CH 629 902 A5

(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
BUNDESAMT FÜR GEISTIGES EIGENTUM

(51) Int. Cl.³: G 07 C 11/00
G 07 D 7/00

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT A5

(11) **629 902**

(21) Gesuchsnummer: 3687/78

(22) Anmeldungsdatum: 06.04.1978

(30) Priorität(en): 20.05.1977 US 799050

(24) Patent erteilt: 14.05.1982

(45) Patentschrift veröffentlicht: 14.05.1982

(73) Inhaber:
International Business Machines Corporation, Armonk/NY (US)

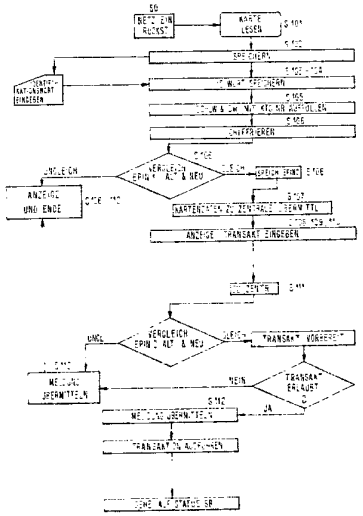
(72) Erfinder:
Donald Cornelius Lancto, Red Hook/NY (US)
Robert Edward Shuck, West Hurley/NY (US)

(74) Vertreter:
Dipl.-Ing. Günter O. Rudack, c/o IBM Corp., Rüschlikon

(54) Verfahren zur Identitätsüberprüfung.

(57) Die Identitätsüberprüfung von Personen, die mittels einer Identifikationskarte Zugriff zu einem Computer verlangen, erfolgt durch Ablesen (S 101) eines Schlüsselwortes und eines ersten Teilkennwortes von der Karte, sowie durch Eingeben eines Personalwortes über eine Tastatur (S 103-104). Aus dem Schlüsselwort und dem Personalwort wird ein Kennwort berechnet (S 106), dessen erster Teil mit dem von der Karte gelesenen Teilkennwort verglichen wird (S 106). Der zweite Teil des Kennwortes wird mit einem im Computer gespeicherten Teilkennwort verglichen (S 111, S 112), und nur wenn beide Vergleiche positiv ausfallen, wird der Zugriff freigegeben.

Das Computerterminal zum Durchführen der Identitätsüberprüfung weist einen Kartenleser auf und Schaltungen zum Verschlüsseln des Personalwortes zwecks Erstellens des Kennwortes, sowie Schaltungen zum Vergleichen der beiden Teile des Kennwortes mit dem von der Karte gelesenen ersten Teilkennwort bzw. mit dem aus einem Speicher im Computer entnommenen zweiten Teilkennwort. Es ist ferner eine Anzeigeeinheit vorgesehen, auf der das Ergebnis der Vergleiche dargestellt wird.



PATENTANSPRÜCHE

1. Verfahren zur Identitätsüberprüfung von Personen, die mittels einer Identifikationskarte über ein Terminal Zugriff zu einem Zentralcomputer verlangen, gekennzeichnet durch folgende Schritte:

– Ablesen eines Schlüsselwortes und eines ersten Teilkennwortes von der Karte;

– Eingeben eines Personalworts, das sich auf den Benützer der Karte bezieht;

– Berechnen eines Kennworts aus dem Schlüsselwort und dem Personalwort;

– Vergleichen des ersten Teils des Kennwortes mit dem von der Karte abgelesenen ersten Teilkennwort, um eine erste Übereinstimmung festzustellen;

– Verweigern des Zugriffs bei Nichtübereinstimmung;

– Vergleichen eines zweiten Teils des Kennworts mit einem zweiten, von einem Zentralcomputer gelieferten Teilkennwort, wenn der erste Vergleich zu Übereinstimmung geführt hat, und Feststellen einer zweiten Übereinstimmung;

– Verweigern des Zugriffs, wenn der zweite Vergleich nicht zu Übereinstimmung führt.

2. Verfahren gemäss Anspruch 1, gekennzeichnet durch Berechnen eines neuen Kennworts aus dem Personalwort und eines neuen Schlüsselworts, wenn der zweite Vergleich zu Übereinstimmung geführt hat, und Einschreiben des neuen Schlüsselwortes und eines ersten Teils des neuen Kennworts in die Karte anstelle des alten Schlüsselworts und des alten Teilkennworts, sowie Speichern des zweiten, neuen Teilkennworts im Zentralcomputer anstelle des alten Teilkennworts.

3. Computerterminal zum Durchführen des Verfahrens gemäss Anspruch 1, wobei die Identifikationskarte von Auge lesbare sowie maschinell lesbare und beschreibbare Informationsfelder aufweist, und wobei ein Teilkennwortfeld zur Registrierung eines Teils einer chiffrierten Information, die sich auf den berechtigten Benützer der Karte bezieht, sowie ein Schlüsselwortfeld zur Registrierung des Codes, unter dem die persönliche Information verschlüsselt ist, vorhanden sind, gekennzeichnet durch Mittel (13) zum Ablesen des Schlüsselwortes sowie des ersten Teilkennwortes von der Karte, durch Mittel (18) zum Verschlüsseln des eingegebenen Personalwortes mit Hilfe des Schlüsselwortes zum Bestimmen des Kennwortes, Mittel (56) zum Vergleichen des ersten Teilkennwortes mit einem ersten Teil des soeben bestimmten Kennwortes, Mittel (26, 27) zum Anzeigen des Resultates des Vergleichs, Mittel (14, 15) zum Übermitteln des zweiten Teils des Kennwortes an einen Zentralcomputer zum Vergleichen mit einem dort gespeicherten Teilkennwort, das sich auf die Identifikationskarte bezieht, sowie Mittel zum Empfangen einer Antwort vom Zentralcomputer und zum Anzeigen des Resultats (26, 27) des Vergleichs des zweiten Teils des Kennwortes mit dem genannten gespeicherten Teilkennwort.

4. Computerterminal gemäss Anspruch 3, gekennzeichnet durch Mittel (29) zum Erzeugen eines neuen Schlüsselwortes, Mittel (25) zum Verschlüsseln des Personalwortes mittels des neuen Schlüsselwortes zu einem neuen Kennwort, Mittel (21) zum Registrieren eines ersten Teils des neuen Kennwortes sowie des neuen Schlüsselwortes auf der Identifikationskarte anstelle des alten Teilkennwortes und des alten Schlüsselwortes, und Mittel (14, 15) zum Übermitteln des zweiten Teils des neuen Kennwortes zum Zentralcomputer zwecks Speicherung anstelle des alten Teilkennwortes.

Für viele Transaktionen ist es erforderlich, die Identität der Benützer von Computerterminals mit hinreichender Zuverlässigkeit zu überprüfen. Die Identifikation von Personen mittels Identitätskarten und Kreditkarten ist seit längerem bekannt. Die Zuverlässigkeit der Überprüfung wird jedoch durch die Möglichkeit des Diebstahls oder des Verlusts der Karte beeinträchtigt. Um die Identität einer Person, die eine solche Karte vorweist, zu überprüfen, wurden schon mancherlei Verfahren vorgeschlagen, wie die Erkennung von Fingerabdrücken, des Stimmspektrogramms, der Unterschrift, von Gesichtsmerkmalen und selbst die Analyse der akustischen Transferfunktion des menschlichen Körpers.

Eine bekannt gewordene Methode erfordert, dass der Benützer einer Identifikationskarte zusätzlich eine Zahl, ein Personalwort, auswendig weiss, das im Terminal algorithmisch mit einem anderen Datenwort, z.B. einer Kontonummer, der Nummer eines Reisepasses etc. in Verbindung gebracht wird, das von einem Magnetstreifen in der Identifikationskarte abgelesen wird. Das Personalwort kann auch irgendwie verschlüsselt im Magnetstreifen auf der Karte registriert sein. Wenn das Terminal einen genügend grossen Speicher aufweist, kann dort eine Tabelle stehen, die das Personalwort mit der von der Karte abgelesenen Zahl one mathematischen Zusammenhang in Verbindung bringt, wodurch es unmöglich wird, das Personalwort aus der Kartenzahl direkt zu bestimmen. Reicht der Speicher des Terminals nicht für alle Kontonummern und zu deren Überprüfung aus und ist das Personalwort nicht in der Karte registriert, so muss die Kontonummer von der Karte und das Personalwort an den Zentralcomputer zur Überprüfung übermittelt werden. Mehrere Verschlüsselungssysteme wurden dazu schon vorgeschlagen, um zu verunmöglichen, dass die Zahlen durch Abhören der Leitungen oder durch unerlaubten Zugriff zum Zentralcomputer von Unberechtigten festgestellt werden können.

Beispielsweise wird ein Geldausgabeterminal logische Schaltkreise oder ein Mikroprogramm enthalten, um folgende Schritte auszuführen:

1. Der Benützer führt seine Kreditkarte mit der magnetisch registrierten Information gemäss z.B. dem American Bankers Association Standard (ABA) in den Terminal ein. Dazu tastet der Benützer das Personalwort und andere Information bezüglich der gewünschten Transaktion, beispielsweise den zur Geldausgabe verlangten Betrag, in die Tastatur.

2. Der Terminal verschlüsselt die Kontonummer mittels eines Verschlüsselungscodes A und eines Algorithmus, beispielsweise des National Bureau of Standards Algorithmus (NBS), worauf das Resultat mit dem Personalwort verglichen wird. Der NBS-Verschlüsselungsalgorhythmus ist auf Seite 95 des USA Federal Registers, Band 40, 149, vom 1. August 1975, publiziert. Geht der Vergleich nicht auf, so wird die Transaktion gesperrt und die Karte entweder dem Benützer zurückgegeben oder im Terminal festgehalten.

3. Wird Übereinstimmung festgestellt, so so wird das Personalwort verschlüsselt. Dazu kann ein Bankcode B oder aber der genannte Code A benützt werden. Das verschlüsselte Identifikationswort wird mit einer von der Zeit abhängigen Information kombiniert, z.B. der Transaktionsnummer oder dem Bargeldinhalt des Terminals, wodurch wiederholte Übertragung der selben Information vermieden wird. Das Resultat wird mittels eines Übermittlungscodes C verschlüsselt und an den Zentralcomputer übermittelt.

4. Im Zentralcomputer wird die übermittelte Meldung gemäss dem Schlüssel C entziffert und das nun noch verschlüsselte Personalwort mit der gespeicherten Datenbasis des Kontos verglichen, das durch die Transaktion betroffen ist. Dabei können Kreditgrenzen und andere dem Konto zugeordnete Informationen überprüft werden.

5. Sind die Überprüfungen in Ordnung und ist der Kontostand ausreichend, so wird eine Antwortmeldung, die ebenfalls eine zeitabhängige Angabe enthält, die die Transaktion erlaubt, zusammen mit zu druckenden oder anzuzeigenden Meldungen verschlüsselt und zum Terminal übermittelt.

6. Im Terminal wird die Meldung entschlüsselt und die zeitabhängige Angabe mit der zeitabhängigen Angabe in der ersten Meldung verglichen, um sicherzustellen, dass die selbe Transaktion betroffen ist. Wird die Meldung in Ordnung befunden, so führt das Terminal die verlangte Transaktion aus, vermittelt beispielsweise dem Kunden eine Meldung und gibt gleichzeitig Bargeld an diesen aus.

7. Das Terminal übermittelt eine weitere Meldung an den Zentralcomputer betreffend die Ausführung oder aber die Löschung der Transaktion sowie allfällig aufgetretene Fehler.

Das soeben beschriebene Ausführungsbeispiel des Standes der Technik benützt zwei Verschlüsselungsebenen sowie zeitabhängige Meldungen, um das Personalwort und die Kontonummer der benützenden Person zu schützen, falls Übermittlungsverbindungen abgehört oder angezapft werden, sowie eine Verschlüsselungsebene, um das Personalwort für jedes Konto im Zentralcomputer zu schützen.

Befindet sich beispielsweise das Geldausgabeterminal in einer fremden Bank und ist das Terminal ein anderes Fabrikat als der Zentralcomputer, so muss die die Karte ausgebende Bank den Verschlüsselungscode C der anderen Bank mitteilen, damit die verschiedenen Computer dieser Banken zusammen die Transaktionen ausführen können. Das Personalwort ist dann nur noch mittels einer Verschlüsselungsebene geschützt und kann während der Übermittlung nicht mehr durch die zeitabhängige Angabe geschützt werden. Im Zentralcomputer kann das Personalwort nach der Entschlüsselung überhaupt nicht geschützt werden, sofern nicht der Bankverschlüsselungscode B der anderen Bank ebenfalls mitgeteilt wird, damit das Personalwort verschlüsselt werden kann. Zusätzlich wird die Geheimhaltung bei der Bank des Zentralcomputers gefährdet, wenn der Bankcode B nicht mehr geheim ist, da mit seiner Hilfe und mittels einer Anzapfung der Übertragungsverbindung der Inhalt der Datenbasis rekonstruiert werden kann.

Im Stand der Technik ist stets die Relation zwischen Kontonummer und Personalwort entweder auf der Karte oder im Computer gespeichert. Die USA-Patente 3 662 342 und 3 665 162 betreffen einen wechselnden Schlüssel und verwürfelte oder chiffrierte Information auf der Karte zum Vergleich mit dem Personalwort und erfordern beide, dass alle für diesen Vergleich notwendige Information auf der Karte registriert ist, wo sie verletzlich ist.

Das USA-Patent 3 697 729 zeigt die Benützung zufällig angeordneter Punkte ebenfalls auf der Karte.

Die USA-Patente 3 543 904 und 3 401 830 sowie andere Patente zeigen verschiedene Chiffriersysteme, um die Beziehung zwischen Kontonummer und Personalwort im Zentralcomputer zu verbergen. Gemäss dem USA-Patent 3 648 020 wird das Personalwort an den Zentralcomputer zum Vergleich übermittelt.

Das vorliegende Verfahren zur Identitätsüberprüfung von Personen, die mittels einer Identifikationskarte über ein Terminal Zugriff zu einem Zentralcomputer verlangen, ist gekennzeichnet durch folgende Schritte: Ablesen eines Schlüsselwortes und eines ersten Teilkennwortes von der Karte; Eingeben eines Personalworts, das sich auf den Benützer der Karte bezieht; Berechnen eines Kennworts aus dem Schlüsselwort und dem Personalwort; Vergleichen des ersten Teils des Kennwortes mit dem von der Karte abgelesenen ersten Teilkennwort, um eine erste Übereinstimmung festzustellen; Verweigern des Zugriffs bei Nichtübereinstimmung; Vergleichen eines zweiten Teils des Kennworts mit einem zweiten, von einem Zentralcomputer gelieferten Teilkennwort, wenn der erste Vergleich zu Übereinstimmung geführt hat, und Feststellen einer zweiten Übereinstimmung; Verweigern des Zugriffs, wenn der zweite Vergleich nicht zu Übereinstimmung führt.

Die Erfindung betrifft ferner ein Computerterminal zum Durchführen des genannten Verfahrens nach dem Patentanspruch 3.

Ausführungsbeispiele der Erfindung werden hiernach anhand der Zeichnungen im Einzelnen erläutert. Die Zeichnungen zeigen:

Fig. 1 ein Blockschaltbild eines Systems mit Terminals;
Fig. 2 Blockschaltbild eines einzelnen Terminals;
Fig. 3 die logische Steuerung eines Terminals in Blöcken;
Fig. 4 ein Flussdiagramm, dass die Herstellung einer Identifikationskarte zeigt;
Fig. 5 ein Flussdiagramm, das die Benützung einer Identifikationskarte zur Überprüfung der Personenidentität zeigt;
Fig. 6 eine Tabelle mit einer Signalfolge;
Fig. 7 eine Adressbit-Tabelle;
Fig. 8 Darstellung eines Speicherinhaltes;
Fig. 9 Darstellung eines anderen Speicherinhaltes;
Fig. 10/11/12 Zeitdiagramme;
Fig. 13/14/15 logische Steuerschaltungen.

