BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

PATENTSCHRIFT 1 047 837

DBP 1 047 837
KL. 21 a¹ 21
INTERNAT. KL. H 04 k

ANMELDETAG: 12. APRIL 1955

BEKANNTMACHUNG DER ANMELDUNG UND AUSGABE DER AUSLEGESCHRIFT: 31. DEZEMBER 1958

AUSGABE DER PATENTSCHRIFT: 2. JULI 1959

STIMMT ÜBEREIN MIT AUSLEGESCHRIFT 1 047 837 (H 23593 VIII a / 21 a¹)

Verfahren zur Herstellung von verlängerten Schlüsselstreifen sehr großer Periode

Zusatz zum Patent 1 012 635

Das Hauptpatent hat angefangen am 27. Januar 1955

Patentiert für:

Fa. Dr.-Ing. Rudolf Hell, Kiel-Dietrichsdorf

Dr.-Ing. Rudolf Hell, Kiel, ist als Erfinder genannt worden

1

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Herstellung von verlängerten Schlüsselstreifen sehr großer Periode für Schlüsselmaschinen mit einer einzigen Folge von Aufzeichnungen binärer Zeichen zum Verschlüsseln von auf einem Klartextstreifen in Form von binären Zeichen registrierten Impulsfolgen, die den zu übertragenden Informationen eines Hell- oder Faksimilesenders zugeordnet sind, unter Verwendung von unperiodischen Schlüsselstreifen, deren Länge klein gegenüber der Länge der zu verschlüsselnden Klartextstreifen ist, mit einer kleinen Anzahl n ($n = 3$ bis 7) von gesetzlosen, willkürlich gewählten Folgen von Aufzeichnungen der binären Zeichen mit ungefähr statistischer Gleichverteilung dieser beiden Zeichen, wobei die Zeichen der Folgen in n nebeneinanderstehenden Spalten parallel zur Längsausdehnung des Streifens so angeordnet sind, daß sie quer zum Streifen wechselnde Kombinationen zu je n Zeichen (Codegruppen) ergeben, und unter Verwendung von Speicher- und Abfragevorrichtungen.

Im Hauptpatent ist ein Verfahren beschrieben, aus einem unperiodischen Schlüsselstreifen mit mehreren binären Zeichenfolgen, dessen Länge klein gegenüber der Länge eines zu verschlüsselnden Klartextstreifens mit mehreren binären Zeichenfolgen ist, unter Verwendung von Speicherscheiben und Abfragevorrichtungen einen periodischen Schlüsselstreifen sehr langer Periode herzustellen, dessen Zeichen mit den zugeordneten Zeichen des Klartextstreifens multiplikativ überlagert werden.

Das Verfahren nach dem Hauptpatent hat neben der Sicherheit in verschlüsselungstechnischer Hinsicht den Vorteil, daß der Schlüsselstreifen mit extrem langer Periode gestattet, eine größere Anzahl von Sprüchen verschlüsseln zu können, ohne daß für jeden neuen Spruch ein neuer unperiodischer Schlüsselstreifen hergestellt zu werden braucht, und daß der verwendete unperiodische Schlüsselstreifen kürzer als der zu verschlüsselnde Spruch ist.

Das Verfahren nach dem Hauptpatent hat indessen den Nachteil, daß der Schlüsselstreifen die Schlüsselvorrichtung mit sehr unterschiedlicher Geschwindigkeit verläßt, so daß er, wenn er in einer weiteren Vorrichtung mit dem Klartextstreifen überlagert werden soll, die beide Streifen mit konstanter Geschwindigkeit verarbeitet, zwischen beiden Vorrichtungen eine Schleife bilden muß, die als Puffer wirkt, um den Unterschied zwischen beiden Geschwindigkeiten auszugleichen.

Die vorliegende Erfindung vermeidet diesen Nachteil, indem der Schlüsselstreifen die Schlüsselvorrichtung mit konstanter Geschwindigkeit verläßt. Überdies wird die Verschlüsselung zur Erschwerung der

2

unbefugten Entzifferung noch wesentlich komplizierter gestaltet. Schließlich ist die Erfindung vorzugsweise zum Verschlüsseln von Informationen in Form von Impulsfolgen, wie sie von Hell- und Faksimilesendern geliefert werden, gedacht.

Erfindungsgemäß besteht das neue Verfahren darin, daß jede Zeichenfolge oder Zeichenteilfolge des unperiodischen Schlüsselstreifens in je einer Speichervorrichtung unterschiedlichen Fassungsvermögens gespeichert wird, von deren Fassungszahlen keine zwei einen gemeinschaftlichen Teiler haben und wobei die Zeichenanzahl der längsten Folge gleich der Fassungszahl des größten Speichers ist, daß jede gespeicherte Zeichenfolge aus einer beliebig wählbaren relativen Ausgangsstellung der Speichervorrichtungen zueinander periodisch wiederkehrend mit gleicher Zeichengeschwindigkeit je mehreren Abfragevorrichtungen angeboten wird, die mit den entsprechenden Abfragevorrichtungen der übrigen Speichervorrichtungen zu n Querabfragesystemen von je n Abfragevorrichtungen zusammengefaßt sind, deren jedes je einer Abtastvorrichtung für jede Speichervorrichtung zugeordnet ist, daß jedes Querabfragesystem auf je zwei voneinander verschiedene Querzeichenkombinationen (Codegruppen) von je n Zeichen eingestellt ist und diese aus den gespeicherten Zeichenfolgen auswählt, derart, daß die Abfrage der ersten eingestellten Zeichenkombination (Codegruppe) die dem betreffenden Ab-

fragesystem zugeordnete Abtastvorrichtung veranlaßt, unwirksam zu werden und so lange zu bleiben, als dieselbe Zeichenkombination (Codegruppe) oder andere, von der zweiten verschiedene Zeichenkombinationen abgefragt werden, und die Abfrage der zweiten Zeichenkombination die Abtastvorrichtung veranlaßt, wirksam zu werden und so lange zu bleiben, als dieselbe Zeichenkombination (Codegruppe) oder andere, von der ersten verschiedene Zeichenkombinationen (Codegruppen) abgefragt werden, daß die Zeichen jeder abgetasteten Zeichenkombination nach einem Pyramidenschema so lange multiplikativ miteinander überlagert werden, bis pro Kombination nur noch ein einziges Zeichen übrigbleibt, und daß die Überlagerungsergebnisse auf einem Schlüsselstreifen in Form einer einzigen Zeichenfolge registriert werden, der, mit dem Klartextstreifen überlagert, den Geheimtextstreifen ergibt.

Unter einer Zeichenfolge wird dabei die Gesamtheit der in einer Spalte parallel zur Längsausdehnung des Schlüsselstreifens aufeinanderfolgenden Zeichen verstanden. Teilerfremde Zahlen sind Zahlen, von denen keine zwei einen gemeinschaftlichen Teiler haben.

Nach einem weiteren Erfindungsgedanken wird das Verfahren gemäß der Erfindung durch eine Vorrichtung durchgeführt, die darin besteht, daß die Speichervorrichtungen als rotierende Scheiben ausgebildet sind, die in beliebige relative Ausgangsstellungen zueinander gebracht werden können, in denen sie einrasten, auf deren Umfängen ferromagnetische Schichten aufgebracht sind, auf denen die binären Zeichen der einzelnen Folgen des unperiodischen kurzen Schlüsselstreifens magnetisch gespeichert sind, und daß die Speicherscheiben mit verschiedenen Geschwindigkeiten rotieren, die sich wie teilerfremde Zahlen verhalten, jedoch derart, daß ein Zeichenschritt von allen Scheiben zugleich ausgeführt wird.

Mehrere gesetzlose Zeichenfolgen mit statistischer Gleichverteilung zweier binärer Zeichen, wie z. B. Loch und kein Loch, eines kurzen unperiodischen Schlüsselstreifens werden abgetastet und auf den Umfängen von koaxialen Speicherscheiben, deren Anzahl gleich der Anzahl der Zeichenfolgen des unperiodischen Schlüsselstreifens ist, gespeichert. Für den Erfindungsgedanken ist es gleichgültig, ob die Zeichenfolgen des unperiodischen Schlüsselstreifens auf den Speicherscheiben nach irgendeinem bekannten Verfahren magnetisch, elektrostatisch, optisch oder mechanisch gespeichert werden. Jeder Speicher hat ein Fassungsvermögen für eine Anzahl von Zeichen, die nicht gerade gleich der Anzahl der Zeichen einer Zeichenfolge zu sein braucht. Jedoch ist die Zeichenanzahl, die der größte Speicher aufzunehmen vermag, gleich der Zeichenanzahl der längsten Zeichenfolge des unperiodischen Schlüsselstreifens. Die Anzahlen der Zeichen, die auf jedem der Speicher untergebracht werden können, verhalten sich zueinander wie teilerfremde Zahlen. Die einzelnen Speicherscheiben werden über verschiedene Zahnradübersetzungen angetrieben, deren Übersetzungsverhältnisse sich ebenfalls wie teilerfremde Zahlen zueinander verhalten, jedoch derart, daß, wenn eine Scheibe sich um einen Zeichenschritt weiterbewegt, alle übrigen Scheiben sich ebenfalls um je einen Schritt weiterbewegen, so daß quer zu den Scheiben wechselnde Zeichenkombinationen entstehen, wobei jede Kombination so viele Zeichen enthält, wie Scheiben vorhanden sind. Wird eine relative Ausgangslage der Scheiben zueinander definiert und das Scheibensystem in Rotation versetzt, so kehrt dieselbe Ausgangslage der Scheiben erstmalig nach

einer Anzahl von Schritten wieder, die gleich dem Produkt der Schrittanzahlen aller Scheiben ist. Diese Schrittzahl ist die Periode des Scheibensystems.

