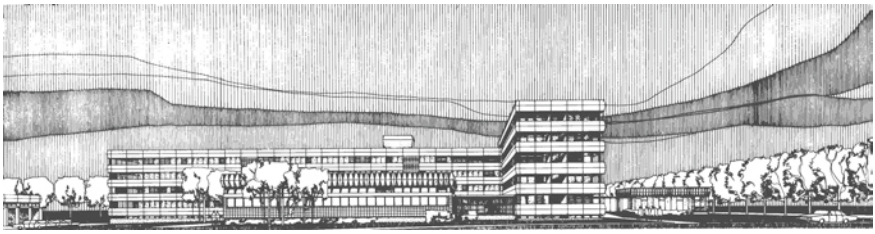
Wolfgang Killmann
Winfried Stephan

Das DDR-Chiffriergerät T-310

Kryptographie und Geschichte

Springer Spektrum

Das DDR-Chiffriergerät T-310



Gebäudekomplex des Zentralen Chiffrierorgans in Dahlwitz-Hoppegarten.
(Quelle: Privatarchiv)

Wolfgang Killmann · Winfried Stephan

Das DDR-Chiffriergerät T-310

Kryptographie und Geschichte

Springer Spektrum

Wolfgang Killmann
Neuenhagen, Brandenburg, Deutschland

Winfried Stephan
Sankt Augustin, Nordrhein-Westfalen
Deutschland

ISBN 978-3-662-61896-7 ISBN 978-3-662-61897-4 (eBook)
https://doi.org/10.1007/978-3-662-61897-4

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Planung/Lektorat: Iris Ruhmann
Springer Spektrum ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Unseren Frauen EVA und PETRA gewidmet

Geleitwort

Es bedurfte einer Revolution, damit dieses Buch geschrieben werden konnte. Nichts Geringeres als eines der größten Geheimnisse eines Staates wird in allen Details vor dem staunenden Leser ausgebreitet. Die jahrzehntelange Entwicklung und Nutzung eines äußerst sicheren Verschlüsselungssystems wurde nicht durch einen wissenschaftlich-technischen Kraftakt beendet wie bei der deutschen Enigma-Chiffriermaschine im zweiten Weltkrieg, sondern durch einen banalen Verwaltungsakt, der mit dem Ende des kalten Krieges und der deutschen Wiedervereinigung möglich geworden war. Kein spektakulärer Spionagecoup, sondern simple Aushändigung aller produzierten Geräte und sämtlicher in präziser mathematischer Form formulierten kryptologischen Konstruktionsprinzipien und Analysedetails markierte das Ende im Lebenszyklus dieses Chiffriersystems. Nach ihrer Auswertung durch die bundesrepublikanischen Fachbehörden wurden die ausgehändigten Unterlagen als obsolet angesehen und in den Aktenbestand des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (BStU) überführt. Der angemessene Aufbewahrungsort dieses Meilensteins deutscher Technikgeschichte ist aber m. E. nicht der Fundus der hässlichen Hinterlassenschaften eines repressiven politischen Apparats, sondern das Deutsche Museum, wie ich im Folgenden begründen werde.

Revolutionär für die Kryptographie selbst war die Veröffentlichung des Data Encryption Standard (DES) im Jahre 1975 und dessen Annahme als verbindlicher Verschlüsselungsstandard für die vertrauliche Kommunikation der US-amerikanischen Bundesbehörden. Man kann sagen, dass der DES den Anstoß gab sowohl zu der rasanten technischen Entwicklung kryptographischer Sicherheitskomponenten in IT- Systemen aller Art als auch und gerade der breit angelegten akademischen Disziplin der Kryptographie in der Mathematik, der Informatik und den Ingenieurwissenschaften.

Vor diesem Hintergrund ist es reizvoll, die Entwicklung des DES, die von einem Kryptologenteam der IBM durchgeführt wurde, mit der der ALPHA-Algorithmenklasse zu vergleichen, die Gegenstand des vorliegenden Buches ist. Eine Gruppe überwiegend junger Leute von etwa zehn Mitgliedern entwickelte, unter der Anleitung erfahrener Praktiker, aufbauend auf einem soliden technischen Hintergrund, die mathematischen Grundlagen für die konstruktiven und analytischen Elemente eines nachweislich sicheren kryptographischen Systems gemäß Kerckhoffs' Prinzip. Interessanter sind aber sowohl die Unterschiede in den

Ziel- und Aufgabenstellungen als auch denen der Anwendungsumgebung beider Projekte.