Fig. 1 zeigt schematisch eine Anlage mit Terminals, die mit Identifikationskarten 1 arbeitet, auf denen nur ein Teil der Relation zwischen einer persönlichen Kontonummer und einem Identifikationswort registriert ist. Das Terminal 2 ist vorgesehen zur Benützung durch einen Beamten der die Karten ausgebenden Institution. An ihm wird zuerst die Relation zwischen einer Kontonummer und dem Identifikationswort festgelegt. Ein Teil dieser Relation wird als Teilkennwort in der Karte 1 als EPIN1 und ein anderer Teil als zweites Teilkennwort im Zentralcomputer 3 als EPIN2 registriert. EPIN1 und EPIN2 beziehen sich natürlich auf den ersten resp. zweiten Teil des verschlüsselten Identifikationswortes. Das Terminal 2 und die Abfrageterminals 4 sind gemeinsam über Fernmeldeverbindungen an den Computer 3 angeschlossen.

Die Identifikationskarte 1 hat im vorliegenden Ausführungsbeispiel drei magnetische Registrierstreifen. Die ersten beiden Streifen 5, 6, entsprechen beispielsweise den Normen der International Airline Transport Association (IATA) und der American Bankers Association (ABA). Die dritte Registrierspur 7 ist eine Schreib- und Lesespur, die vom Terminal 2 beschrieben worden ist und von den Terminals 4 bei jeder Transaktion gelesen und verändert wird. In der Spur 7 wurde vom Terminal z.B. eine Kontonummer und Information betreffend die Deckung und die Benützung der Karte registriert. Solche Angaben sind nützlich bei begrenzten Transaktionen, die ohne Zugriff zum Datenspeicher im zentralen Computer durchgeführt werden können. Diese Transaktionen werden im örtlichen Platten- oder Bandspeicher 8 festgehalten. Zusätzlich enthält die dritte Spur 7 noch ein Feld zur Registrierung des schon genannten Teilkennwortes EPIN1 sowie ein Feld RKEY, das ein Schlüsselwort aufnimmt. Das Schlüsselwort ist eine auswechselbare, beliebige Nummer, die der Chiffrieralgorithmus der Terminals 2 und 4 benützt, um das Identifikationswort zu verschlüsseln. Es ist zu bemerken, dass der von den Terminals benutzte Algorithmus ein irreversibler Algorithmus sein kann, in dem Sinn, dass bei normalem Terminalbetrieb nur die Verschlüsselung notwendig ist. Es kommt nie vor, dass EPIN1 und EPIN2 am Terminal entschlüsselt werden müssen. Theoretisch macht es ein irreversibler Algorithmus unmöglich, das Identifikationswort herauszufinden, selbst wenn die Kontonummer, das Schlüsselwort und das vollständige, verschlüsselte Personalwort bekannt sind. Trotzdem ist im Vorliegenden dafür gesorgt, dass stets nur ein Teil des verschlüsselten Identifikationswortes an jeder beliebigen Stelle des Systems herausgefunden werden kann, weshalb eine hohe Sicherheit selbst dann besteht, wenn der Algorithmus nicht vollständig irreversibel ist.

Fig. 2 zeigt ein Blockdiagramm der internen Logik der Terminals 2 und 4. Jedes Terminal enthält eine Tastatur 12, einen Magnetstreifenleser/schreiber 13, einen Übermittlungsmodem 14 und die zugehörige Übermittlungslogik 15. Der Übergang

zwischen Modem 14 und Logik 15 entspricht vorzugsweise der Norm RS232. Zusätzlich kann jedes Terminal einen Platten- oder Bandspeicher 8 aufweisen, der über die Speicherlogik 16 angeschlossen wird. Im Speicher werden kleinere Transaktionen aufgezeichnet, die ausgeführt werden können, ohne dass das Terminal mit dem Zentralcomputer in Verbindung steht. Ausserdem kann das Terminal einen Drucker 17 aufweisen zur Übermittlung von Meldungen, Bestätigung der Transaktionen, Ausstellung von Quittungen etc. Schliesslich enthält das Terminal eine Verschlüsselungseinheit 18 zur Umwandlung des Identifikationsworts in die Halbkennworte EPIN1 und EPIN2.

Zwischen den zuvor genannten Einheiten innerhalb des Terminals ist vom Speicher 19 eine Speichereingangshauptleitung (SEH) und eine Speicherausgangsleitung (SAH) vorgesehen. Damit die genannten Einheiten mit dem Speicher richtig zusammenarbeiten können, ist eine Steuerlogik 20 vorgesehen. Die Steuerlogik 20 ist eine relativ einfache Einheit und vollständig in Hardware ausgebildet. Dadurch soll erreicht werden, dass der Zugang zur Arbeitsweise und deren Änderung erschwert und die Gefahr des Missbrauchs des Terminals vermindert wird. Es ist aber zu bemerken, dass, wenn die Sicherheit des Terminals gewährleistet werden kann, so dass seine Arbeitsweise nicht böswillig änderbar ist, das Terminal unter der Steuerung eines Mikroprozessors, beispielsweise des Typs ITEL 8080, geschehen kann, der entsprechend programmiert ist. Wenn die Steuerlogik 20 die Form eines Mikroprozessors hat, dann kann die Verschlüsselung durch eine Programmsubroutine desselben Mikroprozessors ausgeführt werden.

Fig. 3 zeigt ein detaillierteres Blockdiagramm der logischen Einheit innerhalb der Steuerlogik 20 sowie der Eingangs- und Ausgangsleitung zu der Übermittlungslogik 15, der Bandspeicherlogik 16 und der Steifenleserlogik 21. Wesentlichster Teil der Steuerlogik 20 ist der Sequenzzähler 22. Das Bitmuster des Sequenzzählers 22 gibt zu jeder Zeit den Arbeitszustand des Terminals an. Der Ausgang des Sequenzzählers 22 gelangt auf die Sequenzhauptleitung zur Verteilung an die verschiedenen Einheiten. Wie aus Fig. 6 zu sehen ist, ist der Ausgang des Sequenzzählers 22 in drei Felder unterteilt.

Das erste, das Sequenzmodusfeld, steuert den Arbeitsmodus des Terminals . Das Terminal kann z.B. in Testmodus betrieben werden zur Fehlerfeststellung oder zur präventiven Diagnostik. Das Terminal kann auch im Ausgabemodus arbeiten, den ein Mitarbeiter einer Karten ausgebenden Institution benützt, um an eine Person eine Identifikationskarte abzugeben. Wenn ein Benützer unter Vorweisung seiner Identifikationskarte das Terminal benützen möchte, so arbeitet dieses im Benützungsmodus. Dass andere Moden auch möglich sind, ist in Fig. 6 in der mit «Verschiedenes» bezeichneten Zeile angedeutet.

Die Sequenz der vom arbeitenden Terminal ausgeführten Schritte in jedem der im ersten Feld angegebenen Moden wird gesteuert durch die Zählung im zweiten Feld. Diese einfache Binärzählung, die vom Eingangssignal INC jeweils erhöht wird, kann auf jede beliebige Binärzahl gesetzt werden. Die Möglichkeit, den Sequenzzähler zu setzen, bedeutet, dass die Arbeitsschritte des Terminals vorwärts und rückwärts springen können, womit unerwarteten Bedingungen, wie einem falschen Eingang u.ä. Rechnung getragen werden kann.

Das dritte Feld der Sequenzhauptleitung enthält Sequenzmodifizierleitungen, die den Sequenzstatus, wie er durch den Modus und das Zählfeld angegeben ist, modifizieren, um besondere Bedingungen anzugeben, wie z.B. einen Feldüberlauf, einen unzulässigen Zustand, ein ungültiges Identifikationswort, eine nichtzulässige Kreditanforderung etc. Die Sequenzmodifikatoren werden vor allem von einer Eingangs/Ausgangslogik, z.B. der Tastatursteuerlogik 24 oder der Übermittlungslogik 15 benützt, die die von der Tastatur oder vom Zentralcomputer kommende Information überwacht und bestimmte Bytes derselben erkennt, um den Sequenzzustand des Terminals zu modifizieren. Wird z.B. im Überlaufzustand ein alphanumerisches Zeichen anstelle eines Feldtrennzeichens entdeckt, so setzt die Tastaturlogik 24 über die SETS-Leitungen den Überlauf-Sequenzmodifizierer im Sequenzzähler 22. Auch wenn ein Nachrichtenbyte vom Zentralcomputer nach einer vorbestimmten Zeitperiode nicht eintrifft, setzt ein Zähler durch ein Signal über die SETS-Leitungen den Haltekreis im Sequenzzähler.

Der Adressenzähler 23 steuert die Adresse des Speichers 19 auf ähnliche Weise wie der Sequenzzähler 22 den Arbeitsstatus des Terminals steuert. Der Adressenzähler steuert dadurch den Informationsfluss innerhalb des Terminals. Das Adressbitmuster am Ausgang des Adressenzählers 23 ist in Fig. 7 dargestellt. Ein Eingang des Adressenzählers ist eine Inkrementierleitung, die die Adressen der Reihe nach aufsucht, und eine Eingangshauptleitung SETA, die den Adressenzähler auf jeden beliebigen Wert einstellen kann, wodurch Sprünge oder Verzweigungen vorgenommen werden können.

Wie aus dem in Fig. 9 dargestellten Beispiel des Sequenzstatus S12 ersichtlich ist, ist der Speicher 19 in verschiedene Pufferzonen unterteilt, um die Sicherheit innerhalb des Terminals zu verbessern. Beispielsweise enthält die Zone für Mitteilungen des Zentralrechners die Speicherstellen A0 bis A128. Dementsprechend muss, wie Fig. 7 zeigt, das höchste Bit des Adressbitmusters Null sein, wenn Information durch Übermittlungskanäle von oder zu dem Hauptpuffer innerhalb des Speichers 19 eines Terminals übermittelt wird. Auf ähnliche Weise umfasst der Pufferteil mit den Daten zur Identifikation der Karte die Adresstellen A128 bis A159. Das Adressbitmuster muss also gemäss Fig. 7 eine Eins in der höchsten Stelle aufweisen und Null in den Bitstellen 4 bis 64, damit Kartendaten behandelt werden. Noch wesentlicher zur Sicherheit des Terminals ist der Umstand, dass die einzigen Operationen, die an den Adressstellen A232 bis 255 vorgenommen werden können, Tastaturoperationen oder Verschlüsselungs/Entschlüsselungsoperationen sind. Die Tastaturoperationen werden von der Tastatursteuerlogik 24 gesteuert und liefern Information, wie das Identifikationswort oder den Übermittlungschifferierschlüssel C. Die Chiffrieroperationen werden durch die Chiffrierlogik 25 gesteuert. Keine andere logische Steuerung darf arbeiten, wenn der Adresszähler eines der in Fig. 7 gezeigten, hohen Bitmuster für das ID-Datenwort oder eines der beiden Schlüsselwörter KW enthält.

Der Ausgang des Sequenzzählers 22 in Fig. 3 wird von der Anzeigelogik 26 decodiert, die eine der vorgegebenen Meldungen 27 dem Benützer des Terminals anzeigt, damit dieser weitere Information eingeben kann oder über den Status des Terminals oder die Transaktion Bescheid weiss. Die Anzeigelogik 26 ist eine einfache, decodierende Schaltung, die aus UND- und ODER-Kreisen besteht, um ein oder mehrere Ausgangssignale zu erzeugen, je gemäss dem eingehenden Bitmuster.

Die Tastaturlogik 24 weist einen Eingang KATTN auf, über den ein Warnsignal übertragen wird, wenn ein Informationsbyte am Ausgang der Tastatur im Puffer bereitsteht. Die Tastaturlogik ist mit der Sequenzhauptleitung und der Adresshauptleitung verbunden, damit die Logik feststellen kann, ob das Terminal in einem Status ist, in dem es Information von der Tastatur über die Speichereingangshauptleitung SEH empfangen kann. Wenn der Sequenzzustand des Terminals und die Speicheradresse, unter der die Tastaturinformation gespeichert wird, mit den vorbestimmten Arbeitsbedingungen für das Terminal übereinstimmen, erfolgt ein Antwortsignal KGATE an die Tastatur, das die Übermittlung der Information über die Speichereingangshauptleitung in den Speicher veranlasst. Die Tastaturlogik 24 ist mit SEH verbunden und kann daher die empfangene Information überwachen und den Sequenzzustand des Terminals über die SETS-Leitung und den Sequenzzähler 22 beeinflussen. Die SETS-Leitung wird beispielsweise benützt, wenn eine Ausgabefunktionstaste betätigt wurde. In diesem Fall wird der Sequenz-

zustand der Maschine auf den Ausgabemodus geändert. Ähnlicherweise ist die Tastaturlogik und der Adresszähler über die Leitungen SETA verbunden, damit der Adresszähler auf vorgegebene Werte eingestellt werden kann, um Information von der Tastatur in den zuständigen Speicherpuffer zu verschieben. Die SETA-Signale werden von Gates erzeugt, wie sie in Fig. 15 dargestellt sind. Diese Gates sind im Stande der Technik bekannt. Während der üblichen sequentiellen Arbeitsweise wird der Adresszähler durch Signale auf der Leitung INCRA und der Sequenzzähler durch Signale auf der Leitung INCRS fortgeschaltet. Die Tastaturlogik umfasst auch ein Datenübertragungsregister, ähnlich dem in Fig. 14 dargestellten.

Die anderen Einheiten, die Druckerlogik 28, die Magnetstreifenleserlogik 21, die Übermittlungslogik 15 und die Verschlüsselungs- oder Chiffrierlogik 25 haben ähnliche Ein- und Ausgangsleitungen. Alle diese Einheiten müssen sich nach dem Sequenzzustand und den Speicheradressbedingungen des Terminals richten, um richtig arbeiten zu können, und müssen die Speicheradresse des Terminals fortschalten oder ändern, je nach dem die Arbeitsweise der betreffenden logischen Einheit fortschreitet oder vollendet ist. An einem Beispiel sollen die Schaltkreise und Signalleitungen in Bezug auf die Übermittlungslogik 15 anhand der Fig. 13 beschrieben werden.

Anhand der Fig. 13 wird als Beispiel die Detailschaltung der Übermittlungslogik 15 beschrieben. Die Übermittlungslogik, die den Modem steuert, arbeitet in Übereinstimmung mit der RS232-Norm. Wichtigster Teil der Übermittlungslogik 15 ist das Sendeschieberegister 30 sowie das Empfangsschieberegister 31. Vom Modem 14 empfangene Daten RDATA gelangen auf die UND-Schaltung 32 und von dort seriell in das Schieberegister 31. Dies geschieht im Takt der UND-Schaltung 33, die jedesmal einen Puls abgibt, wenn das Empfangssignal RLS mit dem Taktsignal RTAKT zusammentrifft. Die UND-Schaltung 33 schaltet ausserdem den RTAKT-Zähler 34 fort, der ein 8Bit-Empfangssignal abgibt, jedesmal wenn acht Bits empfangen und in das Schieberegister 31 eingeschoben worden sind. Das «8 BIT E»-Signal gelangt vom Schieberegister 31 erstens über die UND-Schaltung 35 zur Speicherhauptleitung, zweitens zur Steuerbytelogik 36 und drittens zur Vergleichsschaltung 37. Die ODER-Schaltungen 38 und 39 bereiten die UND-Schaltung 35 vor, den Inhalt des Schieberegisters 31 auf die Speicherhauptleitung zu geben, jedesmal wenn ein Datenwort oder ein «Ende der Meldung»-Wort in den Sequenzzuständen S6 oder S112 festgestellt wurde, d.h. wenn Meldungen vom Zentralcomputer zu erwarten sind. Die Vergleichsschaltung 37 vergleicht den Inhalt des Empfangsschieberegisters 31 mit der Adresshauptleitung, wenn die Steuerbytelogik 36 anzeigt, dass das Byte im Schieberegister 31 ein Adressbyte ist. Die Vergleichsschaltung 37 gibt ein Signal «AD=» ab, um anzuzeigen, dass die Zahl der Bytes, die der Zentralrechner abgesandt hat, mit der Zahl der empfangenen Bytes übereinstimmt, oder «AD $\neq$», wenn der Vergleich nicht aufgeht. Ausserdem gibt die Steuerbytelogik Signale auf verschiedene Leitungen, wie POLL, ACKR, EOTR usw. ab, die verschiedentlich verwendet werden können. Beispielsweise wird jedes Byte, das nicht ein Steuerbyte, z.B. ein «Ende der Meldung»-Byte oder ein Quittungsbyte ist, als Datenbyte mit einem DATAR-Signal versehen, sofern nicht ein Steuerbyte EOM folgt, in welchem Fall das Byte als Längenzählung angesehen wird, die auch über die ADDRR-Leitung abgegeben wird.