Durch mehrere Systeme von Abfragevorrichtungen quer zu den rotierenden Scheiben, wobei so viele Systeme wie Scheiben vorhanden sind und jedes System so viele Abfragevorrichtungen wie Scheiben enthält, werden die wechselnden Zeichenkombinationen quer zu den Scheiben abgefragt. Jedes Abfragesystem ist mit einer Schaltvorrichtung verbunden, die einen Kontakt öffnet, wenn eine vorher vereinbarte Zeichenkombination abgetastet wird, und diesen Kontakt wieder schließt, wenn eine andere vorher vereinbarte Zeichenkombination abgetastet wird. Das Auftreten dieser Zeichenkombinationen wird zwar gesetzmäßig, aber völlig unregelmäßig und unperiodisch innerhalb der Periode des Scheibensystems sein. Durch die bekannte Querabfrage werden aus der Periode des Scheibensystems einzelne Schritte herausgegriffen, die zum Verschlüsseln verwendet werden können. Die Periode dieser Schritte ist zwar kleiner als die Periode des Scheibensystems, jedoch mathematisch sehr schwer zu rekonstruieren.

Vor den Umfängen der Scheiben ist ein weiteres System von Abtastvorrichtungen angebracht, wobei die Anzahl der Abtastvorrichtungen ebenfalls wieder gleich der Scheibenanzahl ist. Jeder Abtastvorrichtung ist ein Abfragesystem zugeordnet. Das Abtastsystem wird durch die Abfragesysteme in der Weise beeinflußt, daß, wenn die Schaltvorrichtung eines Abfragesystems ihren Kontakt öffnet, die zugeordnete Abtastvorrichtung ausgeschaltet wird und, wenn die Schaltvorrichtung den Kontakt schließt, die zugeordnete Abtastvorrichtung wieder eingeschaltet wird, jedoch derart, daß niemals mehr als zwei der Abtastvorrichtungen gleichzeitig ausgeschaltet sein können. Es sind also mindestens drei Abtastvorrichtungen des Abtastsystems immer eingeschaltet. Das Abtastsystem tastet laufend Zeichenkombinationen ab, die mindestens aus drei Zeichen bestehen.

In einer weiteren Vorrichtung werden in bekannter Weise die Zeichen der von den Abtastvorrichtungen abgetasteten Zeichenkombinationen, z. B. entsprechend den algebraischen Vorzeichenregeln der Multiplikation, durch Bildung von Paarungen nach einem Pyramidenschema mehrfach miteinander multiplikativ überlagert, und zwar so lange, bis als Ergebnis pro abgetasteter Zeichenkombination ein einziges Zeichen übriggeblieben ist. Auf diese Weise wird eine Zeichenfolge erhalten, die den Schlüsselstreifen mit sehr langer Periode bildet und mit dem der Klartextstreifen, der aus den Zeichenfolgen der zu übertragenden Informationen eines Hell- oder Faksimilesenders besteht, in einer weiteren Vorrichtung in bekannter Weise multiplikativ überlagert wird. Das Ergebnis der Verschlüsselung ist ein Geheimtextstreifen, der als Lochstreifen hergestellt werden kann und gleichzeitig während seiner Herstellung oder später durch einen Lochstreifensender ausgesendet wird.

Als Verschlüsselungsmittel dienen die nachfolgend aufgeführten Vorrichtungen:

1. Verwendeter unperiodischer Schlüsselstreifen für die Speicherung,
2. relative Ausgangsstellungen der verschiedenen Speicherscheiben,
3. Einstellung der Abfragesysteme auf je zwei verschiedene Zeichenkombinationen,
4. Zuordnung der Abfragesysteme zu den Abtastvorrichtungen,

5. Einstellung der wieder einzuschaltenden ausgeschalteten Abtastvorrichtungen,
6. Art der Überlagerung der Zeichen aus den Abtastvorrichtungen,
7. Art der Überlagerung des Schlüsselstreifens mit dem Klartextstreifen.

In den Fig. 1 bis 7 ist ein Ausführungsbeispiel zur näheren Erläuterung der Erfindung dargestellt.

Fig. 1 zeigt die Anordnung der Speicherscheiben mit dem Aufsprechsystem, dem Abtastsystem und einem Abfragesystem;

Fig. 2 zeigt eine Speicherscheibe mit den zugehörigen Aufsprech-, Lösch-, Abfrage- und Abtastköpfen in Seitenansicht; in

Fig. 3 ist das Prinzip der Erfindung schematisch dargestellt; in

Fig. 4 und 5 sind zwei verschiedene Schaltungen für die Auswahl der gewählten Zeichenkombinationen dargestellt;

Fig. 6 zeigt eine Schaltungsanordnung zum Wiedereinschalten ausgeschalteter Abtastköpfe;

Fig. 7 zeigt die Multiplikationsschaltung des Abtastsystems und die Überlagerung des Schlüssel- mit dem Klartextstreifen.

In Fig. 1 bedeuten **1** bis **5** koaxiale Speicherscheiben, die auf ihren Umfängen mit ferromagnetischen Schichten versehen und drehbar auf der Achse **6** angeordnet sind. Die fünf Speicherscheiben sind mit je einem der fünf Zahnräder **7** bis **11** starr verbunden, die mit den Zahnrädern **12** bis **16** im Eingriff stehen. Die letzteren sind auf der Welle **17** befestigt, die über ein Untersetzungsgetriebe, bestehend aus den beiden Zahnrädern **18** und **19**, durch den Motor **20** angetrieben wird. Die Speicherscheiben haben unterschiedliche Fassungszahlen, die sich wie zueinander teilerfremde Zahlen verhalten. Die Zahnradübersetzungen verhalten sich ebenfalls wie teilerfremde Zahlen und sind so gewählt, daß, wenn eine Scheibe einen Zeichenschritt ausführt, alle übrigen Scheiben ebenfalls einen Zeichenschritt ausführen.

21 ist ein Ausschnitt aus dem unperiodischen Schlüsselstreifen, auf dem fünf gesetzlose Zeichenfolgen in Form eines Fünfer-Loch-Codes aufgebracht sind. **22** ist eine Abtastvorrichtung, z. B. in Form von fünf Schleiffedern, die die Lochzeichen abtasten. In **23** werden die abgetasteten Impulsfolgen verstärkt und in Gleichstrom- oder Wechselstromimpulse umgesetzt. Diese speisen die fünf magnetischen Aufsprechköpfe **24** bis **28**, die die Umfänge der Speicherscheiben entsprechend den abgetasteten Zeichen magnetisieren. Der Papiervorschub wird über geeignet gewählte (nicht gezeigte) Übersetzungen durch den Motor **20** angetrieben. Bei der Speicherscheibe mit dem größten Fassungsvermögen ist der Umfang in so viele Teile geteilt, wie die längste Zeichenfolge des unperiodischen Schlüsselstreifens Zeichen enthält. Entsprechend sind die Umfangseinteilungen der übrigen Speicherscheiben gleich den teilerfremden Zeichenzahlen der übrigen Zeichenfolgen. Alle Speicherscheiben können in beliebige Ausgangsstellungen gedreht werden, in denen sie einrasten.

29 bis **33** sind fünf magnetische Wiedergabeköpfe, die eines der fünf Abfragesysteme bilden. Die übrigen vier Abfragesysteme sind der Übersichtlichkeit halber nicht gezeichnet. Die fünf Abfragesysteme sind beliebig auf den Umfängen der Scheiben verteilt, und die Wiedergabeköpfe eines Abfragesystems brauchen nicht quer zu den Scheiben in einer Flucht zu liegen, sondern können winkelmäßig gegeneinander versetzt sein.

Vor den Umfängen der Scheiben und quer zu diesen ist noch ein achtes System, das Abtastsystem, angeordnet, das ebenfalls aus fünf Wiedergabeköpfen **34** bis **38** besteht und das die wechselnden Impulskombinationen quer zu den Scheiben abtastet. Die fünf Wiedergabeköpfe dieses Systems können ebenfalls winkelmäßig gegeneinander versetzt sein.

In Fig. 2 ist eine Scheibe des Scheibensystems mit den acht auf ihrem Umfang (nicht notwendigerweise gleichmäßig) verteilten Köpfen der fünf Abfragesysteme I bis V, des Aufsprechsystems VI, des Löschsystems VII und des Abtastsystems VIII in Seitenansicht dargestellt.

