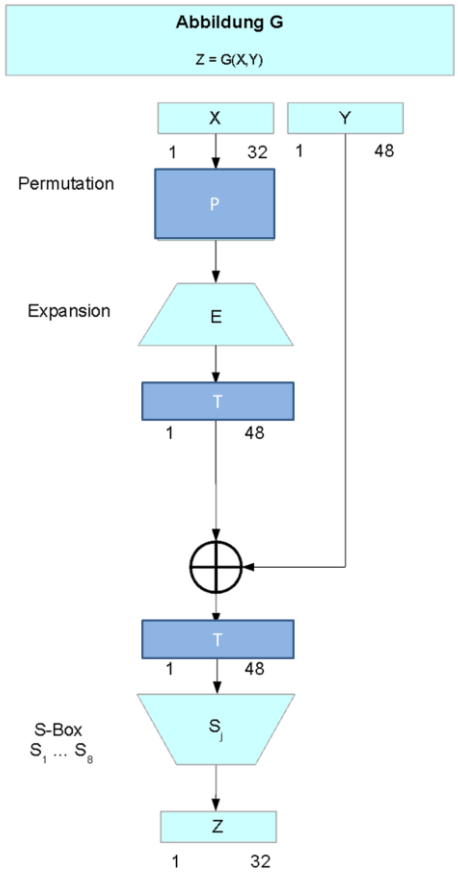

Figure 4: The modified Feistel function LAMBDA1

The idea of integrating a permutation P is retained. It is now positioned before the expansion function E. In addition, two cyclic shifts T of length 48 have been added. The additions are highlighted in darker color in Figure 4.

There was a well-founded hope that this change would eliminate all potential built-in weaknesses.

In addition, care was taken to ensure that the findings from the analysis of the round function of DES and GOST could also be applied to the modified version of LAMBDA1 (Chapter 10).

8 LAMBDA1 The Special Role of the 8th Round

The eighth round occupies a special position (Figure 5). It is therefore modified.

Here, in addition to the usual described round function, an additional round key (K_{17},K_{18}) with a length of 32 bits each is added using two additions $mod 2^{32}$ (also marked in darker color in Figure 5). This effects the mathematical description of the algorithm. The dependencies of the variables are no longer just binary. The idea for this came from the knowledge about the GOST. The idea was to add another option to neutralize possible trapdoors in the S-boxes of the DES. Due to the additions of this other addition, the K_{17} and K_{18} affect different bits in their sum depending on the contents of the 32-bit vectors to be summed.

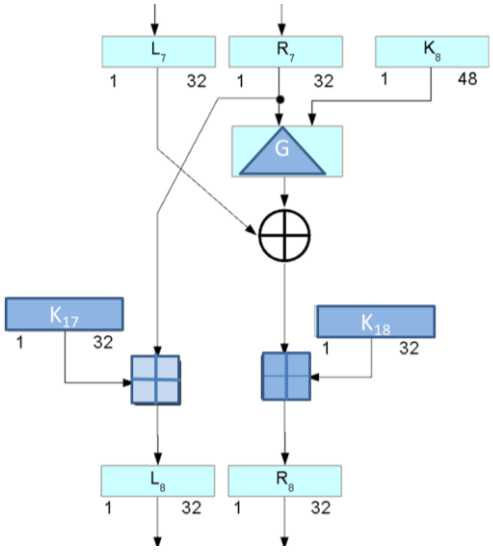

Figure 5: The eighth round of LAMBDA1

If a crypto attack has progressed to the middle round and information about the round keys is already available, then a barrier should be set up here, which would then also have to be overcome. For example, consider a scenario such as a meet-in-the-middle attack.

9 The Development Outcome

The algorithm was handed over to the developers of the T-316 device for technical implementation on March 12th, 1990.

Figure 6 illustrates the basic structure of the algorithm.