Ein entscheidendes Moment der Bedeutung des DES war, dass er ein STANDARD sein sollte, geeignet für die vielfältige Anwendbarkeit in Kommunikationssystemen aller Art, realisierbar gleichermaßen in Software und Hardware. Der Siegeszug der Chipkarte wurde durch einen universellen Kryptostandard erst möglich, die Nutzung in den unterschiedlichen Zahlungssystemen brachte die Förderung und Investitionen in Sicherheitstechnik zuerst in der Finanzindustrie, aus der sich das Verständnis für die Rolle der IT-Sicherheit zum reibungslosen und störungsfreien Funktionieren der gesellschaftlichen Infrastrukturen insgesamt entwickelte. Von praktischer Relevanz des DES war zu dem die Möglichkeit, ihn flexibel in unterschiedlichen Betriebsarten zu nutzen und auch den Schlüsselraum durch Einführung des Triple-DES drastisch zu vergrößern und damit das kryptographische Sicherheitsniveau zu erhöhen. Der DES war ein Blockchiffrieralgorithmus, der Nachrichten in Blöcke von jeweils 64 Bits portionierte und verschlüsselte. Aus einem festen Schlüssel von 56 Bits wurden dabei 16 Zustandswechsel je Eingabeblock gebildet, deren Wirkung insgesamt den 64 Bit langen Chiffreblock ergab. Dafür wurden neue schnelle Hardware-Bausteine entwickelt, die in den verschiedenen Betriebsarten (ECB, CFB, CBC, OFB) genutzt werden konnten, um die sprunghaft steigenden Bedarfe und Märkte des Kommunikations- und IT-Zeitalters mit Sicherheitstechnik abdecken zu können.

So unterschiedlich wie die Aufgabenstellungen waren die kryptologischen Methoden und Konzepte des ALPHA- und des DES-Entwicklungsteams. Die ALPHA-Entwickler waren vor gänzlich andere Aufgaben gestellt, deren Rahmenbedingungen durch die intendierte Verwendung im militärisch-administrativen Umfeld mit einem etablierten Schlüsselmanagement gegeben waren, bei dem ein großer Anteil auch von organisatorischen Sicherheitsmaßnahmen abgedeckt werden konnte. Der DES wurde für einen offenen, die ALPHA-Algorithmen für geschlossene Nutzerkreise vorgesehen.

Das kryptologische Basiskonzept der ALPHA-Algorithmenklasse war ein Automat mit 2^{36} Zuständen, der taktweise aus einem Paar von jeweils 120 Schlüsselbits und einem 61 Bit langen Initialvektor einen Zustandswechsel erzeugte und nach je 127 Takten ein einzelnes Bit für den Bitstrom ausgab, aus dem dann ein Strom von Substitutionen zur buchstabenweisen Verschlüsselung von Fernschreib(klar)texten produziert wurde. Dazu wurden jeweils 13 konsekutive Bits des Stroms zur Auswahl einer von 992 möglichen Substitutionen des Fernschreibalphabets verwendet. Bei der technischen Realisierung des Automaten konnte auf bewährte Bauelemente aus der DDR-Produktion zurückgegriffen werden, mit denen die üblichen Fernschreibübertragungsraten von 50–100 Baud problemlos erreicht wurden.

Eine besondere Finesse des Konzepts bestand darin, dass ein Teil der Logik des Automaten hardwaremäßig auswechselbar war. Dadurch entstand einerseits eine ganze Familie verschiedener Ausprägungen des gleichen Kryptosystems, das andererseits für jede Instanz, jeden sogenannten Langzeitschlüssel, den Nachweis der geforderten kryptographischen Eigenschaften erforderlich machte. Jeder

Langzeitschlüssel erzeugte acht feste Transformationen der Zustände, von denen jeweils eine durch einen Steuerstrom von Bittripeln ausgewählt und für den nächsten Zustandsübergang genutzt wurde.

Am Anfang des Buches zeigt eine Abbildung die Silhouette vom Hauptgebäude des Zentralen Chiffrierorgans der DDR (ZCO). Die Entwicklung, über die in diesem Buch detailliert berichtet wird, fand in einem modernen funktionalen Bau in der Art eines Forschungs- und Entwicklungscampus statt, nicht in einer finsteren Lubjanka. Die Bauherren haben gut begriffen, wie wichtig eine attraktive offene Gestaltung des Umfelds für kreatives und zugleich intensives und zielgerichtetes Arbeiten ist, ob einzeln oder im Team. Aufschlussreich ist der Einblick in das systematische mathematisch-kryptologische Training durch renommierte Professoren sowjetischer Universitäten (gleichwohl hochrangige KGB-Offiziere), von denen zwei im Buch näher vorgestellt werden.

Ob es am akademischen Hintergrund dieser Berater liegt, vermag ich nicht zu beurteilen. Ein großer Teil des vorliegenden Buches jedenfalls ist in der Fachsprache der reinen Mathematik geschrieben, in exakter algebraisch-algorithmischer Diktion formuliert. Dies betrifft sowohl die Darstellung der kryptographischen Spezifikation als auch die kryptoanalytische Untersuchung der Wirksamkeit der konstruktiven Maßnahmen. Manchen Leser wird es überraschen, dass die praktische Arbeit eines Kryptologen zu einem großen Teil in theoretischer Grundlagenforschung besteht, zu anderen großen Teilen in der Modellierung stochastischer Prozesse und in umfangreichen langwierigen statistischen Analysen. Als Beispiel mag die Forderung genannt sein, dass nur solche Langzeitschlüssel zum operativen Einsatz zugelassen wurden, bei denen eine Einzelfalluntersuchung verifiziert hatte, dass die von ihnen bestimmte Permutationsgruppe die alternierende Gruppe von 2^{36} Elementen enthält. Eigenschaften dieser Art sollten gewährleisten, dass nicht aus kompromittiert gewordenen Teilen des Bitstroms dessen weitere Sequenz vorhersagbar würde oder die geheimen Schlüssel berechnet werden konnten.