In Fig. 3 ist das Prinzip des Erfindungsgedankens schematisch dargestellt. I bis V bedeuten die fünf Abfragesysteme mit je fünf Abfrageköpfen *a*, *b*, *c*, *d*, *e*. Jedes dieser Abfragesysteme kann auf je zwei andere, voneinander verschiedene Zeichenkombinationen eingestellt werden, z. B. das System I auf $++--+$ und $-+-+-$, derart, daß, wenn die erste Zeichenkombination abgefragt wird, ein Kontakt sich öffnet und so lange geöffnet bleibt, bis die zweite Kombination abgefragt wird. Ist dies der Fall, so schließt sich der Kontakt und bleibt so lange geschlossen, bis wieder die erste Zeichenkombination abgetastet wird, usw. Jeder Kontakt der fünf Abfragesysteme I bis V schaltet je einen Abtastkopf des Abtastsystems VIII je nach den anliegenden Zeichenkombinationen aus und ein, z. B. der Kontakt des Abfragesystems I den Abtastkopf *a*, der Kontakt des Systems II den Kopf *b*, der Kontakt des Systems III den Kopf *c*, der Kontakt des Systems IV den Kopf *d* und der Kontakt des Systems V den Kopf *e* des Abtastsystems VIII. Die Köpfe dieses Systems tasten also nur dann die auf den Scheiben anliegenden Zeichenkombinationen ab, wenn sie eingeschaltet sind, wobei die Ein- und Ausschaltung durch die fünf Abfragesysteme gesteuert wird.

Die abgetasteten Zeichen werden hierauf in einer Überlagerungsvorrichtung, z. B. gemäß den algebraischen Vorzeichenregeln der Multiplikation, nach einem Pyramidenschema paarweise multiplikativ miteinander überlagert, z. B. die Zeichen des Kopfes *a* mit den Zeichen des Kopfes *b*, *c* mit *d*, die Produkte *ab* mit *cd* und das Produkt *abcd* mit *e*. Ist ein Abtastkopf abgeschaltet, so soll dies bei der Überlagerung damit gleichbedeutend sein, als ob er eingeschaltet wäre und Minus abtasten würde.

In Fig. 4 ist eine Auswählschaltung für die eingestellten beiden Zeichenkombinationen eines Abfragesystems dargestellt.

39 bis **43** sind fünf Relais, deren erstes einen Anker und zwei Kontakte und deren jedes folgende doppelt so viele Anker und Kontakte wie das vorhergehende hat. Die Kontakte jedes Relais sind an die Anker des folgenden Relais angeschlossen, so daß die Relais eine baumartige Verzweigung bilden. Die zweiunddreißig Kontakte des fünften Relais **43** sind an die Kontakte des Drehschalters **44** geführt, auf dem mittels zweier Schleifkurbeln oder Schieber **45** und **46** zwei verschiedene Fünfer-Zeichenkombinationen eingestellt werden können. An den zweiunddreißig Kontakten können alle überhaupt nur möglichen Zeichenkombinationen abgegriffen werden.

Die beiden Schleifkurbeln **45** und **46** sind über die Relaisspule **47** miteinander verbunden. Der Mittelabgriff **48** der Relaisspule ist über die Batterie **49** an den Anker des Relais **39** angeschlossen. Das polarisierte Relais **50** mit neutraler Ruhelage des Ankers kann den Abtastkopf **34** ein- und ausschalten. Die

fünf Relaisspulen **51** bis **55** sind über (nicht gezeigte) Verstärker, Gleichrichter und Siebglieder an die Abfrageköpfe **29** bis **33** der Fig. 1 angeschlossen. Nur dann, wenn die erste eingestellte Zeichenkombination, z. B. ++−−+, gerade abgefragt wird, legen sich die Ankergruppen der Relais **39** bis **43** in solche Stellungen, daß sie nach der Kurbel **46** durchgeschaltet sind. Die rechte Hälfte der Relaisspule **47** erhält dann Strom und bewirkt das Umlegen des Ankers des Relais **50** beispielsweise nach links, wodurch die eine Zuleitung **56** zum Abtastkopf **34** unterbrochen, d. h. der Kopf ausgeschaltet wird. Werden durch die Abfrageköpfe jetzt die erste eingestellte Zeichenkombination oder andere, von der zweiten verschiedene Zeichenkombinationen abgefragt, so ist kein Durchgang der Relais **39** bis **43** mehr vorhanden, die Relaisspule **47** wird stromlos, der Anker **50** bleibt in seiner letzten Stellung stehen, und der Kopf **34** bleibt ausgeschaltet. Wird die zweite mittels der Kurbel **45** eingestellte Zeichenkombination, z. B. −+−+−, abgefragt, so legen sich die Ankergruppen **39** bis **43** in solche Stellungen, daß sie nach der Kurbel **45** durchgeschaltet sind. Die linke Hälfte der Relaisspule **47** erhält jetzt über die Batterie **49** Strom in entgegengesetzter Richtung und bewirkt das Umlegen des Relaisankers **50** nach rechts, wodurch die Zuleitung **56** zum Abtastkopf **34** geschlossen, d. h. der Kopf eingeschaltet wird. Werden durch die Abfrageköpfe jetzt die gleiche Zeichenkombination oder andere, von der ersten verschiedene Zeichenkombinationen abgetastet, so bleibt der Abtastkopf so lange eingeschaltet, bis wieder einmal die erste eingestellte Zeichenkombination abgefragt wird, wodurch der Abtastkopf wieder ausgeschaltet wird, usw. Die beschriebene Relaisanordnung ist fünfmal vorhanden, und zwar je einmal für jedes Abfragesystem. Der Vorteil dieser Relaisanordnung liegt in der einfachen Einstellung der beiden Zeichenkombinationen durch Drehen zweier Schleifkurbeln, der Nachteil in der großen Anzahl von Relaiskontakten.

Eine andere Auswählschaltung ist in Fig. 5 dargestellt. **57** bis **61** sind fünf Doppelrelais, **62** bis **66** sind die zugehörigen fünf Relaisspulen, die über (nicht gezeigte) Verstärker, Gleichrichter und Siebglieder an die Abfrageköpfe **29** bis **33** eines Abfragesystems angeschlossen sind. Die Relais sind in Reihe geschaltet, d. h., jeder Relaisanker ist mit einem der beiden Kontakte des vorangehenden Relaisankers verbunden. **67** ist ein polarisiertes Relais mit neutraler Ruhelage des Ankers, **68** die zugehörige Relaisspule mit Mittelabgriff **69**. Einer der beiden oberen Kontakte des Relais **61** ist über die Spule **68** mit einem der beiden unteren Kontakte des Relais **61** verbunden. Die beiden parallel geschalteten Anker des Relais **57** sind über die Batterie **70** an den Mittelabgriff **69** angeschlossen. Es werden angenommen, daß, wenn die Relaisspulen **62** bis **66** Strom erhalten, die Anker sich nach oben umlegen. Wenn durch Stecken von Brücken **71** bis **75** und **76** bis **80** zwischen jedem Relaisanker und einem der beiden Kontakte des vorangehenden Relaisankers zwei vereinbarte Zeichenkombinationen, z. B. ++−−+ und −+−+−, eingestellt sind, werden nur dann, wenn diese Zeichenkombination durch das Abfragesystem abgefragt werden, die oberen bzw. unteren Relaisanker durchgeschaltet. Die Relaisspule **68** erhält dann über die Batterie **70** in der einen bzw. entgegengesetzten Richtung Strom, und der Relaisanker **67** öffnet bzw. schließt die eine Zuleitung **96** nach dem Abtastkopf **34**. Werden durch die Abfrageköpfe die erste eingestellte Zeichenkombination oder andere, von der zweiten verschiedene Zeichenkombinationen abgefragt, so bleibt der Abtastkopf so lange aus- bzw. eingeschaltet, bis die zweite eingestellte Zeichenkombination abgefragt wird, wodurch der Abtastkopf wieder ein- bzw. ausgeschaltet wird, usw.

Die beschriebene Relaisanordnung ist fünfmal vorhanden, und zwar je einmal für jedes Abfragesystem. Der Vorteil dieser Relaisanordnung liegt in der geringeren Anzahl von Kontakten, der Nachteil in der umständlichen Einstellung der vereinbarten Zeichenkombinationen durch Stecken von fünfzig Brücken.

Bei den in den Fig. 4 und 5 beschriebenen beiden Schaltanordnungen zum Aus- und Einschalten der Abtastköpfe **34** bis **38**, die durch die fünf Abfragesysteme gesteuert werden, kann es vorkommen, daß drei, vier oder fünf Abtastköpfe gleichzeitig ausgeschaltet werden. Aus Sicherheitsgründen in verschlüsselungstechnischer Hinsicht sollen aber niemals mehr als zwei Köpfe gleichzeitig ausgeschaltet werden können, d. h. also immer mindesens drei Köpfe eingeschaltet bleiben. Eine Schaltungsanordnung zur Erfüllung dieser Forderung ist in Fig. 6 dargestellt.