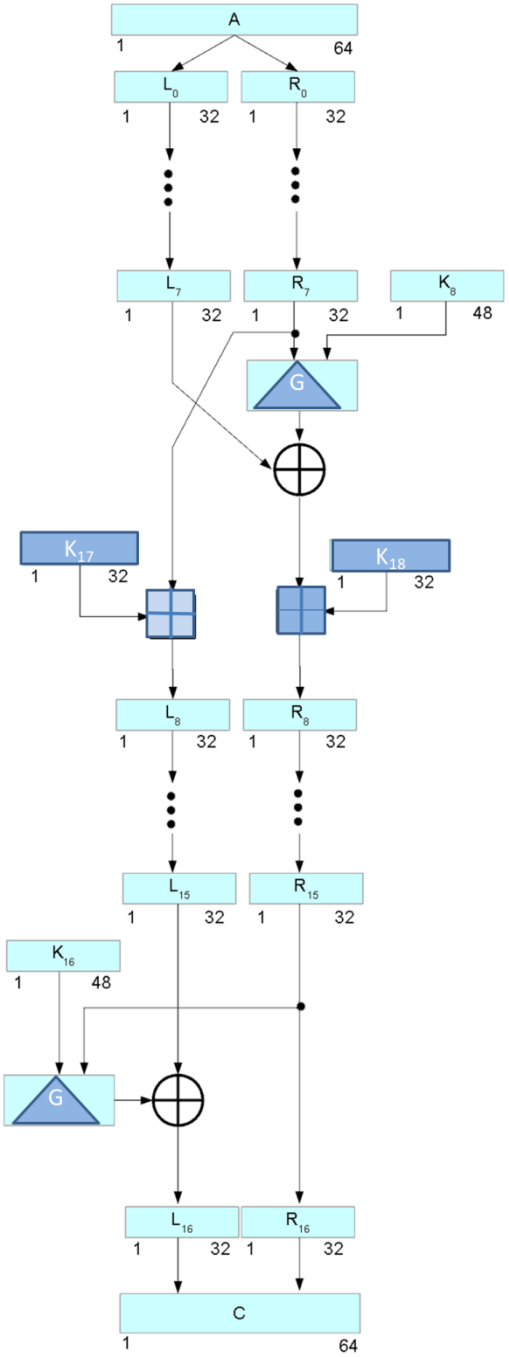

Figure 6: The Algorithm LAMBDA1[2]

[2] All figures are based on the sketches in, *DESCRIPTION LAMBDA1* (ZCO3 1990).

The algorithm was developed within about three weeks in February and March 1990. The following changes were made to the DES:

• The effective key length was increased from 56 bits to 256 bits.

• The way in which the key sequence is generated for the 16 round keys with a length of 32 bits each has been changed (section 6).

• The number of rounds is the same as the DES with 16 rounds.

• The 8th round has been modified by inserting two additional key vectors and adding them *mod* 2^{32}.

• Omission of the initial and final permutations of the DES. It is well known from the literature that the initial and final permutations in DES have no cryptographic relevance. That's why they were simply omitted.

• There is a built-in cryptographic reserve that can be activated if the permutation is kept secret. In this context, the term "long-term key" (commutator/permutation *P*) was introduced.

• If weaknesses or trapdoors were to appear, it would be conceivable to counteract them with this permutation.

• Different permutations P can also be used to define algorithms for different application areas and to separate them from each other.

• Obviously, the basics of GOST were sufficiently camouflaged. This was a desirable side effect at the time. The design results in the desired difference to both DES and GOST.

• Cryptographic attacks should be prevented, or at least made more difficult, for the intelligence services, which may be well versed in DES.

A thorough and comprehensive development analysis was not possible due to time constraints. To minimize the risk of use, tried and tested basic structures (Feistel ciphers) were used. Once development was complete, a control analysis was carried out with the resources available.