Tatsächlich betreibt das Buch eine Demystifizierung und ersetzt das Geraune über die fantastischen Mittel und Möglichkeiten des ZCO durch eine Beschreibung der akribischen, soliden und gewissenhaften kryptologischen Arbeit, die dort geleistet wurde. Nur auf dieser Grundlage konnte eine sorgfältige verantwortungsvolle Abwägung der Risiken getroffen werden, die einer seriösen Entscheidungsfindung vor dem operativen Einsatz vorausgehen muss. Das Bewusstsein für ein verbleibendes Restrisiko und dessen qualitative Bewertung, aber auch die methodische Erarbeitung geeigneter Abläufe für die Nutzungsphase des kryptographischen Gesamtsystems als wichtige Aspekte und Aufgaben werden ausführlich dargelegt. Detailliert wird die Bedeutung von Schlüsselerzeugung und -verteilung als wesentliche Komponenten des Gesamtkonzepts erläutert.

Die Rolle der Fernschreiber in der Kommunikationstechnik wurde in den 1980er Jahren immer unbedeutender, im Westen etwa fünf bis sechs Jahre früher als im Osten. Sichere Daten- und Kommunikationsnetze! hieß die neue Aufgabe. Jeder höhere Grad der Vernetzung in Wirtschaft, Industrie, öffentlicher Verwaltung und im Alltag erforderte geeignete kryptographische Schutzmaßnahmen. Dem

veränderten Bedarf trug man ab 1985 durch eine Neustrukturierung der Zentralstelle für das Chiffrierwesen (ZfCh) in Bonn-Mehlem Rechnung, indem ein Teil ihrer Aufgaben im Februar 1987 in einer neuen Zentralstelle für Sicherheit in der Informationstechnik (ZSI) unter der Aufsicht des Bundesinnenministeriums zugeordnet wurde. Ein entscheidender Schritt war die Herausgabe der IT-Sicherheitskriterien im Juni 1989, durch die die Positionierung und Aufgabenstellung der ZSI für die Öffentlichkeit dokumentiert wurde. Zu Jahresbeginn 1991 wurde aus der ZSI das neue Bundesamt für Sicherheit in der Informationstechnik (BSI) gegründet, zu dessen Aufgaben und Kompetenzen die Bearbeitung der technisch-wissenschaftlichen Grundlagen der Informationssicherheit sowie die Prüfung von DV-Systemen auf Sicherheit und Vertrauenswürdigkeit gehörten. Dr. Otto Leiberich, der Leiter der ZfCh, wurde Gründungspräsident des BSI.

In dieser Phase technischer und organisatorischer Veränderungen der IT-Sicherheit für Gesellschaft, Wirtschaft und Staat ging mit dem Fall der Berliner Mauer der kalte Krieg zwischen Ost und West zu Ende. Aufgrund des Einigungsvertrages von 1990 wurde das ZCO aufgelöst, dessen Dokumente und Geräte an die Behörden der Bundesrepublik übergeben.

Welchen Nutzen und welche Relevanz hatten die übergebenen Informationen für die westdeutschen Stellen, die nunmehr nicht nur Wissensfragmente gewannen, sondern sogar alle Details der ALPHA-Algorithmenklasse geliefert bekamen? Die ausgehändigten Dokumente des ZCO belegen eine tiefschürfende und ausführliche Untersuchung der Konstruktion und geben Aufschluss von einer äußerst gewissenhaften Kryptoanalyse, die keinerlei Schwachstellen zu Tage gebracht hat. Auch die Kenntnis aller konstruktiven Details nutzt nichts, die Kompromittierung des Bauplans ist sogar das Ausgangsszenario der Analysen. Die Resistenz gegen alle denkbaren Angriffe ist exzellent begründet. Das Kerckhoffs' Prinzip wurde vorbildlich umgesetzt.

Auf Seiten von ZSI/BSI gab es andererseits eindeutig keinen Bedarf an diesem System, im Zuge NATO-weit einheitlicher Lösungen war auf eigene Entwicklungen von Stromchiffren sogar verzichtet worden. Auch zu den Aufgaben des BSI konnten sie unmittelbar keinen signifikanten technischen Beitrag leisten, ebenso wenig wie die subtilen, aber auch sehr speziellen, grundsätzlichen mathematischen Ergebnisse, die bei der Arbeit am ALPHA-System gewonnen wurden. Bei einer nüchternen Betrachtung war daher der geschenkte kryptologische Schatz für das BSI wertlos.

Blockchiffren wurden das Mittel der Wahl zur kryptographischen Sicherheit in Kommunikations- und IT-Systemen. Zwar wurde der DES-Algorithmus durch den AES ersetzt, weil sich letztlich der Schlüsselraum als zu klein erwies, jedoch war seine Entwicklung wegweisend für Sicherheit im Informationszeitalter und gab den entscheidenden Anstoß für die explosive theoretische und praktische Stellung, die die Kryptologie heute einnimmt.

Das Erbe der ALPHA-Entwicklung ist weniger spektakulär aber gleichwohl sichtbar. BSI-Präsident Leiberich schätzte die Qualität der Kryptologen des ZCO sehr hoch ein und wollte deren Know-how für den Aufbau seines neuen Bundesamtes sichern. Eine besondere Rolle kamen nach seiner Meinung einer stringenten

Entwicklungssystematik und der entwicklungsbegleitenden Evaluierung zu und er ermunterte daher Firmen aus dem Auftragnehmerkreis des BSI, aktiv auf die Erfahrungen des ZCO zuzugreifen und die teilweise arbeitslos gewordenen Leute als eigene Mitarbeiter zu gewinnen. Diese Strategie erwies sich als sehr erfolgreich, im Laufe der Jahre entstand eine gut kooperierende Community, die im wirtschaftlichen Wettbewerb der Sicherheitsindustrie innerhalb der EU gut etabliert war.