Ähnlich wie die Empfangslogik arbeitet auch die Sendelogik, welche Daten aus dem Schieberegister 30 unter der Steuerung der UND-Schaltung 40 verschiebt. Die UND-Schaltung 40 gibt ein Ausgangssignal ab, wenn ein Sendesignal CTS und ein STACKT-Signal gleichzeitig vom Modem empfangen werden. Der STAKT-Zähler 41 zählt die Bits, die aus dem Sendeschieberegister 30 geschoben und über die S-Datenleitung zum Modem 14 übertragen werden. Wurden acht Bits übertragen, so gelangt ein Signal «8 BIT S» an die Steuerschaltung 47, wodurch veranlasst wird, dass das Schieberegister 30 neu geladen wird. Während das Register 30 geladen wird, überwacht die Steuerbytesendenlogik 43 das Bitmuster und setzt einen Haltekreis, der das soeben zu sendende Byte kennzeichnet, damit eine fortlaufende Übertragung von Bytes sichergestellt wird. Wird beispielweise von der Steuerbyteempfangslogik 36 ein Abrufbyte festgestellt, so lädt die UND-Schaltung 44 das Sendeschieberegister 30 mit dem NACK-Byte, sofern der Terminal nicht in den Sequenzzuständen S5, S6, S13, S14, S111 oder S112 ist. Andererseits lädt die UND-Schaltung 45 das Sendeschieberegister 30 mit dem ACK-Byte, wenn das Terminal im Sequenzstatus S5, S6, S13, S14, S111 oder S112 ist. Die Sequenzstatus werden von den Decodern 51 und 52 festgestellt und den UND-Schaltungen 44 und 45 zugeführt. Wenn das Sendeschieberegister 30 mit einem NACK- oder einem ACK-Byte geladen ist, das gesendet wird, erzeugt die Steuerbytesendenlogik 43 das entpsrechend gekennzeichnete Ausgangssignal. Das Ausgangssignal veranlasst über die ODER-Schaltung 46 die Steuerschaltung 47, das «Ende Übertragungs»-Byte zu erzeugen und ihm entsprechend das ACKS, NACKS oder ADDRS-Byte.

Die Übermittlungslogik 15 stellt mittels des Zählers 48 fest, ob das Terminal mit der Zentrale in Verbindung steht. Wenn der Zähler 48 ein Übertragssignal erzeugt, wird angenommen, dass die Verbindung besteht und wenn das höchste Bit eine binäre Null ist, wird angenommen, dass die Verbindung unterbrochen ist. Wenn das Terminal nicht Information im Band- oder Plattenspeicher 8 registriert, entsteht ein Ausgangssignal der UND-Schaltung 49 jedesmal, wenn acht Bits empfangen wurden, wodurch der Zähler 48 fortgeschaltet wird. Wenn das Terminal Information im Bandspeicher 8 registriert, entsteht ein $\overline{\text{CTL}}$-Signal, das die UND-Schaltung 49 blockiert. Der Zähler 48 wird durch eine Zeitschaltung mit so geringer Frequenz periodisch zurückgeschaltet, dass unter normalen Arbeitsbedingungen während einer Verbindung mindestens ein Abrufbyte oder Informationsbyte vom Zentralcomputer übertragen wird, bevor das nächste Rückschaltsignal erwartet wird. Der Zähler 48 wird also im Betrieb geringfügig vorwärts oder rückwärts geschaltet, steht jedoch meistens bei seiner höchsten Zahl, da er nicht wieder von Null anfängt zu zählen. Wenn das «8 BIT EMPFANGEN»-Signal für eine genügend lange Zeit nicht auftritt und sich der Zählerstand unter den halben gespeicherten Wert erniedrigt, verschwindet sein höchstes Bit. In diesem Zustand müssen mehrere Abfragesignale empfangen werden, bevor der Zähler 48 so weit fortgeschaltet ist, dass ein Übertragsbit entsteht. Auf diese Art wird vermieden, dass das Terminal allzu oft die Verbindung herzustellen sucht.

Das Sendesignal für den Modem 14 kommt von der ODER-Schaltung 50 auf ein empfangenes Abrufbyte oder ein anderes der dort empfangenen Steuerbytes.

Die Steuerkreise 21, 16, 24, 25 und 28 sind dem Kreis 15 ähnlich. Insbesondere die Kreise 21, 16 und 28 haben Ausgangsleitungen, deren Funktion der der Ausgangsleitung des Kreises 15 analog ist. Zudem ist die Magnetbandspeicherlogik 16 der Übermittlungslogik 15 sehr ähnlich. Einer der beiden arbeitet immer dann, wenn das Terminal Verbindung mit dem Hauptcomputer hat und die andere immer, wenn es diese Verbindung nicht hat. Es ist daher klar, dass manche Kreise mehrere der in Fig. 2 und 3 gezeigten Funktionen ausführen können, wodurch Ersparnisse entstehen. Praktisch wird der ganze Ausgang der Logik 15 sowohl dem Modem 14 als auch der Bandlogik 16 zugeführt, so dass das Magnetband beschrieben wird, wenn das Terminal keine Verbindung hat und gesendet wird, wenn die Verbindung mit dem Zentralrechner besteht.

Die Chiffrierlogik 25, die in Fig. 14 im Detail dargestellt ist, arbeitet ähnlich, wie es in Bezug auf die Übermittlungslogik 15 beschrieben wurde. Die Daten zirkulieren hier zwischen Spei-

cherstellen, wobei das Datenwort IDDW und das Schlüsselwort IDKB benützt wird, und diese Wörter mit der Verschlüsselungseinheit 18 ausgetauscht werden, Byte pro Byte, wie im Zeitdiagramm der Fig. 10, 11 und 12 dargestellt. Ein wesentlicher Unterschied zwischen der Logik 25 und der Logik 15 besteht darin, dass die letztere vom Zykluszähler 53, Fig. 14, synchronisiert ist. Die Übermittlungslogik 15 andererseits muss wegen den auf den Übermittlungskanälen herrschenden Bedingungen sowie der auftretenden Steuerinformation innerhalb der zu übertragenden Daten asynchron arbeiten.

Der Zykluszähler 53 in Fig. 14 wird beim Beginn eines jeden Zyklus durch die erste Phase eines vierphasigen Taktsignals fortgeschaltet, wie in Fig. 5 des USA-Patents 3 958 081 beschrieben ist. Die UND-Schaltung 54 lässt die Fortschaltung des Zykluszählers 53 nur während der Sequenzstaten S8, S10, S11, S102, S105, S106 und S107 zu, wenn gemäss dem Status des Terminals eine Datenübertragung zwischen verschiedenen Speicherstellen oder eine Datenchiffrierung erforderlich ist. Der Zyklussteuerdecoder 55 stellt die Sequenzstaten auf der Sequenzhauptleitung sowie die Zählung des Zykluszählers 53 fest und erzeugt Steuersignale für den Zykluszähler, die Vergleichslogik 56, das Datenübertragungsregister 57, die Verschlüsselungslogik 18, den Zufallsgenerator 29 usw. Das Datenübertragsregister 57 sorgt für die Bewegung der Daten zwischen verschiedenen Teilen des Speichers 19. Die Daten werden von der Speicherausgangsleitung über die UND-Schaltung 58 ins Register 57 geladen und verlassen das Register über die UND-Schaltung 59 auf der Speichereingangshauptleitung.

Fig. 15 zeigt Schaltkreise, die die Funktionen des Zyklussteuerdecoders 55 ausführen können. Ein erster Block von UND-Schaltungen 60 decodiert die einzelnen Sequenzstände auf der Sequenzhauptleitung zu Signalen auf einzelnen Leitungen S8, S10 usw. Ein weiterer Satz von UND-Schaltungen 61 decodiert den Ausgangszyklus des Zählers 53 in Signale auf einzelnen Leitungen. Das Ausgangssignal der Schaltungen 60 und 61 steuert andere Schaltungen 62, 63 und 64, welche Signale erzeugen, die anzusteuernde Speicheradressestellen angeben und die für weitere Schaltungen, wie 66 bis 72, als Eingang dienen. Wie Fig. 15 zeigt, sind die Ausgänge der Schaltungen 62 mit Adressen bezeichnet, die während des Sequenzzustandes S10 erzeugt werden. Die Adressen werden von den ODER-Schaltungen 65 erzeugt, deren Ausgangssignal der SETA-Hauptleitung zugeführt wird, um den Adresszähler 23 auf die Speicherstelle einzustellen, zu welcher Zugriff gewünscht wird. Die ODER-Schaltung 72 steuert die Pulsbreite der Ausgangssignale der Schaltungen 66 bis 70, so dass Information in den Speicher und in die Verschlüsselungsschaltung 18 synchron mit der Arbeit dieser Schaltungen eingeschrieben oder ausgelesen wird. Nur ein Teil der Schaltungen 65 bis 71 sind in Fig. 15 dargestellt, um zu zeigen, dass zusätzlich zu den im Beispiel erläuterten Bedingungen noch andere existieren. Die Schaltungen 72 beispielsweise, stellen den Zykluszähler 53 am Ende der auszuführenden Sequenz wieder zurück. Beispielsweise ist aus Fig. 11 zu sehen, dass der Sequenzzustand die dreizehn Zyklen von 0 bis 12 umfasst. Während des Zyklus 12 erzeugt die Schaltung 68 das mit RÜCKSTC bezeichnete Ausgangssignal, das den Zykluszähler 53 auf Null stellt. Dasselbe Ausgangssignal der UND-Schaltung 68 gelangt auch zum INCS-Eingang des Sequenzzählers 22, um denselben vom Sequenzzustand 10 auf Sequenzzustand 11 fortzuschalten.

Für die Verschlüsselung des Personalwortes, das in der vorliegenden Ausüfhrung ein im Gedächtnis behaltenes Identifikationswort ist, kann die Verschlüsselungsschaltung 18 natürlich auch gemäss dem USA-Patent 3 958 081 arbeiten. Die Chiffrierlogik 25 kann so aufgebaut sein, dass zeitabhängige Information mit den Daten der Mitteilung im Zentralspeicher vor der Verschlüsselung und Übertragung verkettet wird. Diese zusätzlichen Sicherheitsmassnahmen sind bekannt und werden deshalb nicht weiter beschrieben.

Nachfolgend wird der Betrieb des Terminals im einzelnen beschrieben. Fig. 4 zeigt die Arbeitsweise bei der Kartenausgabe. Wenn die Natzstromversorgung eingeschaltet wird, sorgt eine bekannte Rückstellschaltung dafür, dass alle Zähler und Haltekreise auf Null zurückgestellt werden, wodurch das Terminal in den Sequenzstatus S0 gerät.

Um das Terminal in den Ausgabemodus zu bringen, wird eine entsprechende Taste gedrückt. Die Taste erzeugt ein KATTN-Signal für die Tastatursteuerlogik 24. Wenn der Speicher nicht gerade für andere Zwecke benützt wird, d.h. wenn der Sequenzzähler einen der Status S0 bis S4 zeigt, sendet die Tastatursteuerlogik 24 ein Signal KGATE an die Tastatur, das diese veranlasst, ein Informationsbyte auf die Speichereingangshauptleitung SEH abzugeben. Das Byte IM gelangt zum Speicher und wird an der ersten Adressstelle A0 gespeichert. Das Byte gelangt auch an die Tastatursteuerlogik 24. Wenn die Logik 24 das Byte als Ausgabemodus Schlüssel decodiert, wird ein entsprechender Haltekreis im Sequenzzähler 22 gesetzt. Der Sequenzzähler wird gleichzeitig durch ein Signal auf der Leitung SECS auf den Status S1 fortgeschaltet. Die Anzeigelogik 26 veranlasst nun «Namenseingabe» auf dem Meldungstableau 27 anzuzeigen.

Der Benützer beginnt nun, den Namen des Kunden in die Tastatur einzugeben. Jedes eingegebene, alphabetische Zeichen erzeugt das Tastatursignal KATTN an die Tastatursteuerlogik 24, die wiederum ein Abfragesignal KGATE erzeugt, weil das Terminal im Stauts S1 ist. Jedes Zeichen, das die Tastatursteuerlogik 24 als alphabetisches Zeichen erkennt, wird in der zuletzt adressierten Speicherstelle gespeichert, und der Adresszähler 23 wird fortgeschaltet. Wenn der Terminalstatus S1 ist und der Adresszähler A27 erreicht hat, wird von der Tastatur ein Feldtrennzeichen erwartet. Wenn die Logik 24 das 28. Zeichen nicht als Feldtrennzeichen erkennt, setzt der Sequenzzähler 22 ein Neueingabesignal, der Adresszähler 23 wird an den Anfang des Feldes, d.h. an die Adresse A1 zurückgestellt. Das «Feld überfliesst – Neueingabe»-Signal am Meldungstableau wird von der Anzeigelogik 26 eingeschaltet. Wenn die Tastatursteuerlogik 24 das Zeichen in der Speichereingangshauptleitung als Feldtrennzeichen erkennt, wird der Sequenzzähler 22 auf S2 und der Adresszähler 23 auf A28 fortgeschaltet. Wenn der Seqeunzzähler im Status S2 ist, veranlasst die Anzeigelogik 26 das Signal «Betrag pro Ausgabe» zu erscheinen, das den Benützer veranlasst, den Grenzbetrag anzugeben, den er selbst oder die ausgebende Institution für seine Transaktionen festzulegen wünscht. Die Eingabe dieses numerischen Betrages veranlasst ein KATTN-Signal für jede Tastenbetätigung, wodurch ein KGATE-Signal entsteht, das jedes Byte auf die Speichereingangshauptleitung weiterleitet zur Speicherung in aufeinanderfolgenden Adressstellen gemäss der Fortschaltung des Adresszählers 23. Wenn die Tastatursteuerlogik 24 ein Eingangszeichen als Nichtfeldtrennungs-Zeichen erkennt und wenn der Adresszähler die Position A31 erreicht hat, setzt der Feldzähler 22 einen Haltekreis, wodurch die Anzeige «Überlauf – Wiedereingabe» verursacht wird und der Adresszähler auf Position A28 zurückgestellt wird. Die Tastatursteuerlogik 24 schaltet den Adresszähler jedesmal weiter, solange ein Eingangszeichen von der Tastatur als numerisches Zeichen erkannt wird und der Sequenzzähler den Status S2 anzeigt. Wenn die Logik 24 während des Status S2 ein Feldtrenn-Zeichen erkennt, wird der Sequenzzähler auf S3 und der Adresszähler auf A32 weitergeschaltet. Das Ablaufdatum der Kreditkarte wird ebenfalls gespeichert, und zwar der Tag in Adresspositionen 32 und 33, der Monat in Positionen 35 und 36 und das Jahr in Positionen 37 und 38. Wenn das Terminal im Sequenzstatus S4 ist und ein «Ende Meldungs»-Byte von der Tastaturlogik festgestellt wird, wird der Sequenzzähler auf S5 fortgeschaltet und der Adress-

zähler auf A0 zurückgestellt. Wenn der Sequenzzähler auf S5 steht, zeigt die Anzeigelogik 26 «Verarbeiten» an.