Auf der rechten Seite sind die sechzehn verschiedenen Möglichkeiten, die mit 1 bis 16 numeriert sind, angegeben, bei denen von den fünf Abtastköpfen mindestens drei ausgeschaltet sind. Und zwar gibt es zehn Möglichkeiten, daß drei Köpfe, fünf Möglichkeiten, daß vier Köpfe, und eine Möglichkeit, daß alle fünf Köpfe gleichzeitig ausgeschaltet sind. »Eingeschaltet« ist durch das Zeichen »+«, »ausgeschaltet« durch das Zeichen »−« gekennzeichnet. Sind drei Köpfe ausgeschaltet, so muß von diesen ein Kopf, sind vier Köpfe ausgeschaltet, so müssen von diesen zwei Köpfe, sind alle fünf Köpfe ausgeschaltet, so müssen von diesen drei Köpfe wieder eingeschaltet werden.

81 bis **85** sind die Relaisspulen von fünf polarisierten Relais **86** bis **90**, deren Anker **91** bis **95** zum Öffnen und Schließen der Zuleitungen **96** bis **100** zu den fünf Abtastköpfen **34** bis **38** dienen. Hierbei ist die Relaisspule **81** mit den Relaisspulen **47** aus Fig. 4 bzw. **68** aus Fig. 5 und das polarisierte Relais **86** (mit dem Anker **91**) mit den polarisierten Relais **50** aus Fig. 4 bzw. **67** aus Fig. 5 identisch. Bei den Relais **86** bis **90** sind die Kontakte jedes Relais an die Anker (mit Ausnahme der Anker **91** bis **95**) des folgenden Relais angeschlossen, so daß die Relaisanker eine baumartige Verzweigung bilden, ähnlich wie bei der Auswählschaltung nach Fig. 4. Von den zweiunddreißig Durchschaltmöglichkeiten sind jedoch sechzehn weggelassen, und zwar alle diejenigen, deren entsprechende Zeichenkombinationen mindestens drei »Ein« (Plus) aufzuweisen haben. Sechzehn Kontakte des Relais **90** sind an die Anfänge der Relaisspulen **101** bis **116** geführt. Die Enden der sechzehn Relaisspulen sind parallel geschaltet und über die Batterie **117** an den Anker **118** des Relais **86** angeschlossen. Die hierdurch gegebenen sechzehn Durchschaltmöglichkeiten entsprechen den sechzehn möglichen Zeichenkombinationen, die mindestens drei »Aus« (Minus) enthalten. Die sechzehn Relaisspulen **101** bis **116** gehören zu den sechzehn Relais **119** bis **134**. Von diesen sechzehn Relais haben zehn, nämlich **119**, **120**, **121**, **122**, **124**, **126**, **128**, **129**, **131**, je einen Anker entsprechend den Ein-Aus-Kombinationen **1**, **2**, **3**, **4**, **6**, **7**, **8**, **10**, **11**, **13**, fünf Relais, nämlich **123**, **127**, **130**, **132**, **133**, haben je einen Doppelanker entsprechend den Ein-Aus-Kombinationen **5**, **9**, **12**, **14**, **15**, und ein

Relais, nämlich **134**, hat einen Dreifachanker entsprechend der Ein-Aus-Kombination **16**. Die Relais **119** bis **134** sind so in die Zuleitungen **96** bis **100** der Abtastköpfe **34** bis **38** geschaltet, daß sie, wenn drei Köpfe durch die Abfragesysteme ausgeschaltet werden, einen Kopf, wenn vier Köpfe ausgeschaltet werden, zwei Köpfe, und wenn fünf Köpfe ausgeschaltet werden, drei Köpfe wieder einschalten, wobei vereinbart werden muß, welche von den ausgeschalteten Köpfen wieder eingeschaltet werden sollen, wofür es eine sehr große Anzahl von Möglichkeiten gibt. In dem Wechsel dieser Möglichkeiten liegt eine weitere Variante zur Verschlüsselung.

Je nachdem, was für eine Ein-Aus-Kombination der Abtastköpfe **34** bis **38** auf Grund der Steuerung durch die fünf Abfragesysteme gerade vorliegt, werden sich die Ankergruppen der Relais **86** bis **90** in die entsprechenden Stellungen legen, wobei die Anker **91** bis **95** die Ein- und Ausschaltung der Abtastköpfe vornehmen. Bei denjenigen sechzehn Ein-Aus-Kombinationen, die nicht mehr als zwei »Aus« enthalten, ist kein Durchgang vom Anker **118** nach einer der sechzehn Relaisspulen **101** bis **116** vorhanden. Bei den anderen sechzehn Ein-Aus-Kombinationen, die mindestens drei »Aus« enthalten, ist jeweils der Anker **118** zu einer der sechzehn Relaisspulen **101** bis **116** durchgeschaltet, und es ist Stromdurchgang vorhanden. Das zu der betreffenden Relaisspule gehörende Relais legt seinen oder seine Anker um und schaltet einen, zwei oder drei der abgeschalteten Abtastköpfe wieder ein.

In Fig. 7 ist eine Schaltungsanordnung zur Überlagerung der Zeichen der abgetasteten Fünfer-Zeichenkombinationen angegeben. **34** bis **38** sind die fünf Abtastköpfe der Abtastvorrichtung, die über (nicht gezeigte) Verstärker, Gleichrichter und Siebglieder an die Relaisspulen **135** bis **139** angeschlossen sind. **140** bis **144** sind die zugehörigen Relaisdoppelanker. **96** bis **100** sind die Zuleitungen zu den Abtastköpfen **34** bis **38**, die durch die Relaisanker **91** bis **95** nach Fig. 6 aus- und eingeschaltet werden. Die Überlagerung der Zeichen geht nach dem Pyramidenschema der Fig. 2 vor sich. Es werde angenommen, daß, entsprechend den algebraischen Vorzeichenregeln der Multiplikation,

$$+\times+=+,\quad -\times-=+,\quad +\times-=-,\quad -\times+=-$$

ergeben soll. Wird von **34** und **35** Plus abgetastet, so erhalten **135** und **136** Strom, und **140** und **141** legen nach oben um. Die unteren Relaisanker sind durchgeschaltet, und **145** erhält über die Batterie **146** Strom (Plus). Wird von **34** und **35** Minus abgetastet, so bleiben **135** und **136** stromlos, und **140** und **141** legen nach unten um. Die oberen Relaisanker sind jetzt durchgeschaltet, und **145** erhält über die Batterie **146** Strom (Plus). Wird von **34** Plus und von **35** Minus abgetastet, so erhält **135** Strom, und **136** bleibt stromlos. **140** legt nach oben und **141** nach unten um. Zwischen beiden Relais ist kein Durchgang vorhanden, und **145** bleibt stromlos (Minus). Wird endlich von **34** Minus und von **35** Plus abgetastet, so bleibt **135** stromlos, und **136** erhält Strom. **140** legt nach unten und **141** nach oben um. Zwischen beiden Relais ist kein Durchgang vorhanden, und **145** bleibt stromlos (Minus). In derselben Weise werden mittels der Relais **142** und **143** über die Batterie **147** und die Relaisspule **148** die Zeichen aus den Abtastköpfen **36** und **37** überlagert. Die entstandenen beiden Produktzeichen werden in derselben Weise in der Relaisanordnung **149** bis **152** miteinander überlagert. Schließlich wird mittels der beiden Relais **153** und **144** über die Batterie **154** und den Schaltteil **155** das resultierende Produktzeichen mit dem Zeichen aus dem Abtastkopf **38** überlagert. Bei den Überlagerungen wirkt ein abgeschalteter Abtastkopf so, als ob er eingeschaltet wäre und Minus abtasten würde. In den zahlreichen Möglichkeiten, die Abtastköpfe zur Produktbildung zu paaren, liegt eine weitere Variante zum Verschlüsseln.

155 ist ein elektromagnetischer Streifenlocher, der mittels des Stanzstempels **156** die abgetasteten Produktzeichen in den Papierstreifen **157** stanzt, der von der Papierrolle **158** abläuft. **159** bis **162** sind vier Transportrollen, von denen die Rolle **162** über das Schneckenrad **163** und die Zahnräder **164**, **165** durch den Motor **20** angetrieben wird. Der Schlüsselstreifen **166** wird mit dem Klartextstreifen **167** in der Überlagerungsvorrichtung **168** in bekannter Weise überlagert. Die als Überlagerungsergebnis erhaltenen Geheimzeichen werden auf den Geheimtextstreifen **169** gestanzt und auf die Fernleitung **170** gegeben.

Alle beschriebenen Relaisschaltungen stellen nur Ausführungsbeispiele dar und lassen sich in mannigfacher Weise abändern. Grundsätzlich können sie durch Schaltungen mit gittergesteuerten Hochvakuumröhren oder Transistoren oder gasgefüllten Stromtoren ersetzt werden.

