(51) Int. Cl. 2: H 04 L 9/02
H 04 K 1/00

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

DE 9 78 066 C 1

(11) Patentschrift 9 78 066

(21) Aktenzeichen: P 9 78 066.9-31
(22) Anmeldetag: 23. 3. 61
(43) Offenlegungstag: —
(44) Bekanntmachungstag: —
(45) Ausgabetag: 15. 6. 78

(30) Unionspriorität:
(32) (33) (31) —

(54) Bezeichnung: Verfahren zur Herstellung von aus binären Zeichenelementen bestehenden Schlüsselfolgen zum Verschlüsseln binär kodierter Informationen

(73) Patentiert für: Dr.-Ing. Rudolf Hell GmbH, 2300 Kiel

(72) Erfinder: Hell, Rudolf, Dr.-Ing.; Koll, Roman, Dipl.-Ing.; 2300 Kiel

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
Nichts ermittelt

Erteilt auf Grund des Par. 30e PatG i.d. Fassung v. 09.05.61

6. 78 809 624/2

Patentansprüche:

1. Verfahren zur Herstellung von aus binären Zeichenelementen bestehenden Schlüsselfolgen zum Verschlüsseln binär kodierter Informationen unter Verwendung einer verhältnismäßig kurzen aperiodischen Urfolge aus zufallsverteilten mehrstelligen Zeichenelementekombinationen, deren jeweils aus den 1., 2., ..., usw. Zeichenelementen der einzelnen Kombinationen gebildeten Zeichenelementefolgen Zeichenelementeanzahlen aufweisen, deren keine zwei einen gemeinschaftlichen Teiler haben, dadurch gekennzeichnet, daß die Zeichenelemente der einzelnen Folgen, beginnend mit einem beliebigen Zeichenelement in jeder Folge, nach je einem unregelmäßig wechselnde Schrittanzahlen liefernden Programm zyklisch abgezählt werden, daß nach durch diese Programme bestimmten Anzahlen von Zählschritten die angetroffenen Zeichenelemente dieser Folgen ausgewählt werden, daß die Abzählungen jeweils mit den auf die ausgewählten Zeichenelemente folgenden Zeichenelementen fortgesetzt werden und daß den jeweils ausgewählten Zeichenelementen nach irgendeiner Regel ein Zeichenelement (+ oder −) zugeordnet wird, welches ein Zeichenelement der Schlüsselfolge ist.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß für die Festlegung der Anzahlen von Zählschritten die durch die jeweils ausgewählten Zeichenelemente bestimmte Zeichenelementekombination oder eine aus dieser mit weniger Stellen abgeleitete Teilkombination als duale Schreibweise einer natürlichen Zahl (einschließlich 0, z. B. + =1 und − =0) gedeutet wird und daß diese Zahl die für alle Folgen gleiche Anzahl von Zählschritten für die nächste Abzählung liefert.

3. Verfahren nach Anspruch 1 und 2, dadurch gekennzeichnet, daß für die Festlegung der Anzahlen von Zählschritten die entsprechend den Vorzeichen der ausgewählten Zeichenelemente mit den Faktoren 0 oder 1 versehene natürliche Zahl (z. B. + : 1 und − : 0) die Anzahlen der Zählschritte in den einzelnen Folgen für die nächste Abzählung liefert und daß dabei in allen Folgen um einen zusätzlichen Schritt weitergezählt wird.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß für die Festlegung der Anzahlen von Zählschritten jeder der Zeichenelementefolgen eine feste natürliche Zahl zugeordnet wird, daß bei den jeweils ausgewählten Zeichenelementen dieser Folgen die diesen Folgen zugeordneten Zahlen den Faktor 1 oder 0 erhalten, je nach dem das eine (z. B. +) oder das andere (z. B. −) der beiden Zeichenelemente vorliegt, daß die mit diesen Faktoren versehenen Zahlen addiert werden und daß die dabei entstehende Summe, vermehrt um den Summanden 1, die für alle Folgen gleiche Anzahl von Zählschritten für die nächste Abzählung liefert.