Die genial-einfachen ALPHA-Algorithmen können auch nach heutigen Maßstäben noch eine starke Verschlüsselung leisten, wenn man ihre Prinzipien verstanden hat. Die vorliegende kryptographische Biographie ist eine gediegene Arbeit, möchte ich sagen – sie hat unseren Respekt verdient.

Hürth F.-P. Heider
April 2020

Vorwort

Das Gerät T-310 war das am weitesten verbreitete Fernschreibchiffriergerät in der DDR. Die DDR gibt es seit 30 Jahren nicht mehr. So gut wie alles aus dieser Zeit wurde negiert und geriet mehr oder weniger in Vergessenheit. Seit 1995 veröffentlicht Jörg Drobick eine umfangreiche Dokumentation zum Chiffrierwesen der DDR. im Internet [32]. Der Chiffrieralgorithmus des Geräts T-310 wurde 2006 in der Fachzeitschrift *Cryptologia* veröffentlicht [63]. Der vor fast 50 Jahren in der DDR entwickelte Algorithmus ist immer noch Gegenstand kryptologischer Untersuchungen. Die Kryptologen der DDR werden an der *Kryptologischen Analyse des Chiffriergeräts T-310/50* [2] aus dem Jahr 1980 gemessen und bewertet. Unsere späteren Ergebnisse bis 1990 sind noch nicht öffentlich zugängig. Das scheinbar ungebrochene Interesse an dem Algorithmus und der Untersuchung seiner Sicherheit erstaunte und elektrisierte uns, denn wir sind zwei der Entwickler dieses Chiffrieralgorithmus und auch Mitautoren dieser Analyse. Der besondere Reiz, sich wieder mit dem Thema zu beschäftigen, erwächst für uns vor allem aus der Tatsache, dass die neuen Analyseergebnisse von Kryptologen der uns nachfolgenden Generation erarbeitet wurden. Ihnen stehen heute ganz andere mathematische Erkenntnisse und Methoden, aber auch deutlich bessere technische Möglichkeiten zur Verfügung. So bekamen wir beim Lesen den Eindruck, dass sich heute kaum noch jemand vorstellen kann, wie wir damals arbeiteten und über welche Mittel wir zu jener Zeit verfügten.

Die Entwicklung und der Einsatz der T-310 muss in der historischen Situation gesehen werden. Der Chiffrieralgorithmus, das Gerät T-310 und deren Analyse sind Kinder ihrer Zeit. Der Chiffrieralgorithmus war der zweite einer Algorithmenklasse und, weil sich die technische Basis änderte, war er der letzte seiner Art. Der Chiffrieralgorithmus und das Gerät T-310 waren auf die heute weitgehend ausgestorbene Fernschreibtechnik und deren Übertragungsgeschwindigkeit abgestimmt. Für die kryptographische Analyse nutzten wir die uns damals verfügbaren mathematischen Methoden, aber auch die Kopplung von Spezialtechnik an Computer für umfangreiche Routineberechnungen. Es kommt nur selten vor, dass ein zum Schutz von Staatsgeheimnissen verwendeter Chiffrieralgorithmus und dessen Analyse durch seine Entwickler in der Öffentlichkeit bekannt werden. Deshalb ist es nach genauerer Überlegung auch nicht verwunderlich, dass sich Kryptologen aus dem akademischen Bereich jetzt noch mit diesem alten Algorithmus beschäftigen. Während es in den 70er Jahren weder in

Ost noch in West kaum eine öffentliche akademische Kryptographie gab, kann sich heute die gesamte Kryptocommunity einem Algorithmus zuwenden. Dass daraus neue Erkenntnisse, aber auch Fragen und gelegentliche Missverständnisse entstehen, ist ganz natürlich. So haben wir uns entschlossen, aus dem Schatten der Verschwiegenheit herauszutreten und unseren Beitrag zum besseren Verständnis unserer Arbeit und damit zur Geschichte der Kryptologie zu leisten. Die Arbeiten an der T-310 waren mehr als 15 Jahre lang der Mittelpunkt unserer beruflichen Tätigkeit. Wenn wir von unseren Ergebnissen der T-310-Entwicklung und Analyse sprechen, dann sind immer die Resultate gemeint, die von den Mitarbeiterinnen und Mitarbeitern des Zentralen Chiffrierorgans der DDR erarbeitet wurden. Die Darstellung und Bewertung dieser Ergebnisse in diesem Buch sind sicher nicht vollständig und auch subjektiv beeinflusst, das lässt sich nicht vermeiden. Die erneute Beschäftigung mit ihnen ist für uns auch ein Ausflug in unsere Vergangenheit. Deshalb wählten wir den Untertitel des Buches *Kryptographie und Geschichte.* Uns würde es freuen, wenn wir zum Verständnis unserer damaligen Denk- und Arbeitsweise beitragen und eine Brücke zur heutigen Kryptographie schlagen können.