Während der Sequenz S5 werden die in den Sequenzen S0 bis S4 eingegebenen Daten an den Zentralcomputer übertragen. Die Übertragung wird durch die Übertragungssteuerlogik 15 veranlasst, die mit dem Modulator/Demodulator 14 zusammenarbeitet, der beispielsweise der Standardschnittstelle RS232C entspricht. Es wird im vorliegenden Beispiel angenommen, dass der Zentralcomputer periodisch über die Übermittlungskanäle alle Terminals abfragt, d.h. wiederholt an jedes Terminal eine Abfrageadresse sendet. Die Übertragungssteuerlogik in jedem Terminal antwortet auf das Abfragesignal normalerweise mit dem «Nicht Annahme»-Signal NACK und dem «Ende Übertragung»-Signal EOT, wenn die Logik die Adresse als die ihres Terminals erkennt, wenn aber das Terminal keine Information zur Übermittlung bereit hat, d.h. sich nicht im Stauts S5 befindet. Wenn andererseits das Terminal Information zur Übermittlung bereit hat, erzeugt die Logik das Annahme-Byte ACK, dem dann die Information folgt, ein die Länge definierendes Signal sowie das «Ende Übermittlungs»-Byte EOT. Da der Sequenzstatus S5 die Ausgabe einer Identifikationskarte betrifft und da dazu Information vom Zentralcomputer am Terminal benötigt wird, kann die Karte nicht ausgegeben werden, wenn das Terminal unabhängig, d.h. ohne Verbindung, arbeitet. Dieser Zustand kann von einer Verzögerungsschaltung festgestellt werden, immer dann, wenn das Terminal nicht innerhalb einer bestimmten Zeit vom Zentralcomputer angerufen wird. Wenn unter normalen Umständen ein Anruf mindestens alle zehn Sekunden zu erwarten ist, kann die Zeitschaltung ein entsprechendes Signal beispielsweise erzeugen, wenn seit einer Minute kein Anruf erfolgt ist. Das «Ohne Verbindung»-Signal setzt einen entsprechenden Haltekreis im Sequenzzähler 22, der von der Anzeigelogik 26 ausgewertet wird, um das Signal «Verarbeiten» zu löschen und das Signal «Ohne Verbindung» darzustellen. Erscheint dieses Signal, so kann der Benützer entweder die Transaktion aufgeben und die erforderliche Information später neu eintasten oder er kann das Terminal im Sequenzstatus S5 belassen und versuchen, die Verbindung mit dem Zentralcomputer wieder herzustellen, oder andere Gründe für den Zustand zu beheben. Wenn die Übertragungslogik 15 eine Anzahl von Abfragen, beispielsweise sechs oder mehr, empfangen und auf jede mit dem NACK- und EOT-Byte geantwortet hat, so ändert sie den Status des Terminals von «Ohne Verbindung» zum Verbindungsstatus, worauf dieser die ursprünglich eingegebene Information an den Zentralcomputer überträgt.

Jedesmal, wenn das Terminal sich im Sequenzstatus S5 befindet, versucht die Übermittlungslogik 15 Information, die vom Zentralcomputer her übertragen wird, im Speicher von der Adressstelle A0 an zu speichern. Wenn das nächste Abfragesignal vom Zentralcomputer übertragen wird, antwortet die Übermittlungslogik 15 mit dem Anforderungssignal RTS. Der Modem 14 seinerseits erzeugt ein Bereitschaftssignal TTS und überträgt das ACK-Byte über die Sendeleitung Bit für Bit unter Synchronisation des STAKT-Signals vom Modem. Wenn das letzte Bit des ACK-Bytes auf den Modem 14 übertragen wird, leitet die Übermittlungslogik 15 das Datenbyte in der Speicherausgangshauptleitung des Speichers 19 in den Übertragungspuffer 30 der Übermittlungslogik. Der Abfall des in Fig. 13 gezeigten «8 BIT S»-Signals schaltet den Adresszähler 23 auf die nächste Adressstellung und veranlasst den Speicher 19, die Daten aus der nächsten Adressstelle in das Speicherausgangsregister zu übertragen, wo sie stehen, bis das nächste «8 BIT S»-Signal auftritt. Weil der Modem in seiner Geschwindigkeit auf maximal 9600 Bit/Sekunde begrenzt ist, stehen 104 Mikrosekunden zur Verfügung zwischen den Modemtaktimpulsen, d.h. reichlich Zeit, um ein Datenbyte aus dem Speicher in den Puffer zu übertragen. Das nächste Übertragungstaktsignal schickt das erste Bit des ersten Datenbytes zum Modem und schaltet den Taktzähler weiter. Wenn der Taktzähler achtmal fortgeschaltet ist und das achte Byte den Modem erreicht hat, wird ein neues «8 BIT S» (-Signal erzeugt, wodurch das nächste Datenbyte vom Ausgangsregister ins Übertragungsschieberegister 30 gelangt.

Jedes in den Puffer 30 übertragene Byte wird von der Steuerbytesendenlogik 43 decodiert, um festzustellen, ob es sich um ein EOM-Byte handelt, das das Ende der Übertragung anzeigt. Wenn ein EOM-Byte in den Puffer 30 übertragen wird, setzt die Logik 43 einen entsprechenden Haltekreis. Wenn das letzte Bit des EOM-Bytes zum Modem gelangt, wird ein Informationsbyte von der Adressenhauptleitung ins Register 30 übertragen, das die Länge der Meldung anzeigt. Die derzeitige Adressposition des Adresszählers zeigt die Länge der soeben übermittelten Meldung an. Wenn das letzte Bit der Adresszahl zum Modem übertragen wird, erzeugt der Abfall des STAKT-Signales ein neues «8 BIT S»-Signal und ein «Ende Übertragungs»-Zeichen gelangt zum Register 30, um die Übertragung abzuschliessen. Das «Ende Übertragungs»-Zeichen EOTS schaltet den Sequenzzähler auf S6 und setzt den Adresszähler auf A0 zurück. Im Status S6 kann eine Meldung vom Zentralcomputer empfangen werden.

Es ist möglich, dass bei der Übertragung der Meldung im Status S5 die gezählte Länge nicht mit der tatsächlichen Anzahl von übertragenen Bytes übereinstimmt oder auf andere Weise ein Fehler entdeckt wird. Im Fall eines Fehlers antwortet der Zentralcomputer mit den Bytes NACK und EOTE, wodurch eine Neuübertragung veranlasst wird. Wenn die Steuerbytelogik 36 die Bytes NACK und EOT in der Übertragungssteuerlogik 15 entdeckt, wird der Sequenzzähler 22 auf die Sequenz 5 geschaltet und die gesamte Meldung wiederholt.

Wurde die im Status S5 übertragene Meldung beim Zentralcomputer richtig empfangen, so wird sie dort gemäss dem Flussdiagramm in Fig. 4 behandelt. Dazu sind normalerweise weniger als zwei Sekunden nötig. Hat der Zentralcomputer eine Antwort bereit, so wird ein ACK-Byte und darauf die Datenbytes der Antwort, eine Längenzählung und ein EOT-Byte an den Terminal übertragen. Die Übermittlungssteuerlogik 15 arbeitet während des Empfangs wie folgt: Wenn der Modem 14 ein Signal über den Übermittlungskanal empfängt, das den Geräuschpegel deutlich übersteigt, so gibt er ein Empfangssignal RLS ab und stellt ein mit dem ETAKT synchronisiertes Datenbit auf der E-Daten-Ausgangsleitung zur Verfügung. Die Übermittlungssteuerlogik 15 überträgt jedes empfangene Bit in den Empfangspuffer 31. Im Puffer werden die Bits jeweils weitergeschoben, um für neueintreffende Bits Platz zu machen. Nach acht ETAKT-Pulsen, die vom ETAKT-Zähler 34 festgestellt werden, wird der Inhalt des Puffers decodiert und je nach dem entdeckten Zeichen der Abfrage-ACKR-, NACKR- oder EOTR-Haltekreis gesetzt. Wenn der Antwortkreis gesetzt wird, wird das ACK-Byte nicht gespeichert, sondern ein DATAR-Signal sowie das nächste «8 BIT E»-Signal erzeugt. Das «8 BIT E»-Signal schickt das erste Antwortbyte im Puffer auf die Speichereingangshauptleitung und veranlasst den Speicher 19, das Byte an der Adresse zu speichern, die der Adresszähler 23 angibt. Die abfallende Flanke des «8 BIT E»-Impulses schaltet den Adresszähler 23 um Eins weiter, damit das nächste Byte in der nächsten Position gespeichert werden kann. Wird ein «Ende Meldungs»-Signal (EOM) entdeckt, so wird der entsprechende Haltekreis gesetzt und das Signal als letztes in den Speicher übertragen. Wenn der EOM-Haltekreis gesetzt ist, wird das nächste Byte als Längenzählungsbyte betrachtet und von der Übermittlungssteuerlogik 15 mit dem Wert des Adresszählers verglichen. Besteht keine Übereinstimmung, dann ist die Meldung vermutlich fehlerhaft und ein Fehlerhaltekreis im Modifikatorteil des Sequenzzählers 22 wird gesetzt. Wird daraufhin das «Ende Übertragungs»-Byte im Empfangspuffer 31 entdeckt, so wird ein NACK-Byte von der Übermittlungssteuerlogik 15 über den Sendepuffer 30 geschickt, das den Zentralcom-

puter veranlasst, die Meldung erneut zu übermitteln. Wenn andererseits die Längenzählung mit dem Adresszähler übereinstimmt, erzeugt die Übermittlungssteuerlogik ein ACK- und ein EOT-Byte als Quittung für den Zentralcomputer. Das vom Zentralcomputer übertragene EOT-Byte setzt den Adresszähler auf A0. Ist der Fehlerhaltekreis nicht gesetzt, wenn das EOT-Byte entdeckt wird, so schaltet dieses den Sequenzzähler auf Sequenzstatus S7. In der Sequenz S7 wird dem Benützer die Antwort des Zentralcomputers ausgedruckt oder angezeigt, so dass Fehler entdeckt und wenn nötig richtiggestellt werden können. Die Arbeitsweise der Druckerlogik 28 entspricht in allem der Sendearbeitsweise der Übermittlungslogik 15. Ist beispielsweise der Drucker nicht unmittelbar beim Terminal angeordnet, so kann ein einzelnes Koaxialkabel ihn mit diesem verbinden, worüber Bit nach Bit vom Speicher zum Drucker übertragen wird. Ist andererseits genug Kabel für ein ganzes Byte vorhanden, so ist ein Taktimpuls ähnlich dem STAKT-Zähler in der Übermittlungssteuerlogik nicht erforderlich, weil die Bytes bereits parallel im Drucker eintreffen.

Wenn die Druckerlogik 28 den Status S7 feststellt, erzeugt sie ein Bereitschaftsbyte RTP, um die nötigen Motoren zu starten und das Papier in die richtige Position zu bringen, je nach der Art des Druckers. Ist der Drucker arbeitsbereit, so zeigt er der Steuerlogik 28 dies durch ein CTP-Signal an, worauf das erste Byte der Antwort des Zentralcomputers aus der Speicherposition A0 übertragen wird. Wenn acht Bits übertragen sind, schaltet der Adresszähler auf die nächste Stellung weiter, um die dort gespeicherte Information vom Speicher 19 über die Speicherausgangshauptleitung auf die Druckerlogik 28 zu übertragen. Die Druckerlogik decodiert alle Bytes, und wenn ein Feldtrennungsbyte oder ein «Ende Meldungs»-Byte festgestellt wird, fällt das RTP-Signal ab. Der Abfall dieses Signals veranlasst den Drucker, den Inhalt seines Puffers auszudrucken. Der Sequenzzähler 22 wird durch den Abfall von RTP auf den Status S8 weitergeschaltet.

Anhand der Fig. 10 wird nun die Arbeitsweise der Chiffrierlogik 25 erläutert. Die Information, die im Sequenzstatus S6 vom Zentralcomputer übermittelt worden war, steht im Sequenzstatus S8 im Speicher des Terminals bereit. Eine Zufallsschlüsselzahl (ZSZ), die fortlaufend vom Zufallsgenerator 29 erzeugt wird, wird während der Zyklen 49, 50, 51 und 52 festgehalten, damit die Zweibyte-Zufallszahl in die Speicherstellen A157 und A158 und in die Chiffrierschlüsselstellen A240 und 241 übertragen werden kann.

Die Daten vom Zentralrechner werden auf den Terminal über das Register 57, Fig. 14, über die Schaltungen 58 und 59 mittels der Signale LADE REG resp. SPEICHER REG übertragen. Diese Signale stammen von den Schaltungen 66 resp. 67 der Fig. 15. Das Zufallssignal wird von der Schaltung 71 erzeugt. Das Zufallssignal hält den Zufallsgenerator 59 an. Auf diese Weise kann eine beliebige Zahl asynchroner Eingänge an die Schaltung 71 angeschlossen werden, damit der Ausgang des Generators 29 tatsächlich eine Zufallszahl ist. Selbstverständlich kann jede andere Form der Erzeugung einer Zufallszahl benützt werden. Die Signale ZSZH und ZSZT stammen von den Schaltungen 69 resp. 70 und veranlassen den Zufallsgenerator 29, das hochstellige resp. das tiefstellige Byte des Zufallsschlüssels auf die Speichereingangshauptleitung abzugeben, so wie dies Fig. 10 zeigt. Im Zyklus 54 der Sequenz S8 wird ein Meldungsendebyte in die Adresse A159 während den Phasenzeiten 1 und 2 geladen. In der Phase 4 der Sequenz 8, Zyklus 54, erzeugt die Schaltung 72 das Signal INCS, das den Sequenzzähler 22 fortschaltet. Dasselbe Signal ist auch als CRÜCK bezeichnet und gelangt auf den Zykluszähler 53, um diesen auf die Ausführung der nächsten synchronen Operation der Chiffrierlogik 25 vorzubereiten.

Der Sequenzstatus S9 wird von der Tastatursteuerlogik 24 erkannt zur Aufforderung an den Benützer, in die Identifikationsworttasten 21, sein nur ihm bekanntes Identifikationswort einzugeben, das damit selbst der Person, die die Karte an den Kunden ausgibt, verborgen bleibt. Die Anzeigelogik 26 reagiert auf den Sequenzstatus S9 durch die Anzeige «Eingang Identifikationswort». Da die Identifikationsworttastatur die Betätigung einer numerischen Taste in einen Vierbinärbit-Hexadezimalcode umwandelt, besetzt ein Identifikationswort mit sechs Dezimalzahlen bereits drei Bytes, die in einem Dreibyte-Register in der Tastatur gespeichert werden, bis alle sechs Zahlen eingegeben sind. Da der Kunde sich bei der Eingabe irren kann, ist eine Löschtaste vorgesehen, die das Register auf einen vorgegebenen Wert zurückstellt. Ist ein Identifikationswort mit vier Dezimalzahlen vorgesehen, wird das Register nicht auf Null sondern auf eine bestimmte Zahl zurückgesetzt, die sicherstellt, das nach Eingabe des Wortes mit vier Dezimalzahlen die drei Bytes ausgefüllt sind. Ist der Kunde sicher, sein Identifikationswort richtig eingegeben zu haben, so betätigt er eine Funktionstaste, die ein KATTN-Signal an die Tastaturlogik 24 weitergibt, worauf das erste Byte in die Speicherstelle A232 übertragen wird. Wenn das KGATE-Signal abfällt, wird der Adresszähler fortgeschaltet und das zweite Byte im Ausgangspuffer der Tastatur veranlasst das nächste KATTN-Signal. Das zweite Byte wird darauf unter der Adresse A233 gespeichert und das dritte Byte in derAdresse A234. Die Tastatursteuerlogik wiederholt darauf das Identifikationswort zur Speicherung in den Adressen A242, A243 und A244, wie aus Fig. 9 ersichtlich.

Damit das Identifikationswort und das Schlüsselwort volle acht Datenbytes ausfüllen, werden in der Sequenz S10 die restlichen Bytes mit Teilen der Kontonummer ausgefüllt. Das Ausfüllen wird durch die Chiffrierlogik 25 der Steuerlogik 20 vorgenommen, wie dies Fig. 11 zeigt. Die Chiffrierlogik 25 empfängt das erste Byte der Kontonummer von der Speicherausgangshauptleitung und schickt es zuerst in den Speicherplatz A235 und dann in den Speicherplatz A245. Die Operation wird wiederholt mit dem zweiten und dritten Byte der Kontonummer, wogegen das vierte und fünfte Byte der Kontonummer lediglich zu den Speicherplätzen A238 resp. A239 geleitet wird. Die Kontonummer ist derart mit dem Dreibyte-Identifikationswort verwürfelt zu einem Achtbyte-Datenwort und das Identifikationswort und ein kleiner Teil der Kontonummer wurde mit der Zufallszahl verwürfelt zu einem Achtbyte-Identifikationsschlüsselwort, die beide der Datenverschlüsselung 18, gemäss dem USA-Patent 3 958 081, zugeleitet werden. Wenn die Verwürfelung des Identifikationsdatenwortes und des Identifikationsschlüsselwortes vollendet ist, wird der Sequenzzähler 22 auf den Status S11 fortgeschaltet.