5. Verfahren nach Anspruch 1 und 4, dadurch gekennzeichnet, daß für die Festlegung der Anzahlen von Zählschritten von den den einzelnen Folgen zugeordneten festen natürlichen Zahlen und den Zählperioden keine zwei einen gemeinschaftlichen Teiler haben, daß diese entsprechend den Vorzeichen der ausgewählten Zeichenelemente mit den Faktoren 0 oder 1 versehenen zugeordneten Zahlen die Anzahlen der Zählschritte in den einzelnen Folgen für die nächste Abzählung liefern und daß dabei in allen Folgen um einen zusätzlichen Schritt weitergezählt wird.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Zuordnung eines Zeichenelementes zu den jeweils ausgewählten Zeichenelementen die ausgewählten Zeichenelemente nach einem Pyramidenschema gemäß den Vernamschen Vorzeichenregeln so lange miteinander gemischt werden, bis ein einziges Zeichenelement, das Schlüsselzeichenelement, übrigbleibt.

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Zuordnung eines Zeichenelementes zu den jeweils ausgewählten Zeichenelementen von den ausgewählten Zeichenelementen festgestellt wird, welches der beiden Zeichenelemente überwiegt (unterwiegt), und daß die Polarität des überwiegenden (unterwiegenden) Zeichenelementes die Polarität des Schlüsselimpulses bestimmt.

8. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Herstellung einer statistischen Gleichverteilung der Zeichenelemente der Schlüsselfolge bei mangelnder Gleichverteilung der beiden Zeichenelemente die Zeichenelemente der Schlüsselfolge paarweise mit den Zeichenelementen einer aus den regelmäßig miteinander abwechselnden beiden Zeichenelementen bestehenden (alternierenden) Folge gemischt werden.

Die Erfindung betrifft ein Verfahren zur Herstellung von aus binären Zeichenelementen bestehenden Schlüsselfolgen zum Verschlüsseln binär kodierter Informationen unter Verwendung einer verhältnismäßig kurzen aperiodischen Urfolge aus zufallsverteilten mehrstelligen Zeichenelementekombinationen, deren jeweils aus den 1., 2., ... usw. Zeichenelementen der einzelnen Kombinationen gebildeten Zeichenelementefolgen Zeichenelementeanzahlen aufweisen, deren keine zwei einen gemeinschaftlichen Teiler haben.

Zum Verschlüsseln von Informationen, die binär kodiert sind, z. B. im Fernschreib- oder Morsecode, oder von Informationen, die von vornherein in binärer Form vorliegen, wie z. B. Faksimilebilder, werden unperiodische oder periodische, aus zwei binären Zeichenelementen mit statistischer Gleichverteilung dieser Zeichenelemente bestehende Schlüsselfolgen benötigt. Das Verschlüsseln besteht in der paarweise erfolgenden Mischung der Schlüsselzeichenelemente mit den Klarzeichenelementen gemäß den Vernamschen Vorzeichenregeln. Das Ergebnis der Verschlüsselung ist eine Folge von Geheimzeichenelementen, die durch Rückmischung mit den entsprechenden Schlüsselzeichenelementen der gleichen Schlüsselfolge wieder entschlüsselt werden können.

Zur Erzeugung der Schlüsselfolgen werden meistens sogenannte Zufallsgeneratoren verwendet. Die auf diese Weise hergestellten Schlüsselfolgen sind aperiodisch und weisen eine Zufallsverteilung der beiden Zeichenelemente auf, was nicht heißt, daß diese gleichverteilt sein müssen. Einer mangelnden Gleichverteilung kann durch zusätzliche Maßnahmen abgeholfen werden.