Wolfgang Killmann
Winfried Stephan

Inhalt und Aufbau des Buches

Das Dokument ist in vier Hauptteile untergliedert. Im ersten Teil beschreiben wir die Rahmenbedingungen für die Entwicklung des Chiffriergeräts T-310. Wir beginnen mit einer historischen Einordnung der Entwicklung und Analyse des Chiffriergeräts T-310, seiner Zweckbestimmung und den vorgesehenen Einsatzbedingungen. Es folgt eine kurze Einschätzung des damaligen kryptologischen Wissensstandes und wir beschreiben, wie wir unser Wissen mit Unterstützung sowjetischer Kryptologen kontinuierlich erweitern konnten. Die von uns genutzten Grundbegriffe des Chiffrierwesens werden vorgestellt. Wir erläutern unser methodisches Herangehen an die Entwicklung des Geräts auf der Basis definierter operativer und technischer Forderungen an das Chiffrierverfahren. In Verbindung mit der Definition des Begriffs der quasiabsoluten Sicherheit werden grundlegende Überlegungen zur Sicherheit von Chiffrierverfahren und -algorithmen diskutiert.

Im zweiten Teil stellen wir in den ersten drei Kapiteln den T-310-Algorithmus vor. Die mathematische Definition des Algorithmus und die Anforderungen an die strukturbestimmenden Langzeitschlüssel im Kap. 5 und im Abschn. 8.8 sind als Einheit zu sehen. In den weiteren Kapiteln diskutieren wir die Ergebnisse der Entwicklungsanalyse [2]. Wo es uns sinnvoll und für das Verständnis notwendig erscheint, erläutern wir die Ergebnisse genauer oder beweisen sie. Als Beispiel sei hier auf das Kap. 8 verwiesen. Die Methode zum Nachweis der Primitivität der durch eine Abbildung im Chiffrieralgorithmus erzeugten Gruppe ist in der Literatur in dieser Form nicht zu finden und wird deshalb ausführlicher beschrieben. An anderen Stellen setzen wir ein gewisses kryptologisches und mathematisches Grundwissen voraus und verweisen lediglich auf entsprechende Quellen. Die gewollte Kompliziertheit des Chiffrieralgorithmus führt auch dazu, dass mitunter nur Modelle betrachtet werden können (Kap. 9) oder in der Analyse nur Teilergebnisse erreicht werden konnten. Im letzten Kapitel unternehmen wir den Versuch einer kryptologischen Bewertung des Chiffrieralgorithmus T-310 und ziehen dazu auch Ergebnisse aus [27] heran.

Der dritte Teil des Buches beschreibt die Chiffriergeräte T-310/50 und T-310/51 sowie deren Anwendung. Die Chiffriergeräte implementierten den Chiffrieralgorithmus T-310 und die Zusammenarbeit mit der Nachrichtentechnik. Die Integration der Chiffriergeräte in Nachrichtennetze und ihr sicherer Einsatz setzte eine geeignete Infrastruktur und verbindliche Anwendungsvorschriften voraus. Der Einsatz der Geräte wurde durch Vorschriften geregelt, deren Gesamtheit das

Chiffrierverfahren bestimmen. Wir stellen dar, wie wir bei der Entwicklung und Analyse unserer Chiffrierverfahren diese Aspekte berücksichtigten. Nicht zuletzt wird im Rahmen der Analyse der Verfahren eingeschätzt, welche kryptologischen Angriffe auf ein Chiffrierverfahren praktisch möglich sind und umgekehrt, welche in der Algorithmusanalyse gefundenen potentiellen Schwachstellen praktisch ausnutzbar sein könnten.

Im vierten und letzten Teil legen wir dar, wie sich zur politischen Wende 1990 das Ende des Einsatzes der T-310 gestaltete und wie wir diesen Prozess begleiten mussten. Soweit es zum Verständnis wichtig ist, gehen wir auf die gesellschaftlichen und historischen Rahmenbedingungen ein. Deshalb beschreiben wir auch den Zusammenhang zwischen dem Ende des Einsatzes der T-310 und dem Ende der DDR. Für historisch Interessierte könnte dies neben der Kryptologie von eigenständigem Interesse sein. Im letzten Kapitel beschreiben wir, wie uns unser kryptologisches Fachwissen beim Neuanfang in der Bundesrepublik geholfen hat.

Im Anhang finden sich eine Liste der Vortragsthemen sowjetischer Kryptologen, eine Liste von Dokumenten zum Chiffrieralgorithmus T-310, die noch nicht wieder verfügbar sind, Protokolle zweier Dienstreisen nach Bonn im Sommer 1990 und die Kurzbeschreibung einer Algorithmenklasse LAMBDA, die 1990 unter Zeitdruck für kommerzielle Anwendung entwickelt wurde.

Wir danken dem Springer-Verlag, der dieses Buch ermöglichte. Dr. Franz-Peter Heider motivierte uns zum Schreiben dieses Buches. Ihm gilt unser besonderer Dank für seine uneigennützige Unterstützung mit seinem Fachwissen und der Prüfung der Zyklenberechnungen. Wir danken dem Leiter des NVA-Museums in Harnekop für die Einsichten in Originaldokumente und die Möglichkeit, Fotos vom Gerät T-310 und relevanten Unterlagen zu erstellen. Insbesondere gilt unser Dank Jörg Drobick, durch dessen Internetseiten [32] uns viele Dokumente, die wir im Rahmen unserer Arbeiten zur T-310 erstellten, wieder zugänglich wurden. Damit hat er uns sehr geholfen, unsere Erinnerungen aufzufrischen und anhand der verfügbaren Materialien zu objektivieren. Er unterstützte uns in Konsultationen in dankenswerter Weise mit weiteren Informationen.