10 Analysis of the LAMBDA1 Algorithm

The cryptologic analysis began in mid-March and was interrupted after an inventory report in June 1990. Nine graduate mathematicians were involved, but they were only able to devote about 30% of their working time to the task. This means that about 180 hours of analysis work were invested.

Due to the chosen design, it was possible to use all known publications on the DES in the GDR in 1990 for the evaluation of LAMBDA1. This gave some assurance that the cryptographic properties of the algorithm were of good quality. The cryptology group's experience from years of development and analysis activities could also be successfully applied.

According to the report *Assessment Report LAMBDA1* (ZCO4 1990), in the short time until 22nd June, about 70 sources were examined and evaluated in terms of LAMBDA1 by these employees. From a cryptological point of view, the following results are worth mentioning, which are reproduced here in abbreviated form:

1. Following the DES-like functions examined in Even S., Goldreich O. (1983), studies of the group of LAMBDA1-like functions have been shown that the alternating group is present.

2. All weak and semi-weak keys with palindrome properties (Simmons G. J., Moore J. H. 1987) have been clearly identified. However, in relation to the key size of 2^{256}, their occurrence is orders of magnitude lower than in the DES.

3. Statements have been proven that significantly restrict the number and type of automorphisms in a basic automaton model of the LAMBDA1 algorithm. This excludes several classes of algebraic structures that could possibly be used cryptologically.

4. Double transitivity is an essential algebraic property of finite groups that should be proved for block ciphers. The verification of this property is also of interest for the analysis of LAMBDA1. So far, the theoretical basis for a computerized test has been worked out.

5. There are a number of different statistical studies in the literature that attempt to discover undesirable regularities in the cipher algorithm (Leung A. K., Tavares S. E. 1984). Experiments on the avalanche effect and the strict avalanche effect and on the testing of special bit dependencies have been planned and partly started. Due to the low performance of the

available computers, only a few tests could be carried out, a final evaluation is currently not possible. However, the tests so far do not show any abnormalities.

The results show that the specialists of ZCO were able to apply the experience gained from other analyses here and to achieve comparable results.

In 1990, the report concluded that there were no objections to use LAMBDA1 to protect classified information up to Top Secret (GVS) until Q1/91. The authorization was granted for a limited period of time, as a control analysis was planned in the near future.

The algorithm was proposed for implementation in a T-316 cipher despite the very short development and analysis period.

However, the LAMBDA1 evaluation report of June 1990 quoted above became the final report due to the political events.

The three literature sources cited here are examples of the state of knowledge at the time.

11 LAMBDA1 is not used

On 24 July 1990, the President of the Central Office for Information Security (Zentralstelle für Sicherheit in der Informationstechnik, ZSI) and future President of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), Dr. Otto Leiberich, made a business trip to Dahlwitz-Hoppegarten to visit the ZCO of the (still) GDR.

There is an internal protocol of the ZCO in which the conclusions from this visit are summarized. An excerpt from this *"Protocol of the ZCO on the Conclusions from this Business Trip of August 1, 1990"* (Killmann, Stephan. 2024 Appendix F) documents main objectives of this trip:

• Specification of the tasks of the ZCO for the territory of the GDR and, after unification, for the territory of the former GDR in a transitional period.

• Continuation of scientific and scientific-technical work, profiling of specialists to carry out analysis work for the evaluation and certification of information technology systems.

In this context, measures to continue work on T-316 and LAMBDA1 are also listed:

• T-316 Completion of the production introduction, preparation of the acceptance of the equipment by the manufacturer, preparation of the use of the equipment by the user, deadline: 11/90,

• Implementation of the framework agreement with Steremat-GmbH for the commercial use of the device, deadline: 8/90,

• Continuation of work on the development and analysis of the LAMBDA1 and DELTA algorithms and inclusion of the FEAL and MASSEY algorithms in the studies, deadline: 11/90.

The points quoted from the minute's show that the ZCO intended to continue working on the algorithm and the devices, also in coordination with or at least with the knowledge of the ZSI.