Im Sequenzstatus S11 wird das Identifikationsdatenwort und das Identifikationsschlüsselwort vom Speicher zur Chiffrierschaltung 18 geleitet, dort chiffriert und die ersten vier Bytes, jetzt als EPIN1 bezeichnet, auf dem Magnetstreifen 7 der Karte 1 registriert. Die anderen vier Bytes des verschlüsselten Resultats sind mit EPIN2 bezeichnet und werden im Zentralcomputer gespeichert. Die Verschlüsselungseinrichtung des USA-Patentes 3 958 081 führt drei Reihen von Impulssignalen, die mit LIB, LDK und DOB bezeichnet sind und von Schaltungen ähnlich den Schaltungen 66 bis 72 kommen. Diese Signale sind in Fig. 12 dargestellt und sind dieselben wie die in Fig. 3B des USA-Patentes 3 958 081 dargestellten, die dort benutzt werden, um das Datenwort DW, das Schlüsselwort KW und das chiffrierte Ausgangswort Byte für Byte zu laden. Damit die im USA-Patent 3 958 081 beschriebenen Mittel benützt werden können, müssen die Steuer- und Synchronisiersignale so weit abgeändert werden, dass das Schlüsselwort und das Datenwort nacheinander und nicht gleichzeitig aus einem separten Schlüsselregister und einem Datenregister geladen werden, wie es im geanannten Patent beschrieben ist. Mit Bezug auf Fig. 12 sowie auf Fig. 7A des genannten Patentes ist festzustellen, dass die Signale LDK, $\overline{\text{LDK}}$ und SR während der Zyklen 0 bis 7 auftre-

ten. Andererseits treten die Takt- und Steuereinheitssignale LIB und $\overline{\text{LIB}}$ nur verzögert während der Zyklen 0′ bis 7′ auf, während aufeinanderfolgende Datenbytes, die zu verschlüsseln sind, auf der Speicherausgangshauptleitung bereitstehen, die mit der Speichereingangshauptleitung während den Zyklen 0′ bis 7′ in Verbindung steht.

Die Einzelheiten der Übertragung der Bytes des Achtbytes-Identifikationsdatenworts und der Bytes des Achtbytes-Identifikationsschlüsselworts in die Datenwortpuffer 100 und 150, sowie die Schlüsselwortpuffer 350 und 400 sind in Kolonnen 12, 13 und 14 des USA-Patentes 3 958 081 beschrieben. Die dortige Beschreibung trifft auch auf die hier vorliegende Fig. 10 zu, mit der Ausnahme, dass das Identifikationsdatenwort und das Identifikationsschlüsselwort sequentiell und nicht gleichzeitig geladen werden.

Nach der Chiffrierung steht ein chiffriertes Achtbyte-Datenausgangswort Byte für Byte zur Ausgabe bereit in der Chiffriereinheit 18. Die Bytes können synchron zum Signal DBO abgerufen werden. Während der ersten vier DBO-Impulse der Sequenz S11 werden die Bytes im Kartenpufferspeicher an den Adressen A152 bis A155 gespeichert. Die anderen vier Bytes werden zur Übermittlung an den Zentralcomputer an den Speicheradressen A24 bis A27 gespeichert. Die Übermittlung erfolgt als EPIN2, während dem Sequenzstatus S12.

Die Arbeitsweise des Speicheradresszählers und der Übermittlungslogik während der Sequenz S12 ist im wesentlichen identisch zu ihrer Arbeitsweise während der Sequenz S5 und wird daher hier nicht wiederholt. Es ist jedoch zu bemerken, dass die gesamte Mitteilung, die vom Zentralcomputer während der Sequenz S6 empfangen wird, zur Vergleichsprüfung an den Zentralcomputer zurückübermittelt wird. Die vier Bytes EPIN2 werden mit der zurückgegebenen Meldung verwürfelt zur Speicherung in der Kundeninformationskartei, die durch die Kontonummer des Kunden gekennzeichnet ist.

Während des Sequenzstatus S13 wird eine Quittung vom Ausgabeterminal empfangen, wenn die Längenzählung und die anderen Prüfungen der Meldung eine richtige Übertragung anzeigen. Der Sequenzzähler wird dadurch auf den Status S14 fortgeschaltet.

Im Sequenzstatus S14 zeigt die Anzeigelogik 26 das Signal «Registrieren Karte», um den Benützer zu veranlassen, eine Identifikationskarte durch den Magnetstreifenleser zu schicken, so dass die Daten an den Speicheradressen A125 und A129 im dritten Streifen 7 der Magnetkarte 1 registriert werden können.

Nachfolgend soll die Benützung der Karte anhand der Fig. 5 erläutert werden. Dazu sei angenommen, dass das Terminal sich im Sequenzstatus Null befindet, die Netzstromversorgung eingeschaltet ist und das Rückstellsignal alle Zähler und Schaltkreise auf Null zurückgestellt hat.

Um das Terminal in den Benützungsmodus zu bringen, wird eine Benützungstaste gedrückt. Diese ruft ein KATTN-Signal hervor, das in die Tastatursteuerlogik 24 gelangt. Da das Terminal im Status SO ist, erzeugt die Tastatursteuerlogik ein KGATE-Signal, das die Tastatur veranlasst, das Byte, das die gedrückte Benützungstaste erzeugt, auf die Speichereingangshauptleitung zu schicken. Das Byte wird in der Adresse A0 gespeichert und gleichzeitig der Tastatursteuerlogik zugeleitet. Die Tastatursteuerlogik erkennt das Byte als das Signal der Benützertaste, setzt den entsprechenden Haltekreis im Sequenzzähler und schaltet den Sequenzzähler über die Leitung SETS auf den Status S101. Die Anzeigelogik veranlasst das Meldungstableau das Signal «Karte lesen» zu zeigen, das den Benützer veranlasst, seine Karte in den Magnetstreifenleser einzusetzen. Die auf der Karte registrierten Daten werden abgelesen und an den Speicherstellen A128 bis A159 gespeichert, wie Fig. 9 zeigt. Stellt die Streifenleserlogik 21 das Endsignalbyte EOM fest, so wird der Sequenzzähler 22 über die Leitung INCR fortgeschaltet, während das «Ende Meldungs»-Signal im Speicher registriert wird. Nach der Fortschaltung steht der Sequenzzähler auf dem Status S102.

Im Sequenzstatus S102 wird der Zufallsschlüssel ZSZ von den Speicherplätzen A157, A158, von der Chiffrierlogik 25 auf die Speicherplätze A240 und A241 übertragen und der Sequenzstatus auf S103 erhöht.

Im Status S103 zeigt die Anzeigelogik 26 das Signal «Eingang Identifikationswort» und veranlasst so den Kunden sein nur ihm bekanntes Identifikationswort über die Tastatur 12 einzugeben. Das Identifikationswort besteht, wie schon bemerkt, aus einer persönlichen Zahl mit vier oder sechs Dezimalen. Wenn es eingegeben ist, betätigt der Benützer eine Funktionstaste, die ein KATTN-Signal an die Tastaturlogik gibt. Dieses Signal veranlasst im Sequenzstatus S103 die Tastatursteuerlogik 24, ein KGATE-Signal auszugeben, um das erste Byte mit den ersten beiden Dezimalziffern des Identifikationsworts an der Adresse A232 des Speichers 19 zu speichern. Am Ende des KGATE-Signals wird der Adresszähler 23 fortgeschaltet, worauf das zweite Byte des Identifikationswortes in gleicher Weise übertragen und an der Adresse A234 gespeichert wird.

Um die Entzifferung der Information auf der Identifikationskarte oder im Speicher des Zentralcomputers und damit den Zugang zum Identifikationswort zu erschweren, ist das Identifikationswort ein Teil des Schlüsselwortes an den Speicherplätzen A242 bis A244. Die Übertragung dieser Daten geschieht unter dem Einfluss der Chiffrierlogik 25, während des Sequenzstatus S104 in den bereits früher beschriebenen Schritten. Während des Sequenzstatus S105 wird ein Teil der Kontonummer, der an der Speicheradresse A129 beginnt, mit dem Datenwort, das an der Adresse A235 beginnt, und dem Schlüsselwort, das an der Adresse A245 beginnt, verwürfelt, bis diese Wörter volle 64 Bits aufweisen. Erst dann erfolgt die Verschlüsselung. Anschliessend wird der Sequenzzähler auf den Status S106 fortgeschaltet.

Die Ausführung der Sequenz S106 wird unter erneutem Hinweis auf Fig. 12 beschrieben. Während der Sequenz S106 werden das Identifikationsdatenwort und das Identifikationsschlüsselwort vom Speicher zur Chiffriereinheit 18 übertragen und die ersten vier Bytes des EPIN1 in der Vergleichslogik 56 mit den EPIN1-Bytes, die an den Adressen A152 bis A155 des Terminalspeichers stehen, verglichen. Wenn die ersten vier Bytes identisch sind mit den von der Karte abgelesenen EPIN1-Bytes, ist eine erste Überprüfung bestanden. Die Chiffrierlogik speichert die anderen vier Bytes EPIN2 an den Speicheradressen A24 bis A27 für die spätere Übermittlung zum Zentralcomputer. Stimmt jedoch der Ausgang EPIN1 von der Chiffrierlogik nicht mit den im Terminalspeicher an den Adressen A152 bis A155 gespeicherten überein, so wird ein Ungültigmodifikator gesetzt, der den Sequenzzustand auf S106′ abändert. Im Status 106′ zeigt die Anzeigelogik 26 das Signal «Nicht genehmigt». Das Terminal verbleibt im Status S106′ bis ein Rückstellschalter betätigt wird, der das Terminal in den Status S0 versetzt.

Stimmt hingegen das von der Chiffrierlogik gelieferte Signal EPIN1 mit dem im Terminalspeicher an den Adressen A152 bis A155 gespeicherten EPIN1-Signal überein, so liefert die Schaltung 72 der Chiffrierlogik 25 ein Fortschaltsignal, das den Sequenzzähler in den Status S107 bringt.

Im Status S107 wird die von der Identifikationskarte 1 abgelesene Information, die jetzt an den Adressen A128 bis A151 gespeichert ist, zum Zentralcomputer übertragen, wo sie in den Adressen A0 bis A23 gespeichert wird. Da dazu die Tastatursteuerlogik benützt werden kann, sind andere Schaltkreise nicht erforderlich. Wenn die Kartendaten auf den Zentralcomputer übertragen sind, wird der Sequenzzähler fortgeschaltet zum Sequenzstatus S108.

Im Sequenzstatus S108 zeigt die Anzeigelogik 26 gleichzeitig ein oder mehrere Signale, die den Benützer veranlassen,

Angaben über die gewünschte Transaktion einzugeben. Dazu gehört beispielsweise die Art der Transaktion, ein Geldbetrag oder irgendwelche andere Information, die der Zentralcomputer erkennen kann und die im freien Platz seines Puffers nach der Position A28 Platz hat. die Transaktionsinformation wird von der Tastatur weitergeleitet, wie schon früher in Bezug auf den Ausgabemodus beschrieben. Als einfaches Beispiel eines Transaktion können Daten in mehreren separaten Teilen eingegeben werden, wobei ein erster Teil die Art der Transaktion, z.B. die Ausgabe eines Kreditchecks oder den Transfer von Geld, betrifft. Die Transaktionsart kann durch ein Informationsbyte von der Tastatur her in der Position A28 des Speichers registriert werden, worauf der Sequenzstatuszähler auf S109 weitergeschaltet wird. In der Sequenz S109 kann die Anzeigevorrichtung beispielsweise den verlangten Geldbetrag anzeigen, der gleichzeitig von der Speicherposition A30 an im Speicher registriert wird. Andere Information kann in der Sequenz S111 folgen. Die Betätigung einer Taste «Meldungsende» schaltet den Statuszähler auf S111 und den Adresszähler auf A0, wo er nun bereitsteht für die Übertragung der Identitätsüberprüfungsdaten an den Zentralcomputer.

Die Arbeitsweise des Terminals im Sequenzstatus S111 ist identisch mit der Arbeitsweise im früher beschriebenen Sequenzstatus S5, und die Einzelheiten brauchen hier nicht wiederholt zu werden. Ist die Meldung beim Zentralcomputer empfangen worden, so werden unter der Steuerung des dortigen Programmes die Kontonummer des Benützers festgestellt und die sein Konto betreffenden Aufzeichnungen aufgesucht. Danach wird das vom Terminal übertragene Feld EPIN2 vom Programm mit dem Inhalt des im Speicher registrierten EPIN2-Felds verglichen, wie das Flussdiagramm in Fig. 5 zeigt.

Stimmt das übertragene EPIN2-Feld mit dem im Zentralcomputer gespeicherten EPIN2-Feld überein, so ist die zweite Überprüfung bestanden und mit grosser Sicherheit bewiesen, dass der Benützer tatsächlich diejenige Person ist, die rechtmässig Zugriff zum Konto verlangt. Wenn andererseits das vier Byte lange, vom Terminal übertragene EPIN2-Feld mit dem im Zentralcomputer gespeicherten nicht übereinstimmt, so ist die zweite Identifikationsprüfung nicht bestanden. Das kann hervorgerufen sein durch einen Übertragungsfehler, der nicht entdeckt wurde, oder durch die Eingabe eines unrichtigen Identifikationswortes. Ohne Rücksicht auf den Grund wird die Transaktion nicht vorgenommen, sondern als ungültig am Terminal angezeigt.

Wurde die zweite Identitätsüberprüfung als richtig befunden, so behandelt das Programm die verlangte Transaktion weiter. Dazu wird z.B. festgestellt, ob die Transaktion den zulässigen Geldbetrag pro Zeiteinheit über das für den betreffenden Benützer festgesetzte Maximum belastet. Andere Prüfungen können eine zu häufige Benützung, das Ablaufdatum der Identifikationskarte und die Verfügbarkeit des gewünschten Betrags auf dem Konto betreffen. Diese Schritte sind alle bekannt, und Computerprogramme, beispielsweise das «IBM 360 On-Line Teller Program» sind erhältlich. Wenn in einer Prüfung die Transaktion als unzulässig erkannt wird, erfolgt eine entsprechende Anzeige am Terminal. Sind alle Prüfungen bestanden, so erfolgt eine Genehmigungsanzeige. Die Übermittlung der Antwortmeldung vom Zentralcomputer zum Terminal ist so gut wie identisch zu der, die früher im Zusammenhang mit Sequenzstatus S6 betreffend die Kartenausgabe beschrieben wurde. Der Hauptunterschied liegt natürlich im Inhalt der Meldung an das Terminal. Die Meldung wird am Terminal im Sequenzstatus S112 empfangen und im Speicher an Adressen, die mit der Position A0 beginnen, gespeichert. Während der Übertragung entdeckt die Steuerbytelogik 36 allfällige Steuerinformation, die auf ungültige Zeichen, «Genehmigt»- oder «Nicht Genehmigt»-Signale hinweist. Wird ein solches Signal entdeckt, so erzeugt die Übermittlungslogik 15 Modifikatorsignale für den Sequenzzähler 22, um den Sequenzstatus S112 entsprechend zu ändern. Die Anzeigelogik 26 wird darauf den bestehenden Zustand anzeigen. Ist die Transaktion nicht genehmigt, so kann die Nachricht vom Zentralcomputer Mitteilungen enthalten, die vom Drucker auszudrucken sind. Wenn die Meldung vom Zentralcomputer jedoch zuerst ein Genehmigungs-Byte überträgt, so wird der Benützer dadurch veranlasst, die noch ausstehenden Daten über die gewünschte Transaktion einzugeben.