Wir danken Dr. Petra Stephan für die kritische Begleitung und die Übernahme umfangreicher redaktioneller Arbeiten.

Inhaltsverzeichnis

Teil I
Rahmenbedingungen für die Entwicklung

„Nur vordergründig kämpfen Codemaker gegen Codebreaker. In Wirklichkeit findet ein wissenschaftlicher Krieg zwischen den Staaten statt."

Dr. Otto Leiberich [47]

T-310-Chronologie

1

Inhaltsverzeichnis

Das Chiffriergerät T-310 sowie das zugehörige Chiffrierverfahren ARGON waren die wichtigsten Eigenentwicklungen des Zentralen Chiffrierorgans der DDR (ZCO). In den 70er Jahren entwickelt, kam die T-310 nach ihrer Erprobung ab 1983 vor allem in den Staats- und Sicherheitsorganen der DDR zum Einsatz. Zum Ende der DDR existierten fast 3 900 dieser Geräte, die nach der Vereinigung der beiden deutschen Staaten auftragsgemäß so gut wie alle vernichtet wurden. Dieser Lebenszyklus, vom Beginn der Entwicklung über einzelne Entwicklungsetappen bis zur Vernichtung der Geräte, wird im Überblick skizziert. Die personellen, technischen und wissenschaftlichen Voraussetzungen für die Entwicklungsarbeiten, insbesondere die Zusammenarbeit mit den sowjetischen Kryptologen, werden im historischen Kontext beschrieben.

1.1 Historische Einordnung

Das Chiffriergerät T-310 wurde für die Verschlüsselung von Fernschreibverbindungen konzipiert und in den 80er Jahren in mehreren Varianten produziert, wie aus der folgenden Chronologie hervorgeht. Das Chiffrierverfahren ARGON mit dem Chiffriergerät T-310/50 diente zum Vor-, Teildirekt- und Direktchiffrieren von Fernschreiben über Wahl-, Stand- und Funkverbindungen mit einer Übertragungsgeschwindigkeit von 50 oder 100 Baud. ARGON wurde in den Nachrichtenverbindungen der Staatsorgane der DDR (Staatsrat, Ministerrat, Ministerien, Rat der Bezirke und Kreise), den Sicherheitsorganen der DDR (Ministerium für Nationale

W. Killmann and W. Stephan, *Das DDR-Chiffriergerät T-310,*
https://doi.org/10.1007/978-3-662-61897-4_1

Abb. 1.1 Das Gerät T-310/50 (Harnekop NVA Museum)

Verteidigung, Ministerium des Innern, Ministerium für Staatssicherheit), der Sozialistischen Einheitspartei Deutschlands, der Freien Deutschen Jugend und des Freien Deutschen Gewerkschaftsbundes sowie ausgewählter Kombinate eingesetzt. 1989 waren 3 835 Geräte T-310/50 im Einsatz. Der Einsatz des Chiffriergeräts war auf das Gebiet der DDR beschränkt, mit einer Ausnahme: Das Ministerium für Außenhandel setzte die T-310 zeitweise auch im Ausland ein, z. B. während laufender Vertragsverhandlungen. Die Nationale Volksarmee (NVA) nutzte das Chiffrierverfahren ARGON für Nachrichtenverbindungen der Verwaltung (Ministerien, Teilstreitkräfte, Militärbezirke, Wehrbezirkskommandos) und der Grenztruppen. Die Volksmarine nutzte 70 Geräte T-310/51 mit dem Chiffrierverfahren SAGA für die Darstellung der technischen und operativen Lage sowie für die Kommunikation der technischen Beobachtungskompanien (s. Abschn. 12.2). Verbände, die mit den anderen Armeen des Warschauer Vertrags zusammenwirkten, nutzten für die Kommunikation andere Chiffrierverfahren.

Einen Eindruck vom Aussehen des Geräts vermittelt Abb. 1.1.

Mit der Entwicklung der Nachrichten- und Computertechnik wurden weitere Anwendungsgebiete der Chiffriergeräte T-310/50 mit Personalcomputern und Fernschreibmodems untersucht und getestet. Das Zentrale Chiffrierorgan (bis 1989 im Ministerium für Staatssicherheit, ab 1990 Zentrales Chiffrierorgan im Ministerium für Innere Angelegenheiten) entwickelte auch Chiffrierverfahren für den kommerziellen Einsatz. Dazu gehörte die Verwendung der Chiffriergeräte T-310/50 im Chiffrierverfahren ADRIA (s. Abschn. 12.1) mit gesonderten Langzeitschlüsseln (Kap. 5) und Gebrauchsanweisungen mit empfehlendem Charakter für den Einsatz mit Personalcomputern und anderer Kommunikationstechnik.