Patentansprüche:

1. Verfahren zur Herstellung von verlängerten Schlüsselstreifen sehr großer Periode für Schlüsselmaschinen mit einer einzigen Folge von Aufzeichnungen binärer Zeichen zum Verschlüsseln von auf einem Klartextstreifen in Form von binären Zeichen registrierten Impulsfolgen, die den zu übertragenden Informationen eines Hell- oder Faksimilesenders zugeordnet sind, unter Verwendung von unperiodischen Schlüsselstreifen, deren Länge klein gegenüber der Länge der zu verschlüsselnden Klartextstreifen ist, mit einer kleinen Anzahl n ($n = 3$ bis 7) von gesetzlosen, willkürlich gewählten Folgen von Aufzeichnungen der binären Zeichen mit ungefähr statistischer Gleichverteilung dieser beiden Zeichen, wobei die Zeichen der Folgen in n nebeneinanderstehenden Spalten parallel zur Längsausdehnung des Streifens so angeordnet sind, daß sie quer zum Streifen wechselnde Kombinationen zu je n Zeichen (Codegruppen) ergeben, und unter Verwendung von Speicher- und Abfragevorrichtungen nach Patent 1 012 635, dadurch gekennzeichnet, daß jede Zeichenfolge oder Zeichenteilfolge des unperiodischen Schlüsselstreifens in je einer Speichervorrichtung unterschiedlichen Fassungsvermögens gespeichert wird, von deren Fassungszahlen keine zwei einen gemeinschaftlichen Teiler haben und wobei die Zeichenanzahl der längsten Folge gleich der Fassungszahl des größten Speichers ist, daß jede gespeicherte Zeichenfolge aus einer beliebig wählbaren relativen Ausgangsstellung der Speichervorrichtungen zueinander periodisch wiederkehrend mit gleicher Zeichengeschwindigkeit je n Abfragevorrichtungen angeboten wird, die mit den entsprechenden Abfragevorrichtungen der übrigen Speichervorrichtungen zu n Querabfragesystemen von je n Abfragevorrichtungen zusammengefaßt sind, deren jedes je einer Abtastvorrichtung für jede Speichervorrichtung zugeordnet ist, daß jedes Querabfragesystem auf je

909 546/255

zwei voneinander verschiedene Querzeichenkombinationen (Codegruppen) von je n Zeichen eingestellt ist und diese aus den gespeicherten Zeichenfolgen auswählt, derart, daß die Abfrage der ersten eingestellten Zeichenkombination (Codegruppe) die dem betreffenden Abfragesystem zugeordnete Abtastvorrichtung veranlaßt, unwirksam zu werden und so lange zu bleiben, als dieselbe Zeichenkombination (Codegruppe) oder andere, von der zweiten verschiedene Zeichenkombinationen abgefragt werden, und die Abfrage der zweiten Zeichenkombination die Abtastvorrichtung veranlaßt, wirksam zu werden und so lange zu bleiben, als dieselbe Zeichenkombination (Codegruppe) oder andere, von der ersten verschiedene Zeichenkombinationen (Codegruppen) abgefragt werden, daß die Zeichen jeder abgetasteten Zeichenkombination nach einem Pyramidenschema so lange multiplikativ miteinander überlagert werden, bis pro Kombination nur noch ein einziges Zeichen übrigbleibt, und daß die Überlagerungsergebnisse auf einem Schlüsselstreifen in Form einer einzigen Zeichenfolge registriert werden, der, mit dem Klartextstreifen überlagert, den Geheimtextstreifen ergibt.

2. Vorrichtung zur Durchführung des Verfahrens nach Anspruch 1, dadurch gekennzeichnet, daß die Speichervorrichtungen als rotierende Scheiben ausgebildet sind, die in beliebige relative Ausgangsstellungen zueinander gebracht werden können, in denen sie einrasten, auf deren Umfängen ferromagnetische Schichten aufgebracht sind, auf denen die binären Zeichen der einzelnen Folgen des unperiodischen kurzen Schlüsselstreifens magnetisch gespeichert sind, und daß die Speicherscheiben mit verschiedenen Geschwindigkeiten rotieren, die sich wie teilerfremde Zahlen verhalten, jedoch derart, daß ein Zeichenschritt von allen Scheiben zugleich ausgeführt wird.

3. Vorrichtung nach Anspruch 1 und 2, dadurch gekennzeichnet, daß vor den Speicherscheiben Übertragungsvorrichtungen angeordnet sind, durch welche die Zeichenfolge des unperiodischen Schlüsselstreifens auf den Umfängen der Speicherscheiben aufgebracht werden.

4. Vorrichtung nach Anspruch 1 und 2, dadurch gekennzeichnet, daß vor den Speicherscheiben

Löschvorrichtungen angeordnet sind, durch welche die gespeicherten Zeichenfolgen vor dem Aufbringen neuer Zeichenfolgen gelöscht werden.

5. Vorrichtung nach Anspruch 1 und 2, dadurch gekennzeichnet, daß das während des Abfragens von Zeichenkombinationen bei Auftreten zweier voneinander verschiedener, eingestellter Zeichenkombinationen wirksam werdende Steuerorgan aus einem Relaisbaum von n polarisierten Relais besteht, bei dem das erste Relais einen Anker und einen Kontakt und jedes folgende Relais immer doppelt so viele Anker und Kontakte wie das vorhergehende hat.

6. Vorrichtung nach Anspruch 1, 2 und 5, dadurch gekennzeichnet, daß das Steuerorgan aus einer Reihenschaltung von n polarisierten Relais mit Doppelankern besteht.

7. Vorrichtung nach Anspruch 5 und 6, dadurch gekennzeichnet, daß die mechanischen Relais durch elektronische Relais ersetzt sind.

8. Vorrichtung nach Anspruch 1 und 2, dadurch gekennzeichnet, daß Mittel vorgesehen sind, die bewirken, daß bei gleichzeitiger Ausschaltung von mehr als zwei Abtastvorrichtungen ein Steuerorgan wirksam wird, welches die Wiedereinschaltung einer oder mehrerer Abtastvorrichtungen bewirkt.

9. Vorrichtung nach Anspruch 8, dadurch gekennzeichnet, daß das Steuerorgan aus einer sich verzweigenden Kettenschaltung von n polarisierten Relais besteht, bei der jedes folgende Relais immer doppelt so viele Anker und Kontakte wie das vorhergehende hat.

10. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die mechanischen Relais durch elektronische Relais ersetzt sind.

11. Vorrichtung nach Anspruch 1 bis 10, dadurch gekennzeichnet, daß Mittel vorgesehen sind, die bewirken, daß die Zeichen jeder durch die Abtastvorrichtungen abgetasteten Zeichenkombination multiplikativ miteinander überlagert werden.

12. Vorrichtung nach Anspruch 1 bis 11, dadurch gekennzeichnet, daß Mittel vorgesehen sind, die bewirken, daß die Ergebnisse der Zeichenüberlagerung auf einem Streifen in Form einer einzigen Zeichenfolge registriert werden.

Hierzu 2 Blatt Zeichnungen

809 727/219 12. 58
(909 546/255 6. 59)