Um die Sicherheit der Identitätsüberprüfung noch zu verbessern, wird nun eine neue Zufallsschlüsselzahl vom Zufallsgenerator 29 benützt, der an die Verschlüsselungseinheit 18 geht, und ein neues EPIN1 sowie ein neu es EPIN2 erzeugt. Während also an der Tastatur die restlichen Angaben über die Transaktion eingegeben werden, springt der Sequenzstatuszähler zurück auf Status S8 und wiederholt die früher in Bezug auf den Kartenausgabemodus beschriebenen Schritte, um ein neues Signal EPIN1 und EPIN2 zu erzeugen. Eine neue Zufallsschlüsselzahl, die vom Zufallsgenerator 29 erzeugt wird, wird der Speichereingangshauptleitung zur Speicherung an den Positionen A240 und A241 zugeleitet. Die Chiffrierlogik 25 leitet diese Zahl zusätzlich an die Adressen A40 und A41 des Terminals und an die Adressen A257 und A258, damit sie auch als neues EPIN1 auf der Identifikationskarte registriert werden. Wie früher beschrieben, wird das neue EPIN1-Signal auch in den Speicherplätzen A252 bis A255 und das neue EPIN2 in den Plätzen A24 bis A27 registriert. Das neue EPIN2 wird zusätzlich zum Zentralcomputer übermittelt und in dem für das Kundenkonto vorgesehenen Speicherplatz anstelle des alten EPIN2 registriert. Ein Quittungssignal kommt zurück zum Terminal, das eine Anzeige des gesamten Vorgangs veranlasst, damit der Benützer seine Identifikationskarte zur Registrierung des neuen EPIN1 und des neuen Schlüsselwortes in das Terminal einführen kann.

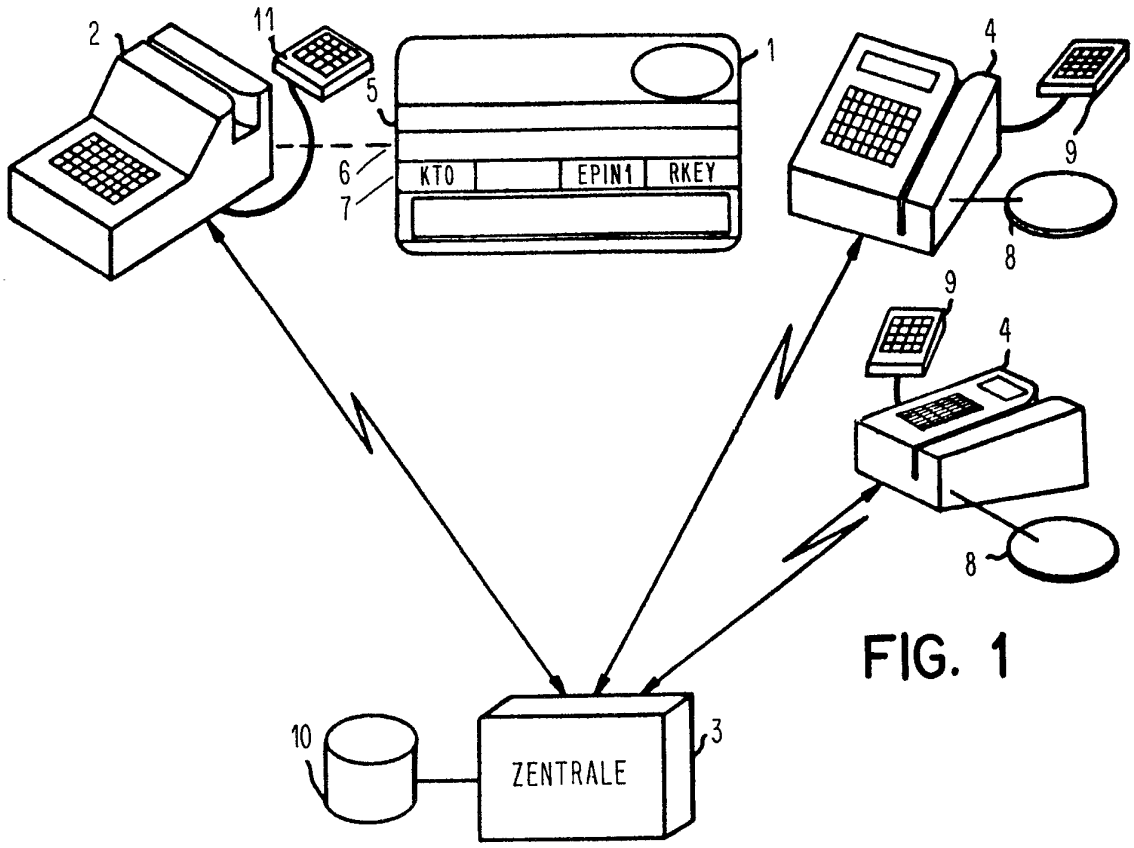

2
11
5
1
4
6
7
KTO
EPIN1
RKEY
9
8
9
4
8
10
ZENTRALE
3

FIG. 1

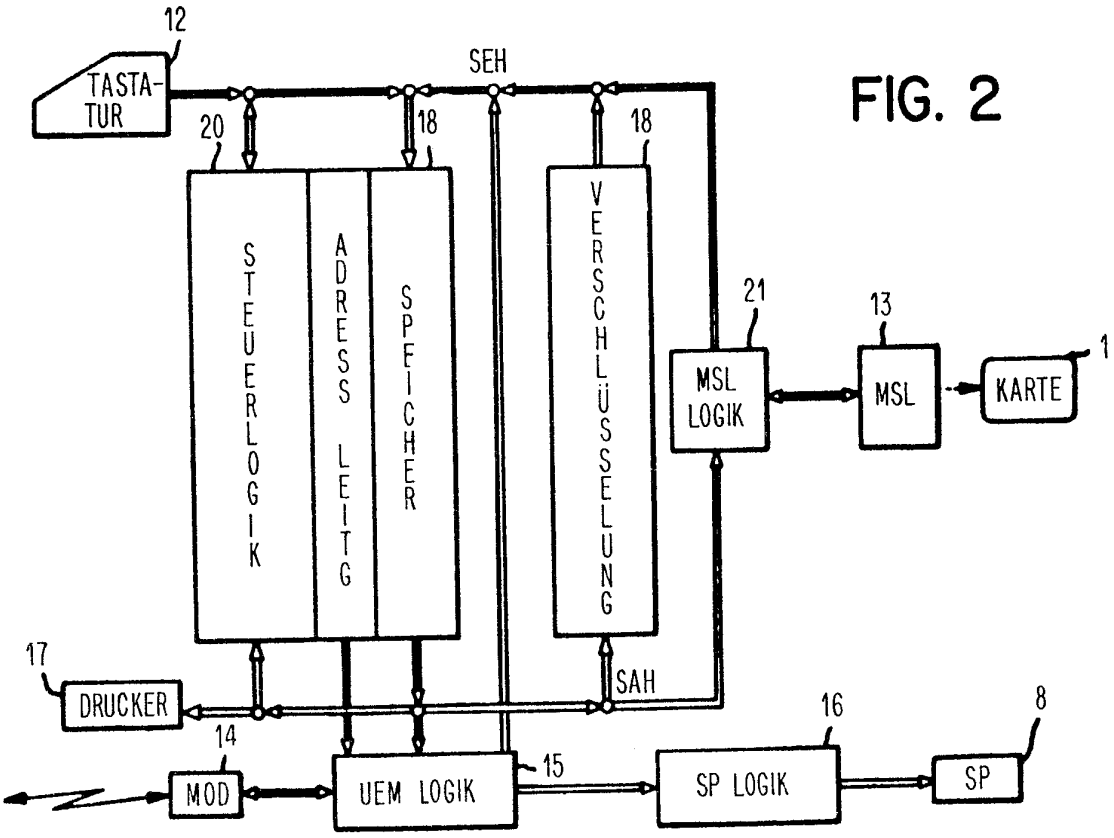

12
TASTA-
TUR
SEH
20
18
18
STEUERLOGIK
ADRESS LEITG
SPEICHER
VERSCHLÜSSELUNG
21
13
1
MSL
LOGIK
MSL
KARTE
17
DRUCKER
SAH
16
8
14
15
MOD
UEM LOGIK
SP LOGIK
SP

FIG. 2

FIG. 3

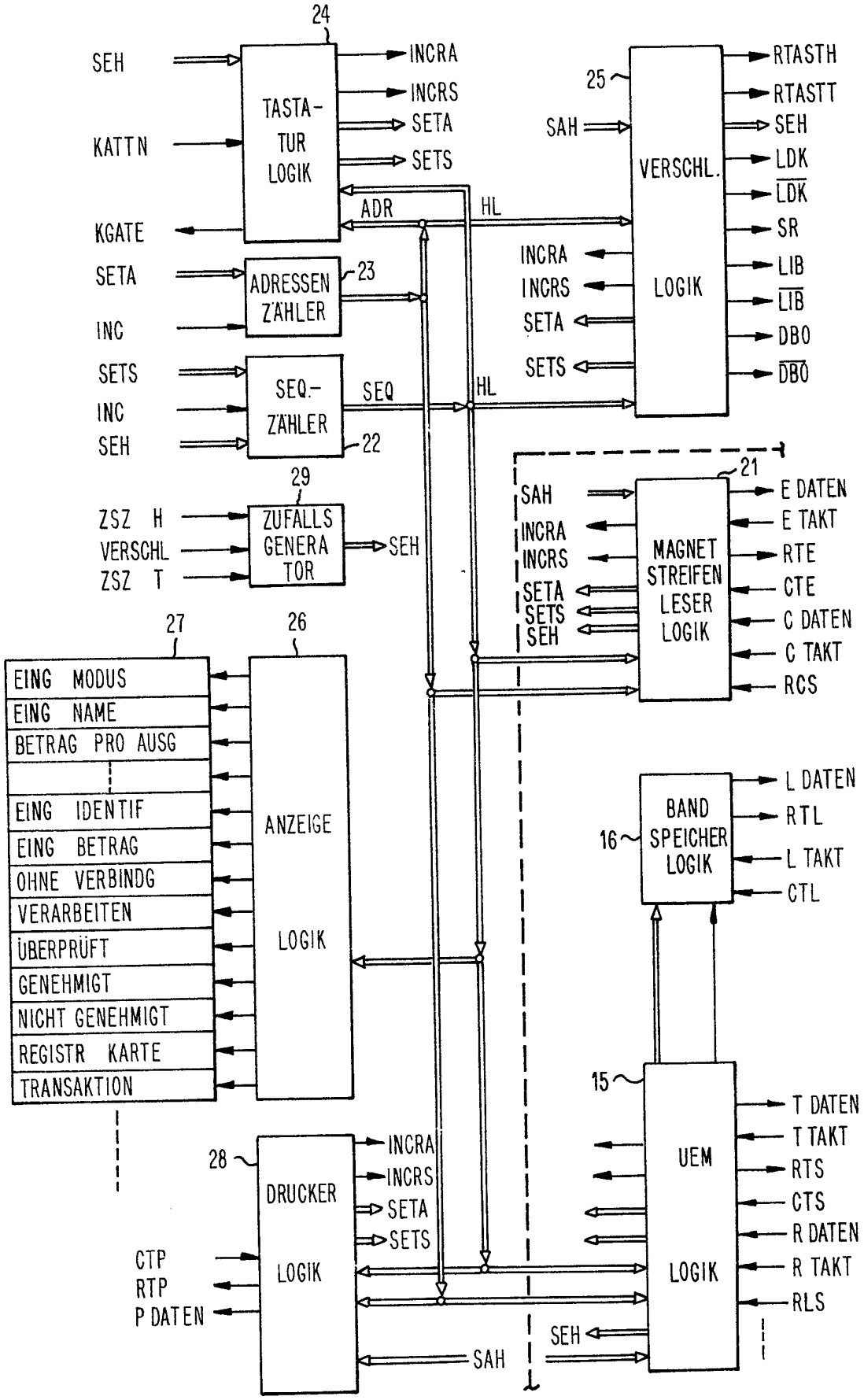

24
SEH
KATTN
KGATE
TASTA-
TUR
LOGIK
INCRA
INCRS
SETA
SETS
ADR
HL
25
SAH
VERSCHL.
LOGIK
RTASTH
RTASTT
SEH
LDK
LDK
SR
LIB
LIB
DBO
DBO
INCRA
INCRS
SETA
SETS
SETA
INC
ADRESSEN
ZÄHLER
23
SETS
INC
SEH
SEQ.-
ZÄHLER
SEQ
HL
22
29
ZSZ H
VERSCHL
ZSZ T
ZUFALLS
GENERA
TOR
SEH
21
SAH
INCRA
INCRS
SETA
SETS
SEH
MAGNET
STREIFEN
LESER
LOGIK
E DATEN
E TAKT
RTE
CTE
C DATEN
C TAKT
RCS
27
26
EING MODUS
EING NAME
BETRAG PRO AUSG
EING IDENTIF
EING BETRAG
OHNE VERBINDG
VERARBEITEN
ÜBERPRÜFT
GENEHMIGT
NICHT GENEHMIGT
REGISTR KARTE
TRANSAKTION
ANZEIGE
LOGIK
16
BAND
SPEICHER
LOGIK
L DATEN
RTL
L TAKT
CTL
15
UEM
LOGIK
T DATEN
T TAKT
RTS
CTS
R DATEN
R TAKT
RLS
28
DRUCKER
LOGIK
INCRA
INCRS
SETA
SETS
CTP
RTP
P DATEN
SAH
SEH

FIG. 4

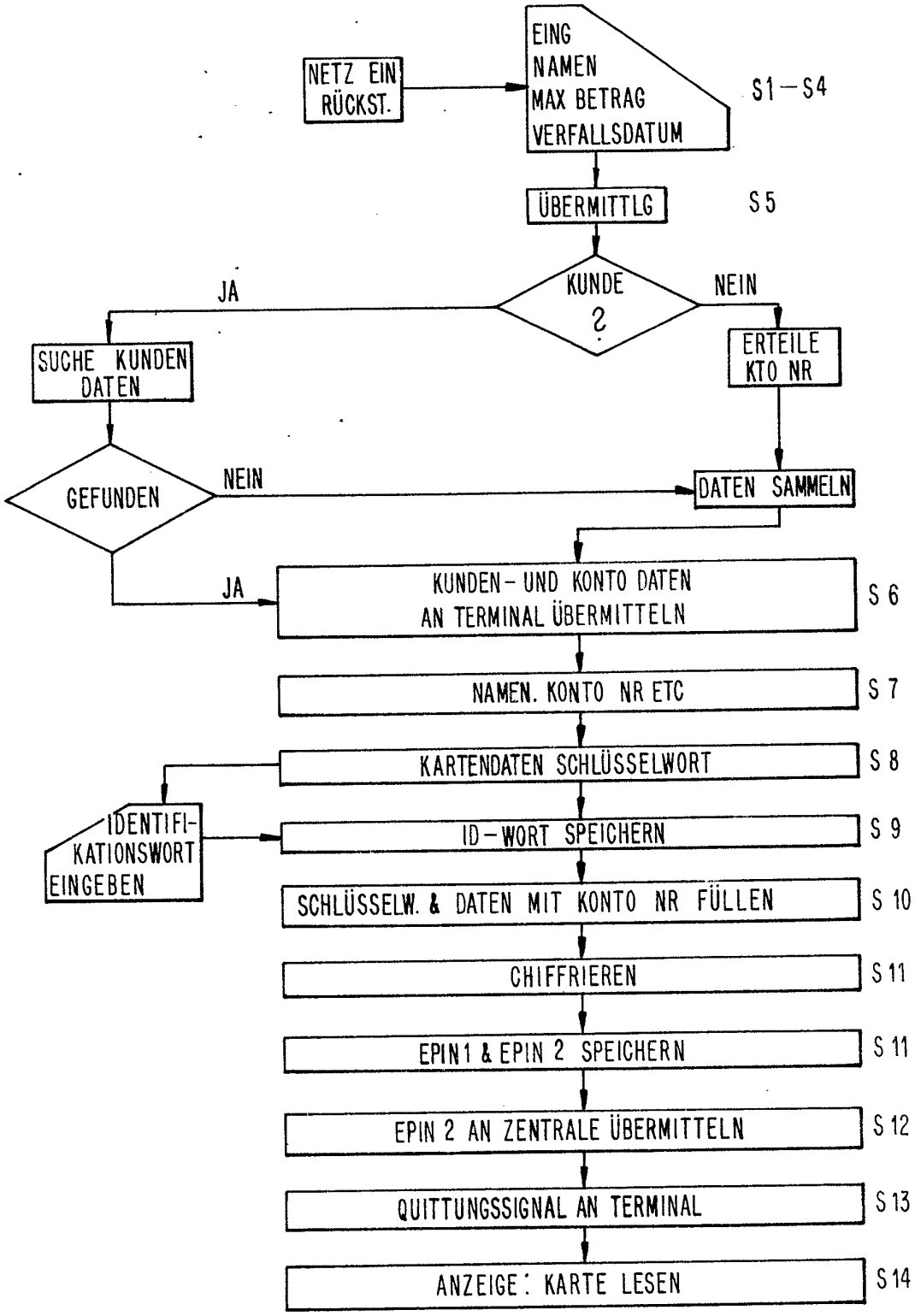

NETZ EIN RÜCKST.
EING NAMEN MAX BETRAG VERFALLSDATUM
S1–S4
ÜBERMITTLG
S5
KUNDE ?
JA
NEIN
SUCHE KUNDEN DATEN
ERTEILE KTO NR
GEFUNDEN
NEIN
DATEN SAMMELN
JA
KUNDEN- UND KONTO DATEN AN TERMINAL ÜBERMITTELN
S6
NAMEN. KONTO NR ETC
S7
KARTENDATEN SCHLÜSSELWORT
S8
IDENTIFI-KATIONSWORT EINGEBEN
ID-WORT SPEICHERN
S9
SCHLÜSSELW. & DATEN MIT KONTO NR FÜLLEN
S10
CHIFFRIEREN
S11
EPIN1 & EPIN 2 SPEICHERN
S11
EPIN 2 AN ZENTRALE ÜBERMITTELN
S12
QUITTUNGSSIGNAL AN TERMINAL
S13
ANZEIGE: KARTE LESEN
S14