Wer sich über die T-310 umfassend informieren möchte, dem empfehlen wir [32]. Die technischen Daten des Chiffriergeräts und die Einsatzbedingungen sind dort ausführlich beschrieben. Außerdem ist dort eine umfangreiche Dokumentation zum Chiffrierwesen der DDR zu finden, die wir als Gedanken- und Erinnerungsstütze nutzen konnten. Die wahrscheinlich erste Publikation in der Fachliteratur über das Gerät T-310 mit einer vollständigen Beschreibung des Chiffrieralgorithmus erfolgte durch Klaus Schmeh 2006 in der *Cryptologia* [63]. Später gab Nicolas T. Courtois dazu eine Reihe kryptologischer Untersuchungen heraus [27], auf die wir im Kap. 11 näher eingehen.

1.2 T-310-Chronologie

Der Lebenszyklus des Chiffriergeräts T-310 von den Anfängen der Entwicklung bis zur Vernichtung fast aller Geräte wird in der folgenden Kurzchronologie zusammengefasst. Hierfür stützen wir uns wesentlich auf die T-310-Chronologie in [32].

1973	Erste Festlegung der taktisch-technischen Anforderungen an das Gerät T-310 für die Verschlüsselung von Fernschreiben und Daten
1974	Konstruktion eines neuen Chiffrieralgorithmus, Einführung des Substitutionsalgorithmus für 5Bit- und 8Bit-Einheiten
1975	Pflichtenheft T-310, Verwendung des Algorithmus SKS V/1

1976	Trennung in T-310/50 Fernschreibchiffriergerät und T-310/80 Datenchiffriergerät
1977	A-Pflichtenheft T-310 (Stufe A2)[1]
1978	K-Pflichtenheft T-310 (Stufe K2)[2], Änderung des Chiffrieralgorithmus und technisch bedingte Einschränkungen des Langzeitschlüssels
1980	Dokumentation der Analyseergebnisse zur kryptologischen Sicherheit des T-310-Chiffrieralgorithmus durch Kryptologen des ZCO und mit beratender Unterstützung durch sowjetische Kryptologen (die Analyse erfolgte parallel zur Entwicklung, mindestens ab 1974) [2]
1980	Operative Erprobung des Geräts T-310
1982	Beginn der Serienproduktion der Geräte T-310/50, Fortführung der technisch-kryptologischen Untersuchungen
1983	01.06.1983 Beschluss zur Vervielfältigung und Anwendung der Gebrauchsanweisung ARGON
1984	Vorbereitung zur Einführung des Chiffrierverfahrens SAGA mit dem Gerätesystem T-310/51 (modifizierte K-Muster T-310/50) für die Volksmarine
1985/1986	Truppenerprobung des Chiffrierverfahrens SAGA
1987	Vorstellung der T-310/50 als nationales Chiffriergerät auf dem Treffen der Chiffrierdienste des Warschauer Vertrages, Kaufwünsche der ungarischen Volksarmee wurden abschlägig behandelt
1988	Festlegung, dass ab Ende 1989 keine weiteren T-310/50 produziert werden
1990	Letzter Wechsel des Langzeitschlüssels (LZS), Einsatz des LZS-33
1990	Mai: Einrichtung einer T-310-Chiffrierverbindung zwischen dem BRD-Regierungsbunker im Ahrtal und dem DDR-Regierungsbunker in Prenden für die Verbindung der Fernschreibnetze der beiden Innenministerien, Einrichtung einer weiteren Chiffrierverbindung zwischen der Hardthöhe und der Hauptnachrichtenzentrale in Strausberg für den Nachrichtenverkehr Bundeswehr - NVA
1990	08. bis 10.07.1990: Vorstellung des Geräts T-310 einschließlich seiner grundlegenden kryptologischen Eigenschaften in der Zentralstelle für Sicherheit in der Informationstechnik (ZSI) in Bonn
1990	25.07.1990: Vorstellung der T-310 in den Rathäusern Berlins durch Politiker und das Fernsehen, um die Aufgaben der Chiffrierstellen in Betrieben und Verwaltungen klarzustellen (vgl. Presse- und Fernsehbeiträge aus dieser Zeit)
1990	01.08.1990: Beschluss, dass keine kommerzielle Nutzung der T-310/50 ADRIA erfolgen soll
1990	16.08.1990: Übergabe einer T-310/50 an das ZSI
1990	Oktober bis Dezember: Vernichtung fast aller T-310-Geräte

[1] Die A-Stufen stehen für angewandte Forschung [50].
[2] Die K-Stufen stehen für die Entwicklung und Einführung von Erzeugnissen [50].

Es gab 1989 folgende Chiffrierverfahren auf der Basis des Geräts T-310 [32]:

- ARGON-F = FS-Modem; T-310/50 an das FS-Modem angebunden
- ARGON-E = eFSM; elektronische Fernschreibmaschine
- ARGON-VU1 ... VU3 = V.24 Umsetzer in den Varianten 1 ... 4
- ARGON-R = RFLZ
- ARGON-PC = Z1013 mit FS-Modem an einer T-310/50 ADRIA

Ab 1990 waren folgende kommerzielle Versionen vorbereitet [32]:

- ARGON/ADRIA V1 Konfiguration mit F1300 oder F2001 Fernschreibmaschine, 100 Baud
- ARGON/ADRIA V2 Konfiguration mit PC zur Steuerung und Nutzung der Fernschreibmaschinen als Drucker
- ARGON/ADRIA V3 Konfiguration mit PC und Paralleldrucker
- ARGON/ADRIA V4 Konfiguration mit PC und Paralleldrucker, das Fernschreibgerät wird durch Softwarelösung des PC ersetzt