AUSGABETAG: 2. JULI 1959

DBP 1047837
KL. 21 a¹ 21
INTERNAT. KL. H 04 k

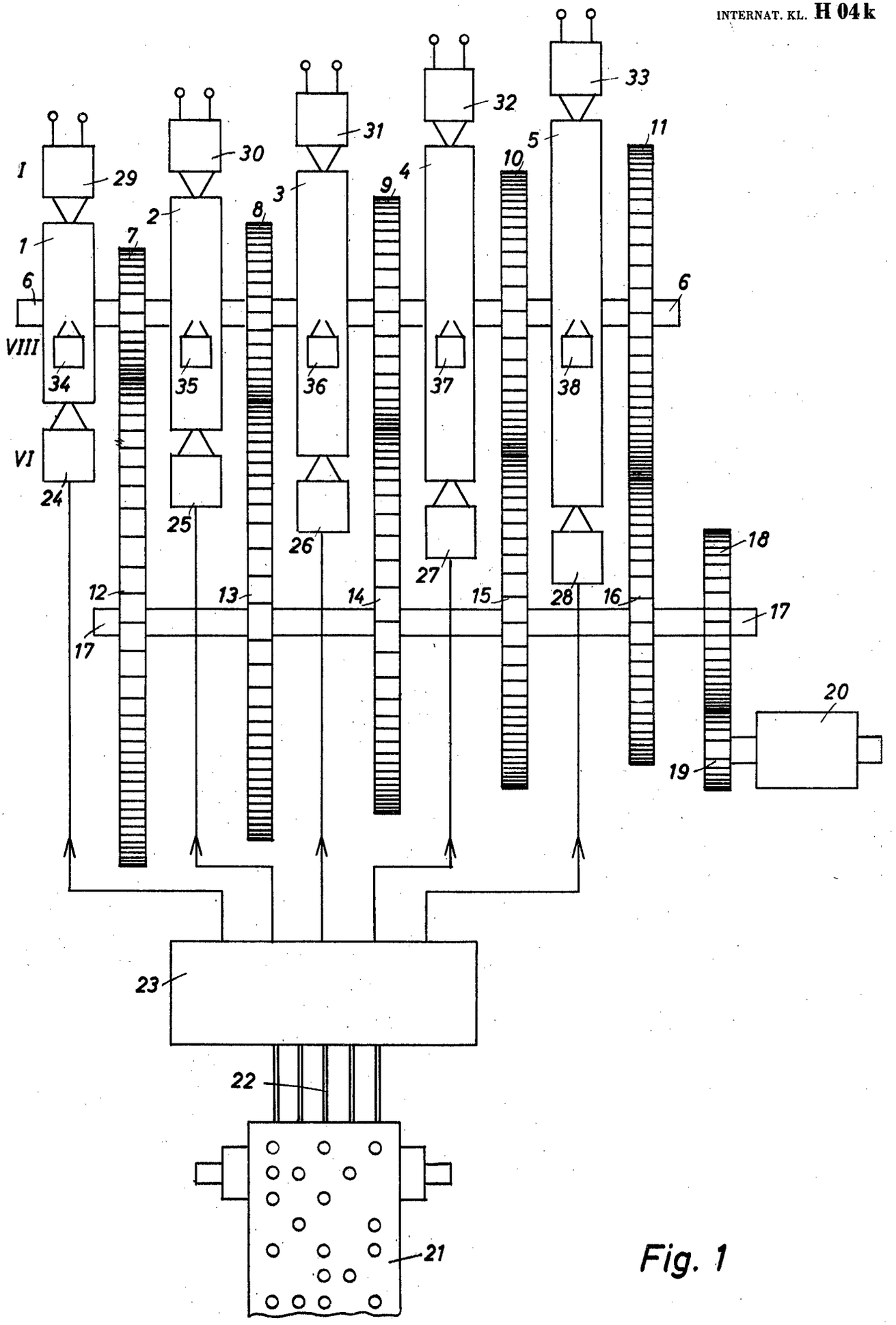


Fig. 1

AUSGABETAG: 2. JULI 1959

DBP 1047837
KL. **21 a1 21**
INTERNAT. KL. **H 04k**

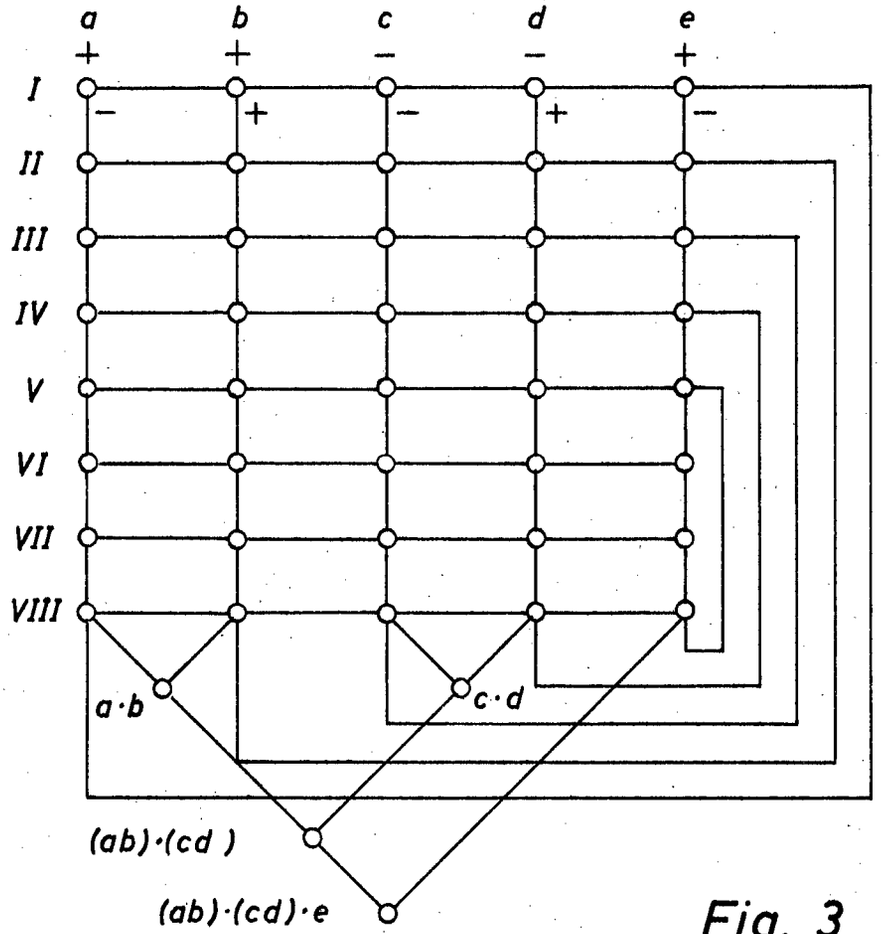


Fig. 3

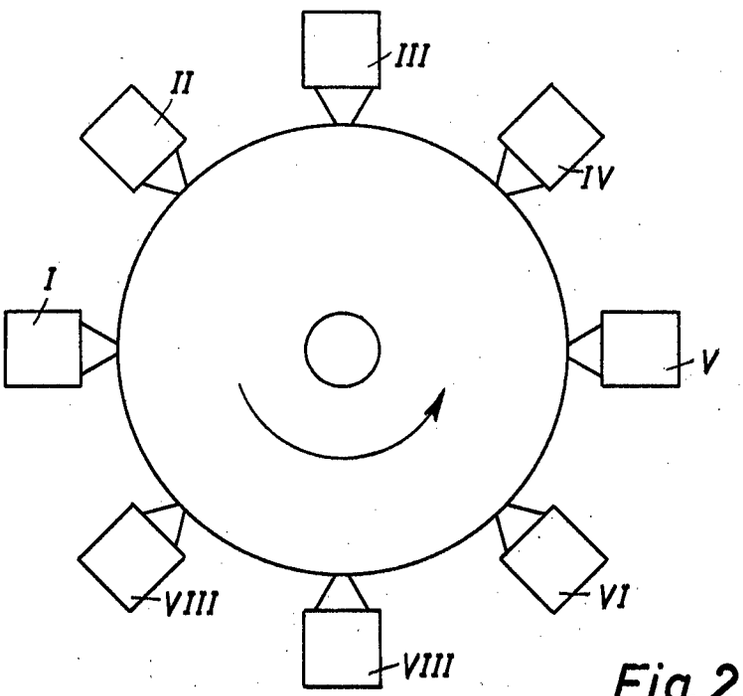