FIG. 5

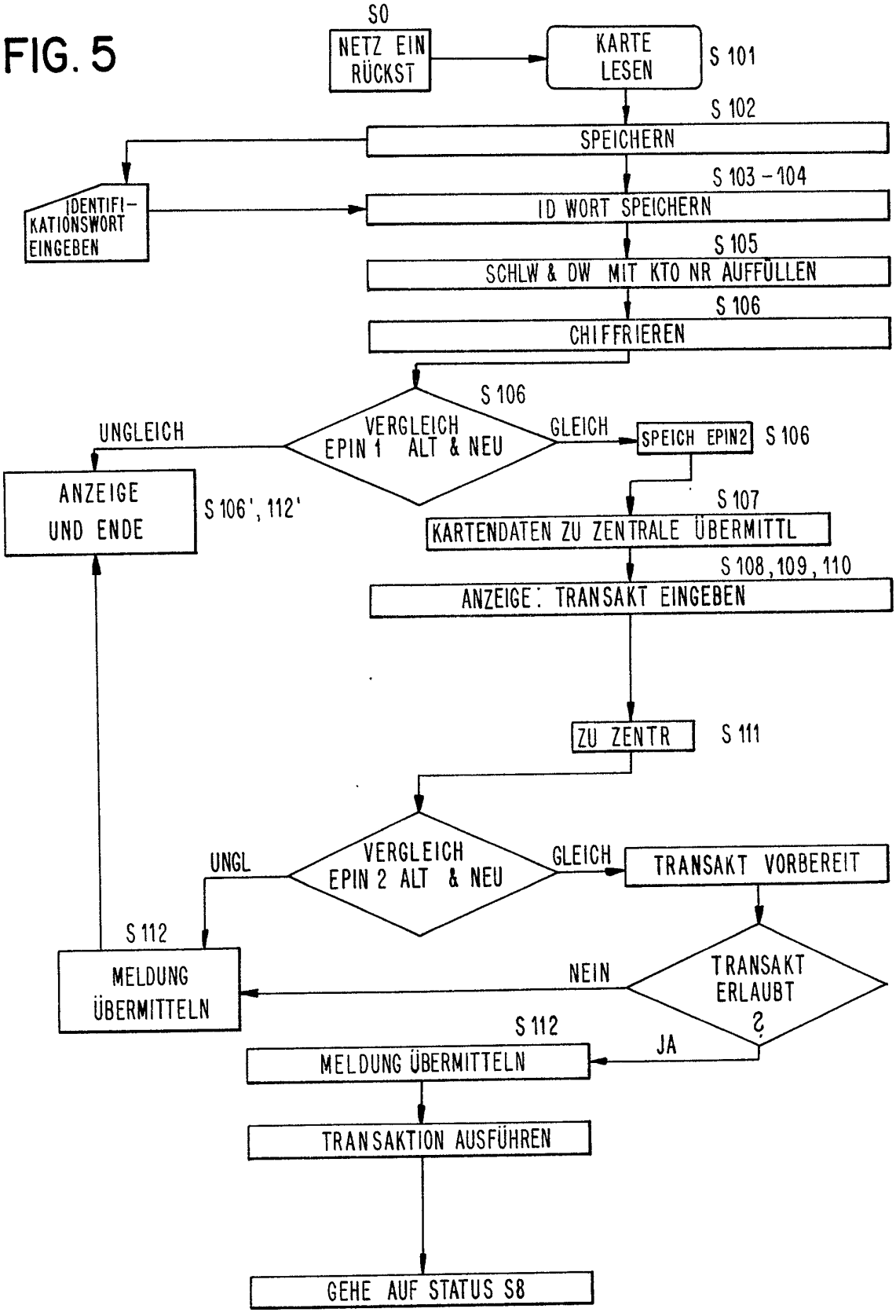

S0
NETZ EIN RÜCKST
KARTE LESEN
S 101
S 102
SPEICHERN
S 103 - 104
IDENTIFI-KATIONSWORT EINGEBEN
ID WORT SPEICHERN
S 105
SCHLW & DW MIT KTO NR AUFFÜLLEN
S 106
CHIFFRIEREN
S 106
VERGLEICH EPIN 1 ALT & NEU
UNGLEICH
GLEICH
SPEICH EPIN2
S 106
ANZEIGE UND ENDE
S 106', 112'
S 107
KARTENDATEN ZU ZENTRALE ÜBERMITTL
S 108, 109, 110
ANZEIGE: TRANSAKT EINGEBEN
ZU ZENTR
S 111
VERGLEICH EPIN 2 ALT & NEU
UNGL
GLEICH
TRANSAKT VORBEREIT
S 112
MELDUNG ÜBERMITTELN
NEIN
TRANSAKT ERLAUBT ?
S 112
MELDUNG ÜBERMITTELN
JA
TRANSAKTION AUSFÜHREN
GEHE AUF STATUS S8

FIG. 6

SEQUENZ LEITG FELDER

	SEQUENZ MODUS		SEQUENZ ZÄHLUNG								SEQUENZ MODIFIKATOREN			
											ÜBER-LAUF	OHNE VERBINDG	ETC	ETC
TEST	0	0	X	X	X	X	X	X	X	X				
AUSGABE	0	1	X	X	X	X	X	X	X	X				
BENÜTZG	1	0	X	X	X	X	X	X	X	X	X	X	X	X
VERSCH.	1	1	X	X	X	X	X	X	X	X	X	X	X	X

FIG. 7

DATEN ART	ADRESS BIT MUSTER							
	MSB	64	32	16	8	4	2	LSB
HAUPTPUFFER	0	X	X	X	X	X	X	X
KARTENPUFFER	1	0	0	0	0	0	X	X
IDDW	1	1	1	0	1	X	X	X
IDKW	1	1	1	1	0	X	X	X
COM KW	1	1	1	1	1	X	X	X

FIG. 8

SPEICHER INHALT ENDE SEQUENZ STATUS S4

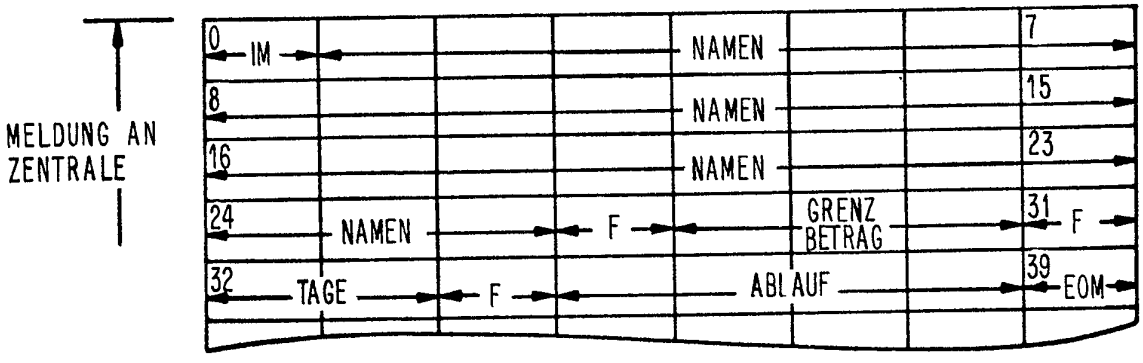


FIG. 9

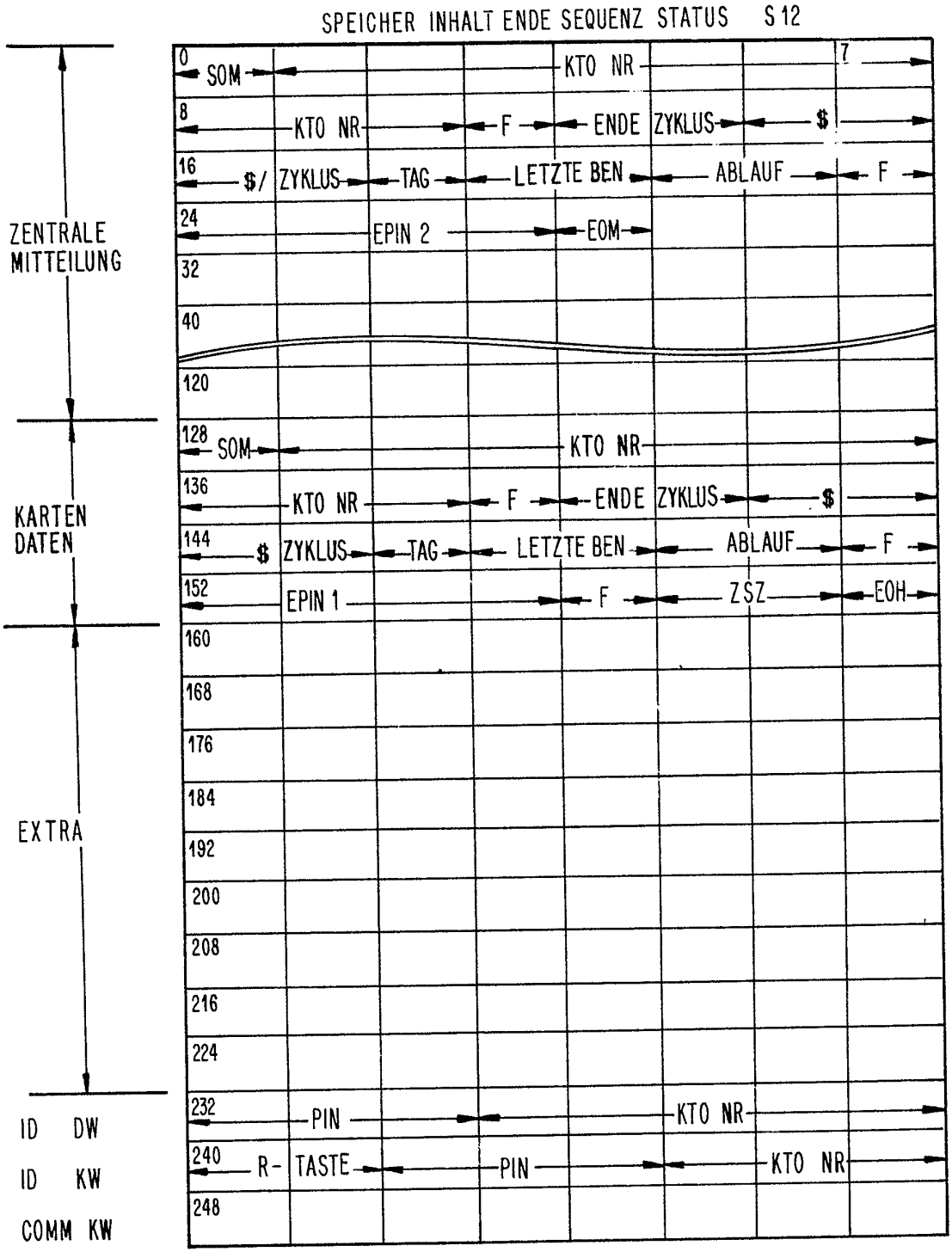
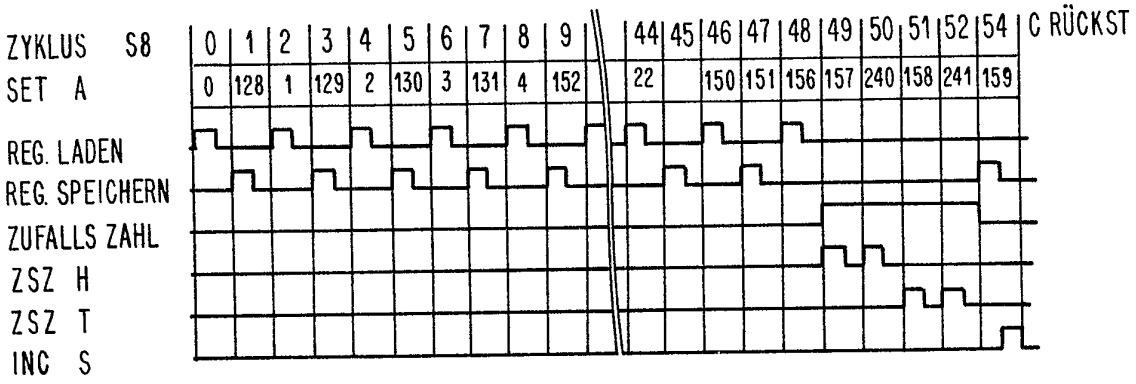

SPEICHER INHALT ENDE SEQUENZ STATUS S 12
ZENTRALE MITTEILUNG
KARTEN DATEN
EXTRA
ID DW
ID KW
COMM KW
0 SOM KTO NR 7
8 KTO NR F ENDE ZYKLUS $
16 $/ ZYKLUS TAG LETZTE BEN ABLAUF F
24 EPIN 2 EOM
32
40
120
128 SOM KTO NR
136 KTO NR F ENDE ZYKLUS $
144 $ ZYKLUS TAG LETZTE BEN ABLAUF F
152 EPIN 1 F ZSZ EOH
160
168
176
184
192
200
208
216
224
232 PIN KTO NR
240 R- TASTE PIN KTO NR
248