It is quite clear, that if the unification had not taken place so quickly, LAMBDA1 would probably have been used by the GDR to secure its communication; especially since ready-to-use T-316 GO devices were already available.

However, political developments in the GDR led to a rapid unification of the two German states. In the July and August, a government crisis developed in the GDR. This was accompanied by a rapid decline in the GDR economy. There was no longer any talk of a transitional period of about two to four years, as had been discussed in political circles. The system changed rapidly.

The two German states were unified on 3 October 1990. The LAMBDA1 block cipher algorithm was not used after that, nor was the T-316 device.

Acknowledgments

The author would like to thank Wolfgang Killmann and Franz-Peter Heider for fruitful discussions and support. The author would like to thank Jörg Drobick for publishing interesting information about the GDR cipher service on his website.

References

Michael Altenhuber. 2018. *Analyse und Implementierung der DDR-Chiffriermaschinen T-310/50 und T-316* Bachelorarbeit Nr. 1510239014
Analysis and implementation of the GDR cipher machines T-310/50 and T-316

CrypTool. 2.1 (Stable Build 9589.1) Programm https://www.cryptool.org/en/ct2/

Github.com. *https://github.com/tassadarius/LAMBDA1/tree/master/docs* (visited on 2023-11-20)

Jörg Drobick. *1990. Extensive documentation on the LAMBDA1 algorithm*
http://scz.bplaced.net/des.html#lambda
(visited on 2023-11-08)

Jörg Drobick. 1989. Informationen zu *T-316 GO*. *http://scz.bplaced.net/316.html*
(visited on 2023-11-08)

Shimon Even and Oded Goldreich. 1983. *DES-like function can generate the alternating group* - IEEE Trans. Inf. Theory, 1983, Vol. IT-29, No. 6, pp. 863-865

A. K. Leung and Safford E. 1984. *Sequence complexity as a test for cryptographic systems* - Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings.

G. J. Simmons and J. H. Moore 1987. *Cycle Structure of the DES for keys having palindromic (or anti-palindromic) sequences of rounds keys.* - IEEE Trans. Software Eng., 1987, Vol. SE-13, No. 2, pp. 262-273

Wolfgang Killmann and Winfried Stephan. 2024. *Das DDR-Chiffriergerät T-310: Kryptographie und Geschichte*. Springer Verlag, ISBN 978-3-662-67584-7
The GDR cipher device T-310: Cryptography and history

FIPS77. Federal Information Processing Standard Publication No. 46, January 1977. *DES Data Encryption Standard*
International Standard ISO 8372. 1987-08-15 Information processing - *Modes of operation for a 64-bit block cipher algorithm*

GOST89. *Encryption, Decryption and Message Authentication Code (MAC)*
https://www.rfc-editor.org/rfc/rfc5830
(visited on 2023-12-11)
Russian Federal standard for electronic encryption, decryption, and message authentication algorithms GOST 28147-89

ZCO1. 1987. *Bedarfsplanung zu den in der Entwicklung befindlichen Chiffriergeräten T-316 und T-314*, 19.08.1987 in BStU-ZAIG 25862
Demand planning for the T-316 and T-314 cipher devices under development

ZCO2. 1990. *Möglichkeiten und Gefahren der Nutzung des DES*, 20.02.1990
http://scz.bplaced.net/des.html#lambda1,
(visited on 2023-11-20)
Possibilities and dangers of using the DES

ZCO3. 1990. *LAMBDA1 64bit Blockchiffrierung, BESCHREIBUNG LAMBDA1*, 04.04.1990
http://scz.bplaced.net/des.html#lambda1,
(visited on 2023-11-20)
LAMBDA1 64bit block cipher, description

ZCO4. 1990. Referat 21. *Sachstandsbericht LAMBDA1* 22.06.1990;
http://scz.bplaced.net/des.html#lambda,
(visited on 2023-11-20)
LAMBDA1 Inventory Report