Fig. 2

AUSGABETAG: 2. JULI 1959

DBP 1047837
KL. 21 a1 21
INTERNAT. KL. H 04k

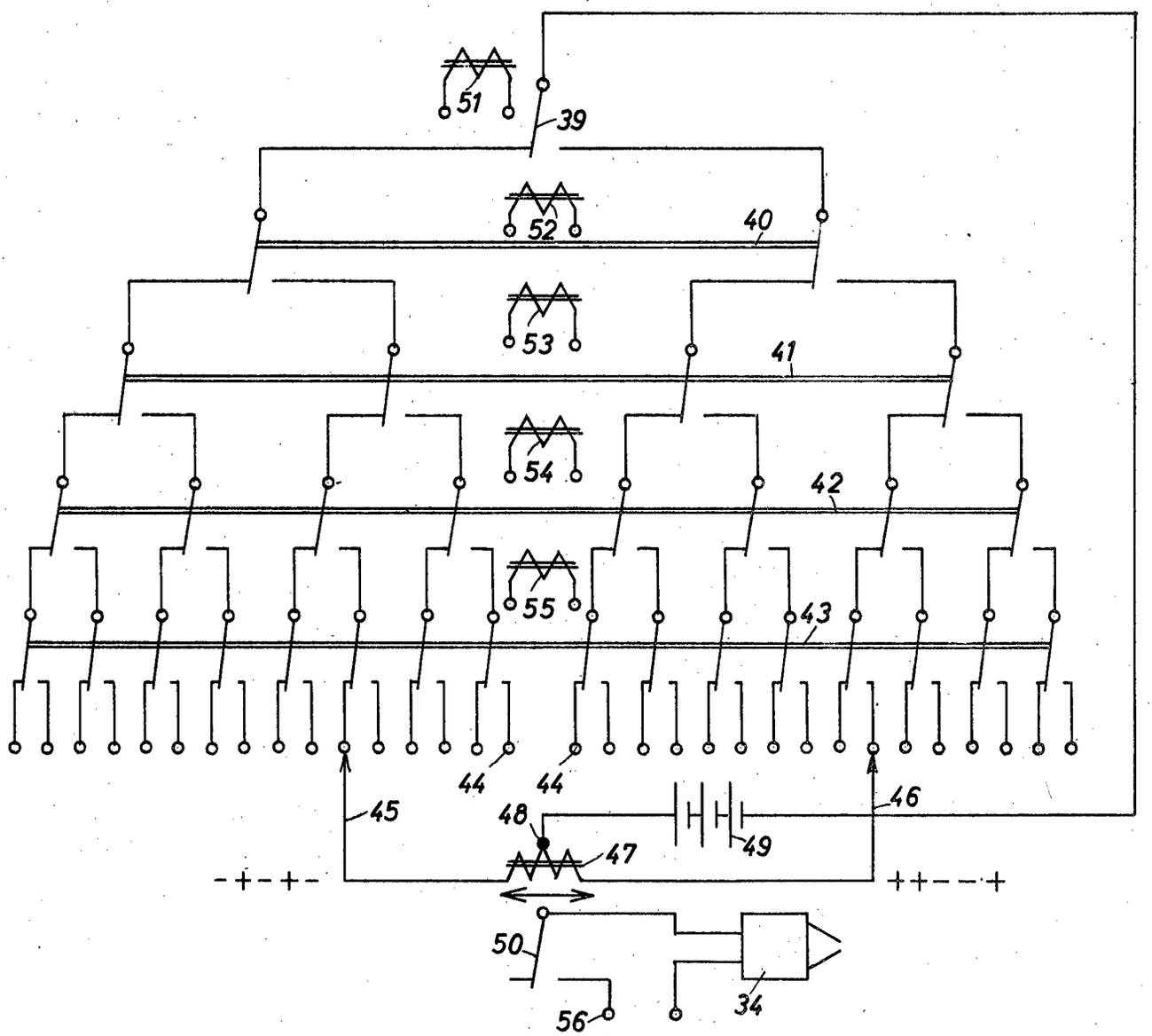


Fig. 4

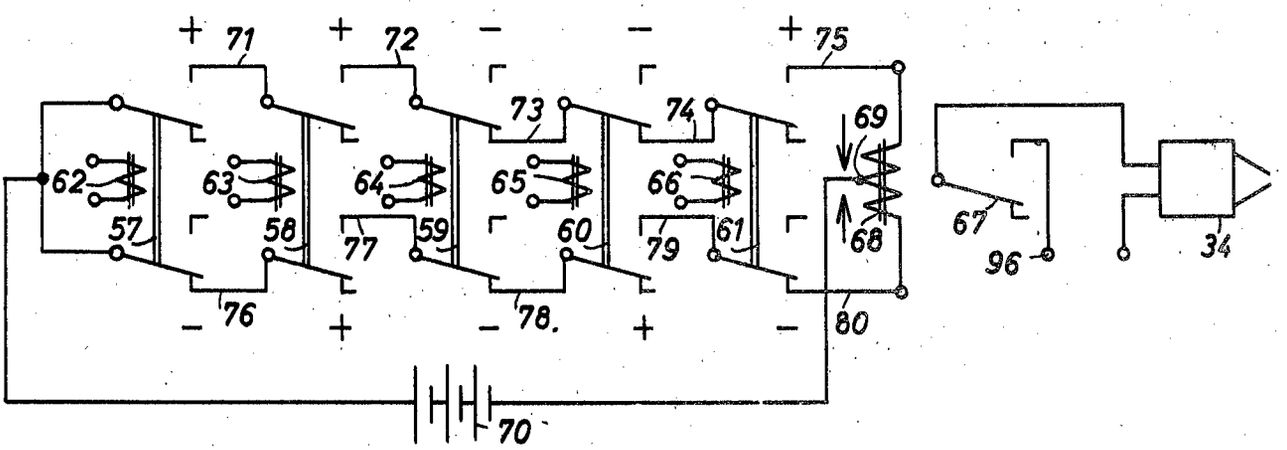


Fig. 5

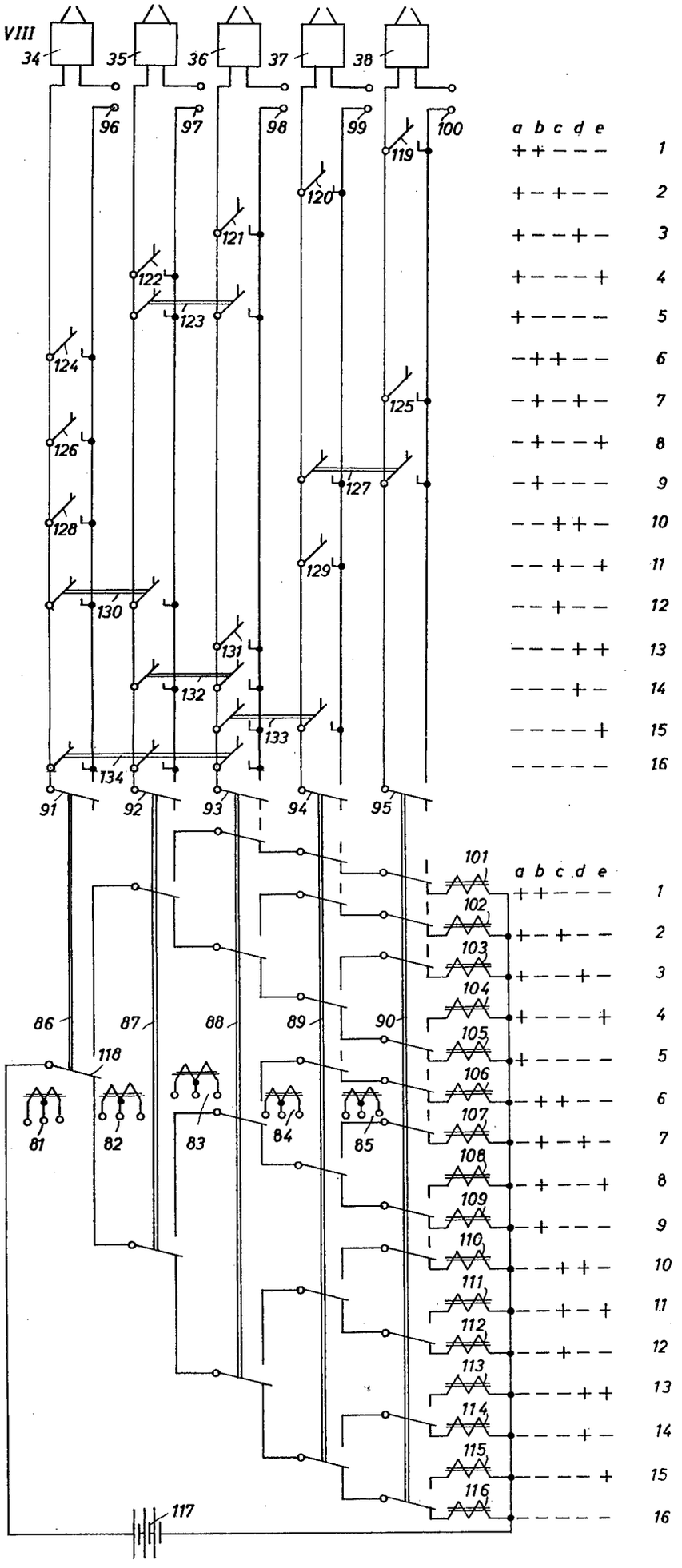
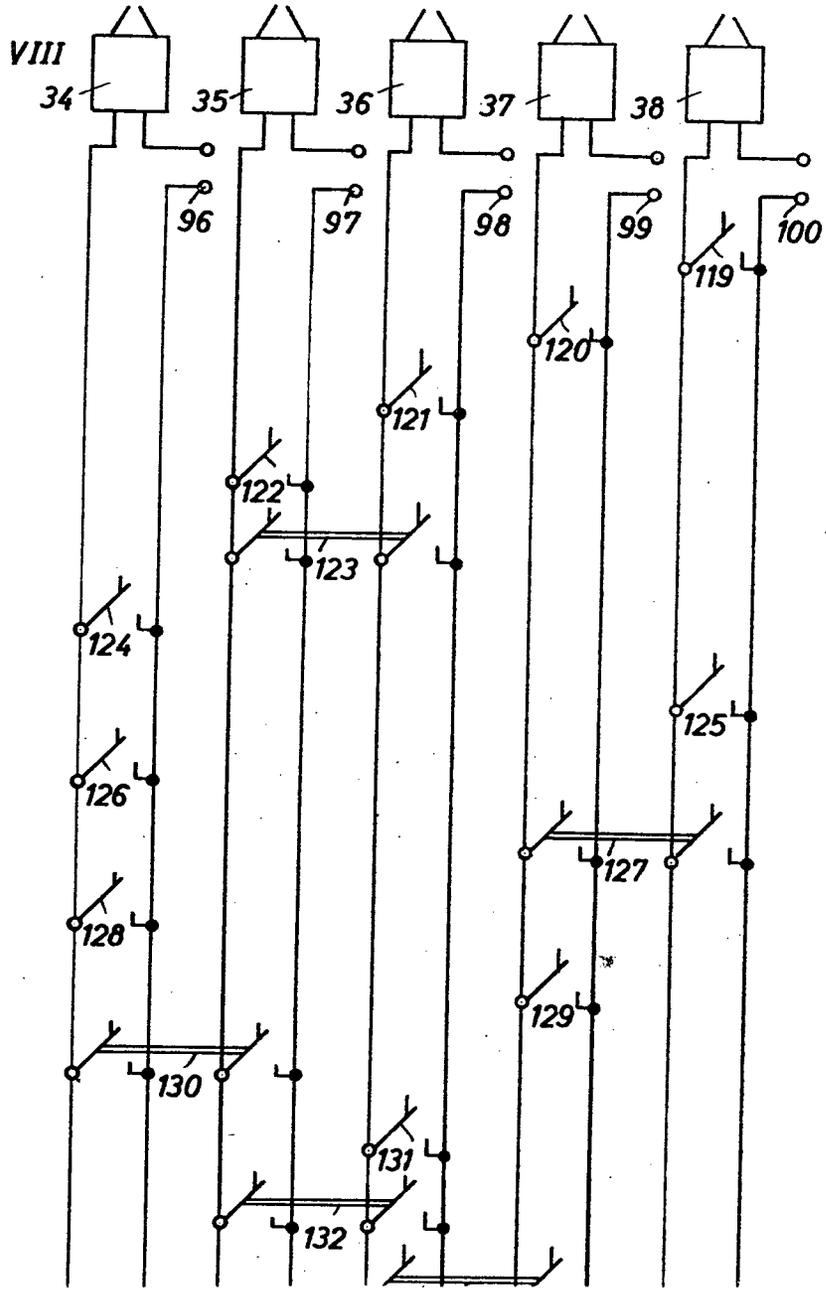