FIG. 10



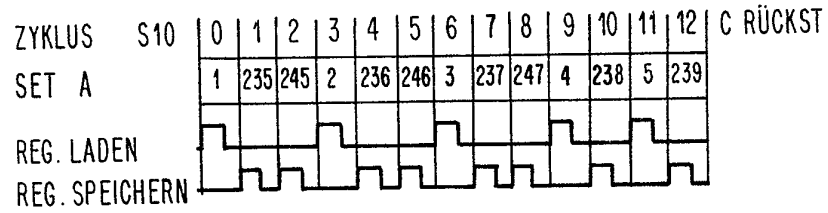


FIG. 11

FIG. 14

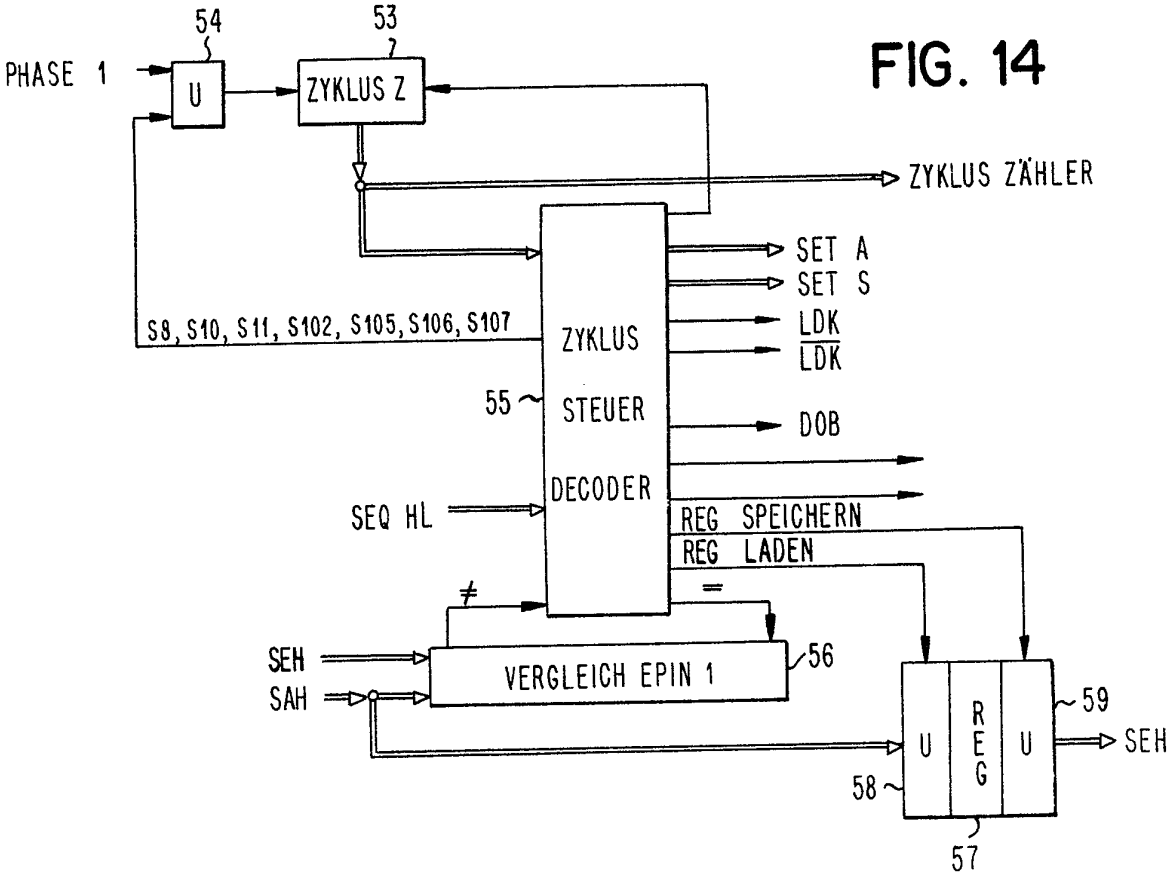
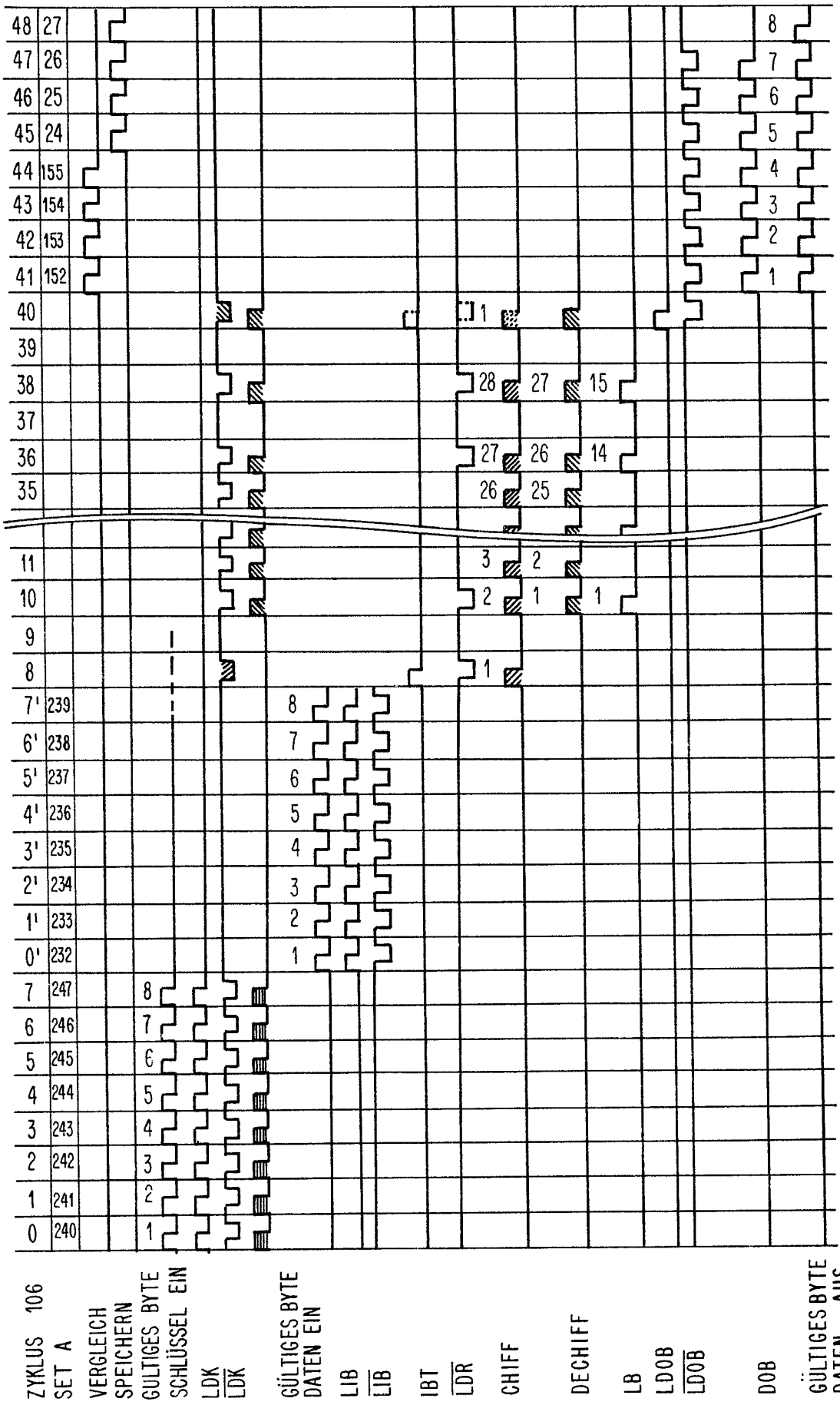


FIG. 12


ZYKLUS 106
SET A
VERGLEICH SPEICHERN
GULTIGES BYTE SCHLÜSSEL EIN
LDK
LDK
GÜLTIGES BYTE DATEN EIN
LIB
LIB
IBT
LDR
CHIFF
DECHIFF
LB
LDOB
LDOB
DOB
GÜLTIGES BYTE DATEN AUS

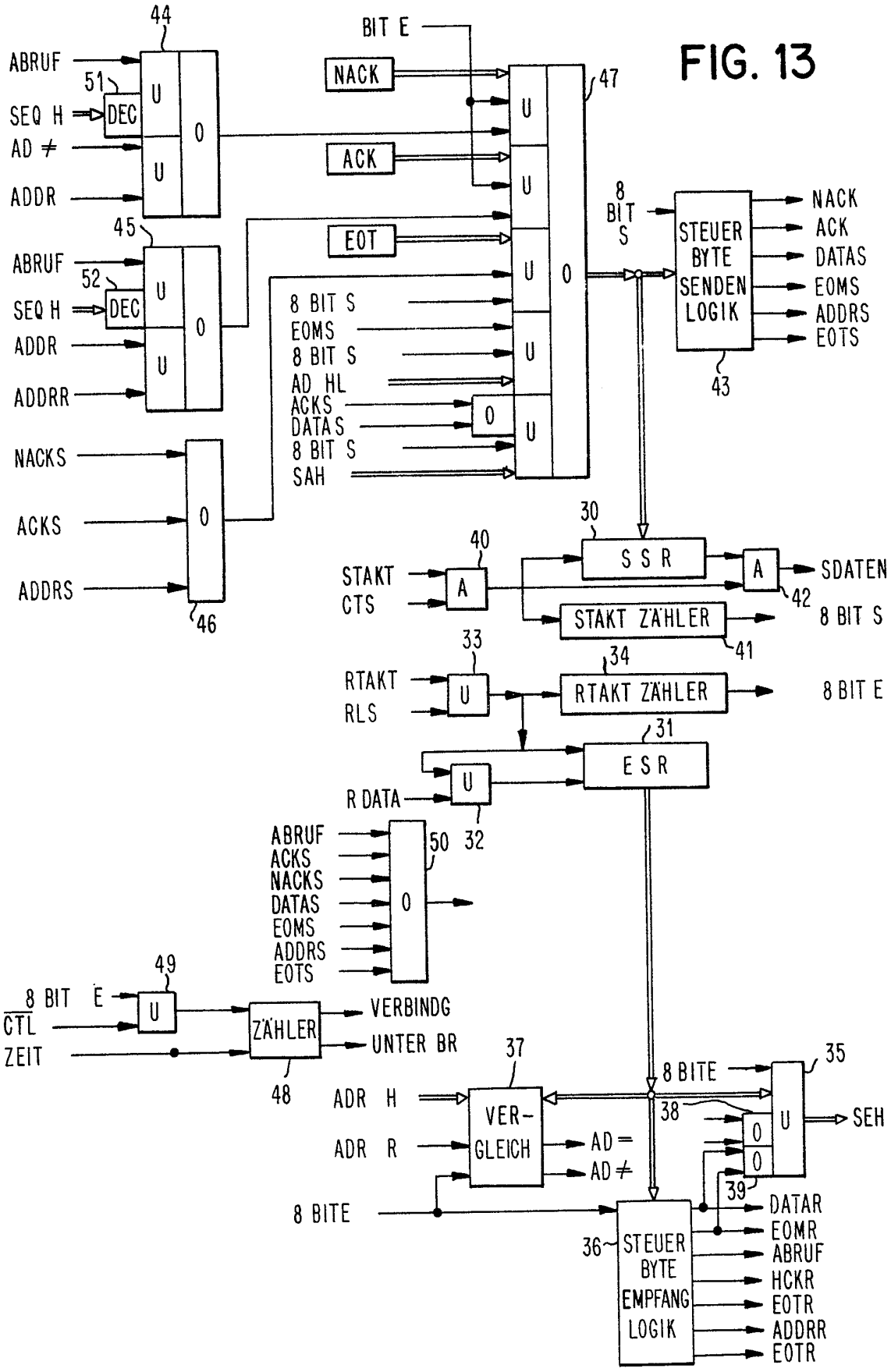

44
ABRUF
51
DEC
SEQ H
AD ≠
ADDR
U
U
0
45
ABRUF
52
DEC
SEQ H
ADDR
ADDRR
U
U
0
NACKS
ACKS
ADDRS
0
46
BIT E
NACK
ACK
EOT
8 BIT S
EOMS
8 BIT S
AD HL
ACKS
DATAS
8 BIT S
SAH
U
U
U
U
0
U
0
47
8 BIT S
STEUER BYTE SENDEN LOGIK
43
NACK
ACK
DATAS
EOMS
ADDRS
EOTS
30
40
STAKT
CTS
A
S S R
STAKT ZÄHLER
A
42
41
SDATEN
8 BIT S
33
34
RTAKT
RLS
U
RTAKT ZÄHLER
8 BIT E
31
R DATA
U
32
E S R
ABRUF
ACKS
NACKS
DATAS
EOMS
ADDRS
EOTS
0
50
49
8 BIT E
CTL
ZEIT
U
ZÄHLER
48
VERBINDG
UNTER BR
37
ADR H
ADR R
VER-GLEICH
AD =
AD ≠
8 BITE
8 BITE
35
38
0
0
U
SEH
39
36
STEUER BYTE EMPFANG LOGIK
DATAR
EOMR
ABRUF
HCKR
EOTR
ADDRR
EOTR

FIG. 13

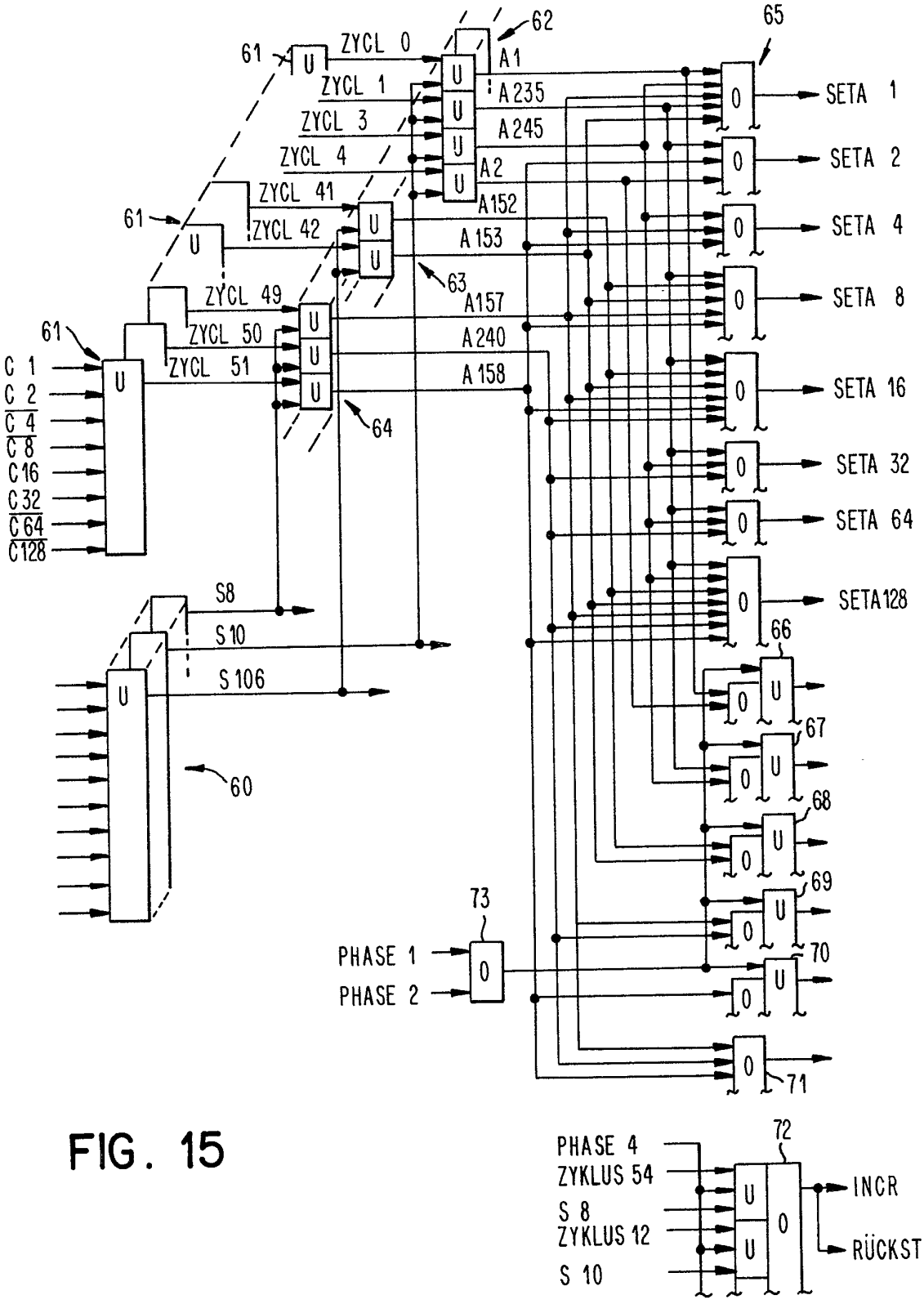

61
62
65
ZYCL 0
ZYCL 1
ZYCL 3
ZYCL 4
ZYCL 41
ZYCL 42
ZYCL 49
ZYCL 50
ZYCL 51
A1
A 235
A 245
A2
A152
A 153
A157
A 240
A 158
63
64
C 1
C 2
C 4
C 8
C16
C 32
C 64
C128
S8
S 10
S 106
60
73
PHASE 1
PHASE 2
66
67
68
69
70
71
SETA 1
SETA 2
SETA 4
SETA 8
SETA 16
SETA 32
SETA 64
SETA128
72
PHASE 4
ZYKLUS 54
S 8
ZYKLUS 12
S 10
INCR
RÜCKST

FIG. 15