Wenn die mit einem Zufallsgenerator erzeugten aperiodischen Schlüsselfolgen, die grundsätzlich nicht in

einer zweiten gleichen Apparatur reproduziert, sondern nur kopiert werden können, einige Zeit reichen sollen, nehmen sie unangenehm große Längen an, was ihren Versand und ihre Aufbewahrung aus Gründen der Geheimhaltung sehr mißlich erscheinen läßt. Daher hat man schon vor längerer Zeit Schlüsselverlängerungsverfahren erdacht, die gestatten, aus einer verhältnismäßig kurzen, aus mehrstelligen Zeichenelementekombinationen bestehenden aperiodischen Urfolge periodische Schlüsselfolgen aus Zeichenelementen oder Zeichenelementekombinationen mit einer so großen Periode abzuleiten, daß sie für Unbefugte nicht zu erkennen ist.

Ein solches bekanntes Verlängerungsverfahren besteht darin, daß die aus den 1., 2., 3., ... usw. Zeichenelementen der einzelnen aufeinanderfolgenden Zeichenelementekombinationen gebildeten Zeichenelementefolgen gleichzeitig, mit gleicher Schrittgeschwindigkeit und periodisch gelesen werden und daß in jeder dieser Folgen mit einem beliebigen Zeichenelement begonnen wird. Die jeweils gleichzeitig gelesenen Zeichenelemente aus den Folgen ergeben dauernd in ihrer Zusammensetzung wechselnde Kombinationen, da sich die Zeichenelementefolgen wegen ihrer unterschiedlichen Zeichenelementeanzahlen beim periodischen Lesen im Laufe der Zeit immer mehr gegeneinander verschieben. Nach einer Gesamtschrittanzahl, die gleich dem Produkt der (teilerfremden) Zeichenelementeanzahlen aller Folgen ist, wird der Anfangszustand wieder erreicht, mit dem das Lesen begonnen wurde. Diese Schrittanzahl ist gleich der Periode der verlängerten Kombinationsfolge. Aus der Kombinationsfolge kann eine lineare Folge aus Zeichenelementen gewonnen werden, indem z. B. die Zeichenelemente jeder gelesenen Kombination nach einem Pyramidenschema gemäß den Vernamschen Vorzeichenregeln so lange einander überlagert werden, bis jeweils ein Zeichenelement übrigbleibt.

Für die Festlegung des Vorzeichens des Schlüsselzeichenelementes sind auch noch andere Maßnahmen denkbar, so könnte z. B. das Vorzeichen des Schlüsselzeichenelementes durch das überwiegende (oder unterwiegende) Vorzeichen jeder gelesenen Kombination bestimmt werden, falls die Stellenzahl des verwendeten Binärcodes ungeradzählig ist.

Ein anderes bekanntes Verlängerungsverfahren bedient sich der sogenannten vergleichenden Querabfrage.

Jede gelesene Kombination wird mit einer Kombination oder mehreren verschiedenen festgesetzten Kombinationen verglichen. Jedesmal, wenn die gelesene Kombination mit einer der festgesetzten Kombinationen übereinstimmt, wird aus einer weiteren, periodischen, sämtliche möglichen Kombinationen in willkürlicher Reihenfolge enthaltenden Folge, die mit der gleichen Schrittgeschwindigkeit wie die erste gelesen wird, die im Übereinstimmungszeitpunkt gerade vorliegende Kombination dieser zweiten Folge ausgewählt und als Kombination der verlängerten Folge verwendet. Deren Periode ist natürlich kürzer als die Periode der Ausgangsfolge und die unverlängerte Folge hat im Gegensatz zu dem ersten Verfahren die Eigenschaft, daß die ausgewählten Kombinationen völlig unregelmäßig nach immer wieder anderen Schrittanzahlen auftreten.

Nach einer Variante dieses Verfahrens wird gleichzeitig und schrittgleich mit der ersten Kombinationsfolge die alternierende, abwechselnd aus dem einen und dem anderen Zeichenelement bestehende Folge gelesen. Jedes Mal, wenn die gelesene Kombination mit einer der festgesetzten Kombinationen übereinstimmt, wird das im Übereinstimmungszeitpunkt gerade vorliegende Zeichenelement der alternierenden Folge ausgewählt und als Zeichenelement der verlängerten linearen Folge verwendet.