Mit Stichtag 04.11.1989 waren im Einsatz:
T-310/50: 3 835 Geräte
T-310/51: 46 Geräte

Die hohe Anzahl von fast 3 900 Geräten, die sich 1989 im Einsatz befanden, entsprach dem Sicherheitsbedürfnis der DDR an der Nahtstelle zwischen NATO und Warschauer Vertrag zum Schutz vor Fernmeldeaufklärung durch die BRD, die USA und andere Staaten. Die Fernmeldeaufklärung gegen die DDR ist in der Literatur ausreichend belegt ([52, Teil III], [17, S. 454 ff.], [33, S. 216 ff.]).

1.3 SKS V/1 – Die Vorgeschichte

Die Geschichte der Entwicklung der T-310 wäre ohne Verweis auf den Vorläufer SKS V/1 nur unvollständig erzählt und bestimmte Entwicklungsentscheidungen wären kaum nachvollziehbar. Der Algorithmus des Chiffriergeräts T-310 basiert kryptologisch gesehen auf dem Algorithmus SKS V/1. Über das Gerät selbst und die Einsatzbedingungen scheint wenig bekannt zu sein. Selbst für die Abkürzung haben wir in den Quellen keine Erklärung gefunden. Wir vermuten aber, dass SKS die Kurzbezeichnung für Schnellkommandosystem ist und SKS V/1 für die Chiffriertechnik steht. SKS war auf der taktischen Ebene der Funkaufklärung eingesetzt. Die umfangreichsten öffentlich zugänglichen Informationen findet man auf der Internetseite [32] bzw. auf verlinkten Seiten.

In den 60er Jahren wurde im Rahmen des Warschauer Vertrags ein System für die Fernmeldeaufklärung entwickelt. Die Federführung dabei hatte sicher die Sowjetunion. Im Rahmen einer Arbeitsteilung fiel der DDR und damit dem ZCO die Entwicklung der Chiffrierung zu, natürlich unter Anleitung und Kontrolle durch

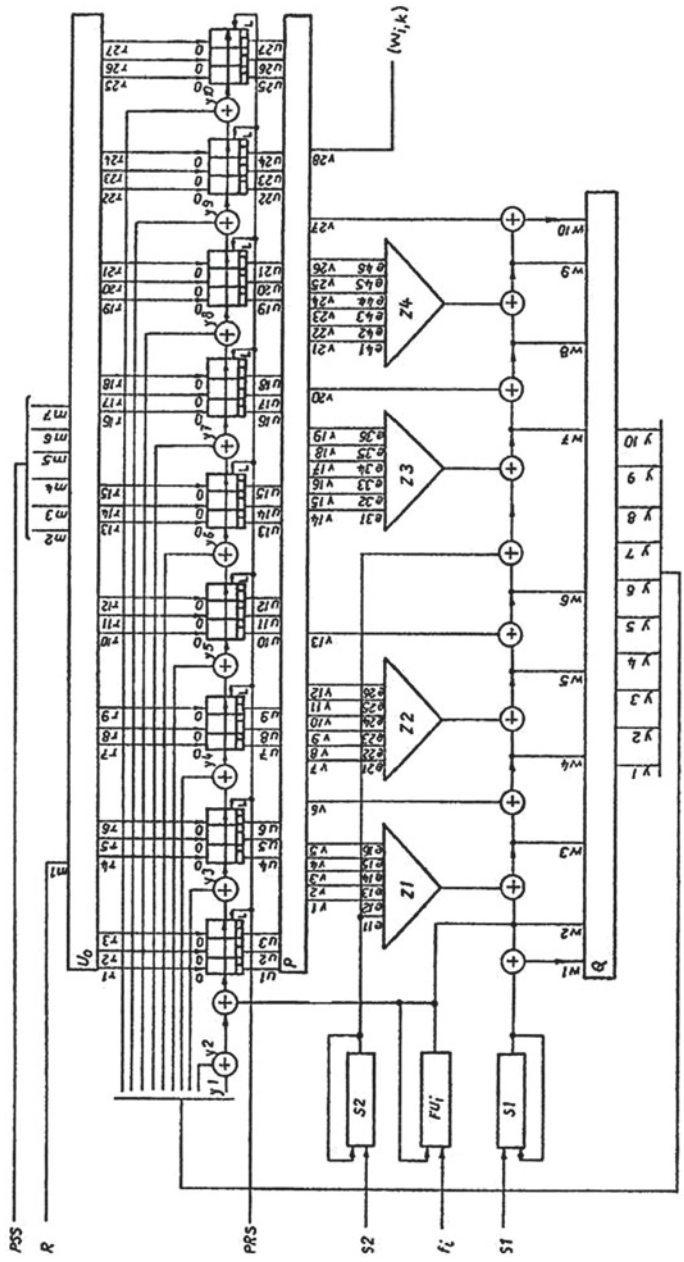


Bild 10: Funktion $\Psi = \Psi_{CH} = \Psi_{PCH}$ zur Erzeugung von wi CH und wi PCH

Abb. 1.2 Grundschema Chiffrieralgorithmus SKS V/1 [32]