Fig. 6

ZEICHNUNGEN BLATT 2
AUSGABETAG: 2. JULI 1959
DBP 1047837
KL. 21a¹ 21
INTERNAT. KL. H 04k



a	b	c	d	e	
+	+	−	−	−	1
+	−	+	−	−	2
+	−	−	+	−	3
+	−	−	−	+	4
+	−	−	−	−	5
−	+	+	−	−	6
−	+	−	+	−	7
−	+	−	−	+	8
−	+	−	−	−	9
−	−	+	+	−	10
−	−	+	−	+	11
−	−	+	−	−	12
−	−	−	+	+	13
−	−	−	+	−	14

AUSGABETAG: 2. JULI 1959

DBP 1047837
KL. **21 a**[1] 21
INTERNAT. KL. **H 04k**

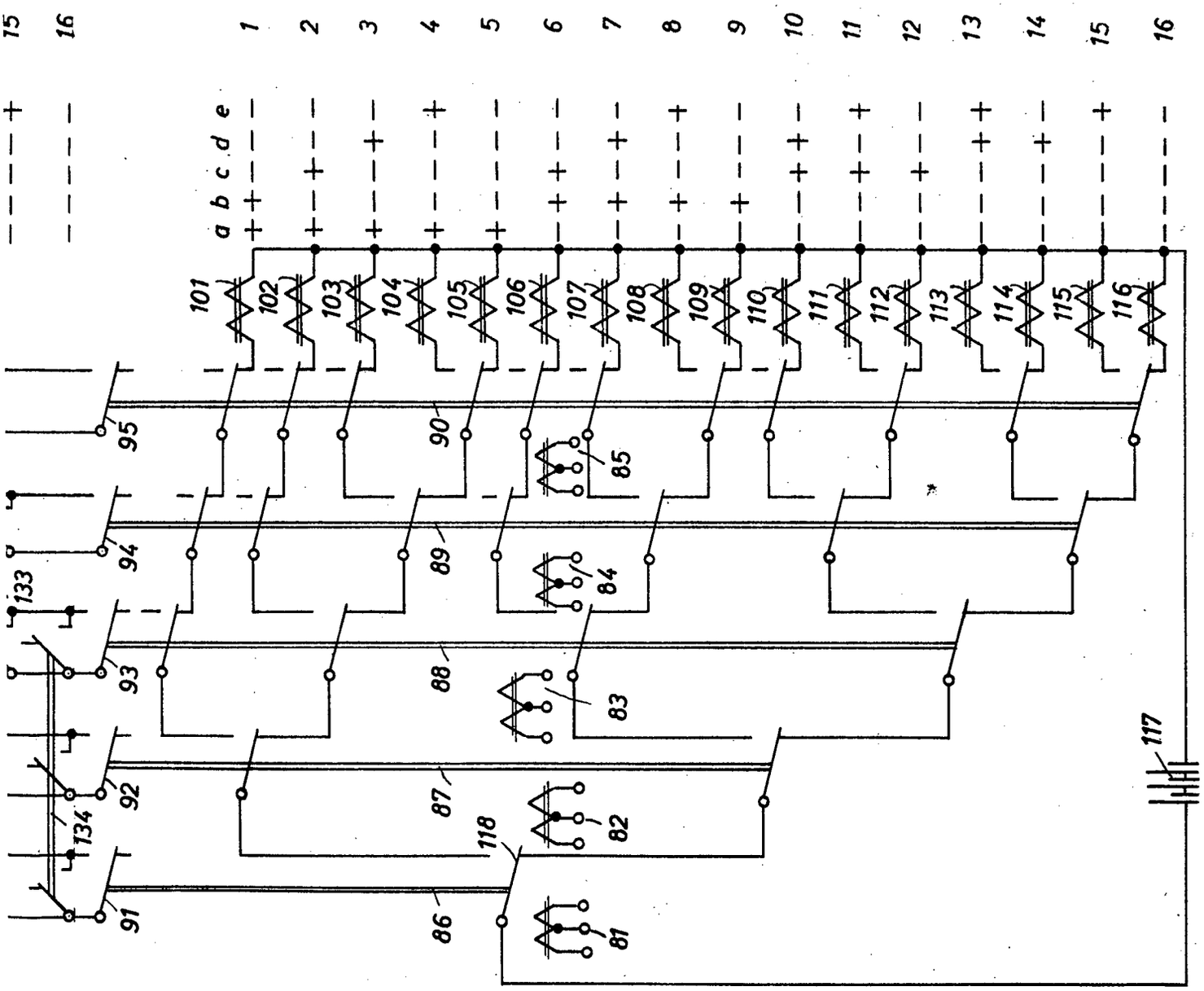


Fig. 6

AUSGABETAG: 2. JULI 1959

DBP 1 047 837
KL. 21 a¹ 21
INTERNAT. KL. H 04 k

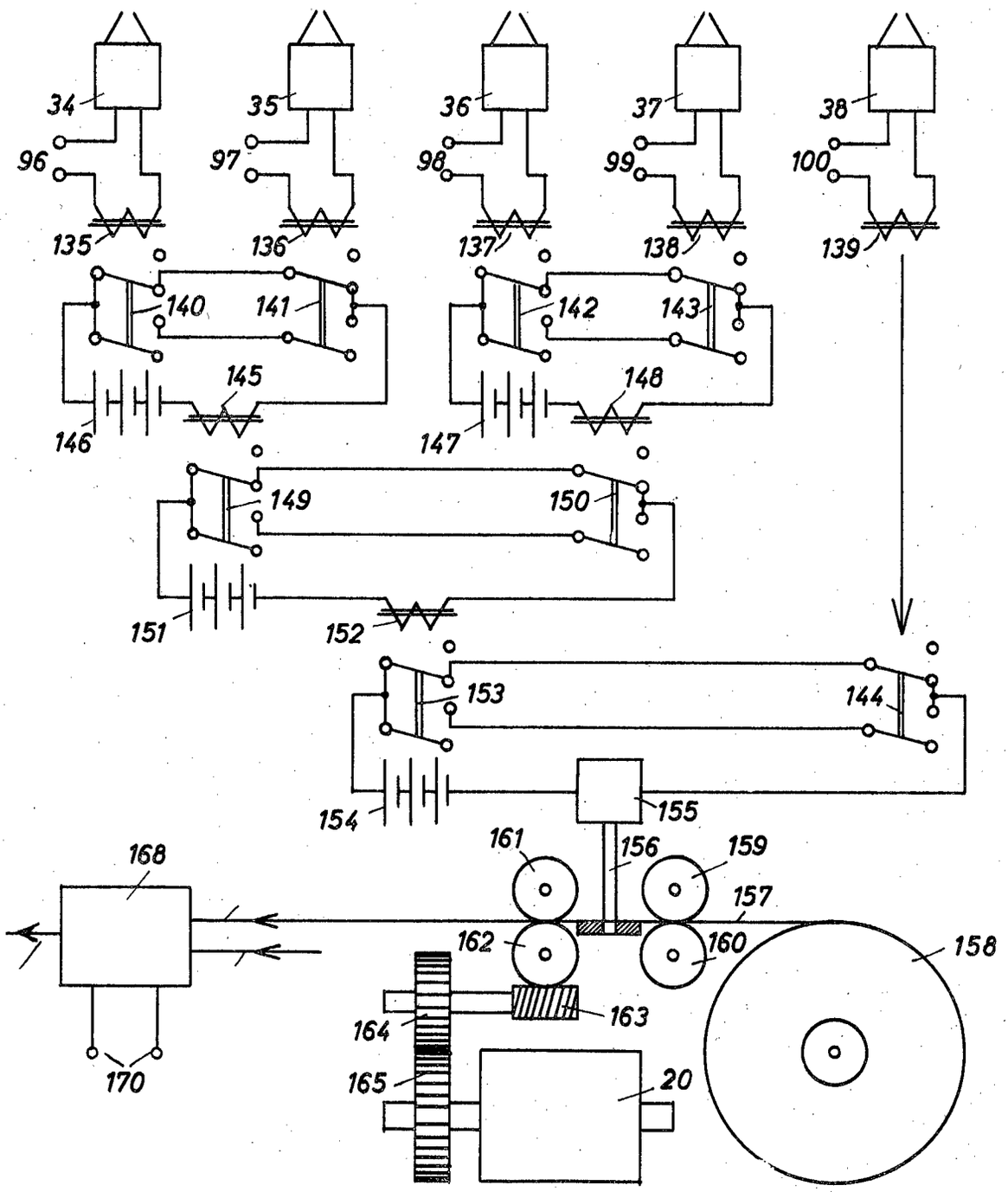


Fig. 7