Bei der praktischen Durchführung dieser bekannten Verfahren wird als aus Zeichenelementekombinationen bestehende Urfolge ein kurzer Lochstreifen verwendet. Dieser Urlochstreifen wird nun nicht unmittelbar abgetastet wie in den Fernschreibmaschinen, sondern mit seiner Hilfe wird ein Kontaktfeld programmiert, dessen Kontakte wie die Löcher eines voll ausgestanzten Lochstreifens angeordnet sind. Der Lochstreifen wird zu diesem Zweck auf das Kontaktfeld gelegt, und auf den Lochstreifen wird eine dünne, elektrisch leitende Metallfolie gelegt, auf welche ein Gummiklotz gepreßt wird. Dadurch erhalten nur diejenigen Kontakte über die Metallfolie Spannung, denen Löcher im Lochstreifen gegenüberliegen, während die durch das Lochstreifenpapier abgedeckten Kontakte keine Spannung erhalten.

Die Kontaktreihen (parallel zur Längsausdehnung der Kontaktanordnung) werden durch eine entsprechende Anzahl von elektronischen Ringzählern synchron und periodisch abgetastet. Dabei haben diese Zähler Zählperioden, deren keine zwei einen gemeinschaftlichen Teiler haben und die in der Nähe der Anzahl der Kontaktspalten (quer zum Kontaktfeld) des Kontaktfeldes liegen.

Für kommerzielle Verschlüsselungen, bei denen keine so große Sicherheit gegen unbefugte Entschlüsselungen wie bei militärischen Verschlüsselungen erforderlich ist, ist es erwünscht, daß der Urlochstreifen mehrfach ausgenutzt werden kann. Dies kann z. B. in der Weise geschehen, daß die Länge des Urlochstreifens ein Mehrfaches der Länge des Kontaktfeldes beträgt, z. B. das Zwei- bis Dreifache, so daß er an einem Ende oder an beiden Enden des Kontaktfeldes herausragt. Legt man einen solchen Urlochstreifen zunächst so in das Kontaktfeld ein, daß sein eines Ende sich mit dem einen Ende des Kontaktfeldes deckt, daß er also anfänglich nur an dem anderen Ende des Kontaktfeldes herausragt, so kann man ihn, nachdem die Periode des in das Kontaktfeld eingelegten Teiles des Lochstreifens abgelaufen ist oder wenn man einen Tages-, Wochen- oder Monatsschlüssel zur Verfügung haben will, jeweils bei Schlüsselwechsel um eine Lochkombination verschieben. Dem neuen, im Kontaktfeld liegenden Lochstreifenteil fehlt dann an seinem Anfang eine Lochkombination, und an seinem Ende ist eine Lochkombination hinzugekommen. Die dazwischenliegenden Lochkombinationen sind hingegen dieselben geblieben. Diese Verschiebung kann offenbar so viele Male vorgenommen werden, wie die Differenz zwischen der Anzahl der Lochkombinationen des Urlochstreifens und der Anzahl Kontaktkombinationen des Kontaktfeldes beträgt, bis der Lochstreifen verbraucht ist.

Nachteilig bei den eingangs beschriebenen Verlängerungsverfahren ist allerdings, daß der um eine Lochkombination verschobene Urlochstreifen in seinem wirksamen Teil, d. h. in dem Teil, der auf dem Kontaktfeld aufliegt, bis auf eine Lochkombination mit dem vor der Verschiebung wirksamen Teil übereinstimmt. Solange die Teilperiode, die der Länge des Kontaktfeldes entspricht, noch nicht abgelaufen ist, sind die abgefragten Lochkombinationen dieselben wie vorher, so daß derselbe Periodenabschnitt noch einmal

verwendet wird, was zu sogenannten phasengleichen Sprüchen führt, die unerwünscht sind.

Das Ziel der Erfindung besteht darin, unter Beibehaltung eines mehrfach langen und mehrfach ausnutzbaren Urlochstreifens, aus seinem wirksamen (eingelegten) Teil eine Folge von möglichst großer Periode von Zeichenelementekombinationen und aus dieser eine Folge von Zeichenelementen abzuleiten, bei der es keine Unterperioden gibt, die bei Verschiebung des Lochstreifens wiederkehren.

Erfindungsgemäß geschieht dies in der Weise, daß die Zeichenelemente der einzelnen Folgen, beginnend mit einem beliebigen Zeichenelement in jeder Folge, nach je einem unregelmäßig wechselnde Schrittanzahlen liefernden Programm zyklisch abgezählt werden, daß nach durch diese Programme bestimmten Anzahlen von Zählschritten die angetroffenen Zeichenelemente dieser Folgen ausgewählt werden; daß die Abzählungen jeweils mit den auf die ausgewählten Zeichenelemente folgenden Zeichenelementen fortgesetzt werden und daß den jeweils ausgewählten Zeichenelementen noch irgendeiner Regel ein Zeichenelement (+ oder −) zugeordnet wird, welches ein Zeichenelement der Schlüsselfolge ist.

Aus diesen Maßnahmen geht hervor, daß sich gewisse Unterperioden bei Verschiebung des Lochstreifens nicht mehr wiederholen können, jedenfalls so lange nicht, bevor nicht die Programmperiode abgelaufen ist, die nicht kleiner als die Lochstreifenperiode sein soll, da ja dann sichergestellt ist, daß mit Ablauf der Lochstreifenunterperioden das Programm nicht wieder dieselbe Anfangskonfiguration aufweisen kann wie bei Beginn der Abtastung.

Das Programm, welches mehrstellige Zählschrittkombinationen enthält, kann unabhängig oder abhängig vom Urlochstreifen sein. Im Falle der Unabhängigkeit müßte für das Programm ein weiterer Lochstreifen zur Verfügung stehen, aus dessen Lochkombinationen nach irgendeiner Vorschrift Zählschrittekombinationen abgeleitet werden.

Da dies für kommerzielle Verschlüsselungsgeräte zu kompliziert wird, wird das Zählschritteprogramm dem Urlochstreifen selbst entnommen.

Nach einer Weiterbildung der Erfindung geschieht dies in der Weise, daß die durch die jeweils ausgewählten Zeichenelemente bestimmte Zeichenelementekombination oder eine aus dieser abgeleitete Teilkombination mit weniger Stellen als duale Schreibweise einer natürlichen Zahl gedeutet wird und daß diese Zahl die für alle Folgen gleiche Anzahl von Zählschritten für die nächste Abzählung liefert.

Eine Variante dieses Verfahrens besteht in weiterer Ausgestaltung der Erfindung darin, daß diese entsprechend den Vorzeichen der ausgewählten Zeichenelemente mit den Faktoren 0 oder 1 versehene natürliche Zahl die Anzahlen der Zählschritte in den einzelnen Folgen für die nächste Abzählung liefert und daß dabei in allen Folgen um einen zusätzlichen Schritt weitergezählt wird.

Nach einer Weiterbildung der Erfindung wird ein abhängiges Zählschritteprogramm aus den Zeichenelementekombinationen der Urfolge in der Weise gewonnen, daß jeder der Zeichenelementefolgen eine feste natürliche Zahl zugeordnet wird, daß bei den jeweils ausgewählten Zeichenelementen dieser Folgen die diesen Folgen zugeordneten Zahlen den Faktor 1 oder 0 erhalten, je nach dem das eine oder das andere der beiden Zeichenelemente vorliegt, daß die mit diesen Faktoren versehenen Zahlen addiert werden und daß die dabei entstehende Summe, vermehrt um den Summanden 1, die für alle Folgen gleiche Anzahl von Zählschritten für die nächste Abzählung liefert.

Eine Variante dieses Verfahrens besteht in weiterer Ausgestaltung der Erfindung darin, daß von den den einzelnen Folgen zugeordneten festen natürlichen Zahlen und den Zählperioden keine zwei einen gemeinschaftlichen Teiler haben, daß diese entsprechend den Vorzeichen der ausgewählten Zeichenelemente mit den Faktoren 0 oder 1 versehenen zugeordneten Zahlen die Anzahlen der Zählschritte in den einzelnen Folgen für die nächste Abzählung liefern und daß dabei in allen Folgen um einen zusätzlichen Schritt weitergezählt wird.

In den Zeichnungen sind vier Ausführungsbeispiele für Schaltungsanordnungen zur Durchführung des Verfahrens gemäß der Erfindung in Blockschaltbildern dargestellt.

Fig. 1 zeigt eine Schaltungsanordnung zur Herstellung von Schlüsselfolgen, bei der in allen Zeichenelementefolgen jeweils um die gleiche Schrittanzahl weitergezählt wird, welche durch die eine Dualzahl darstellende jeweils abgetastete Lochkombination bestimmt wird.

Fig. 2 zeigt eine Schaltungsanordnung zur Herstellung von Schlüsselfolgen, bei der in den einzelnen Zeichenelementefolgen jeweils um verschiedene Schrittanzahlen weitergezählt wird, welche durch die mit den Faktoren 0 oder 1 versehene Dualzahl ermittelt werden.

Fig. 3 zeigt eine Schaltungsanordnung zur Herstellung von Schlüsselfolgen, bei der in allen Zeichenelementefolgen jeweils um die gleiche Schrittanzahl weitergezählt wird, welche durch die Summe der mit den Faktoren 0 oder 1 versehenen, den einzelnen Folgen zugeordneten festen natürlichen Zahlen bestimmt wird, und

Fig. 4 zeigt eine Schaltungsanordnung zur Herstellung von Schlüsselfolgen, bei der in den einzelnen Zeichenelementefolgen jeweils um verschiedene Schrittanzahlen weitergezählt wird, welche durch die mit den Faktoren 0 oder 1 versehenen, den einzelnen Folgen zugeordneten festen natürlichen Zahlen bestimmt werden.

Die mit Hilfe des Verfahrens gemäß der Erfindung hergestellten Impulsfolgen sollen in den Ausführungsbeispielen dazu verwendet werden, um eine Fernschreibnachricht zu verschlüsseln. Die von der in Fig. 1 bis Fig. 4 dargestellten Fernschreibmaschine 1 gelieferten Fernschreibzeichen bestehen aus Gruppen von je sieben positiven und negativen Stromschritten, von denen der erste und letzte der Start- und Stopschritt und die fünf dazwischenliegenden die Informationsschritte sind. Bei der üblichen Fernschreibgeschwindigkeit werden 7,14 Schriftzeichen pro Sek. übertragen. Das ergibt $7{,}14 \cdot 7 = 50$ Stromschritte pro Sek. (50 Baud). Die Dauer eines Stromschrittes beträgt demnach 20 ms. Für jeden einzelnen Stromschritt (Informationsimpuls), welcher positiv oder negativ sein kann, wird durch den Schlüsselimpulsgenerator ein Schlüsselimpuls geliefert, der ebenfalls positiv oder negativ sein kann. Informationsimpuls und Schlüsselimpuls werden nach den Vernamschen Vorzeichenregeln ($+ \cdot + = - \cdot - = -$ und $+ \cdot - = - \cdot + = +$) miteinander gemischt und die Mischergebnisse als Geheimimpulse ausgesendet. Auf der Empfangsseite werden die Geheimimpulse mit den dort erzeugten Schlüsselimpul-

sen entmischt und als klare Informationsimpulse der empfangenden Fernschreibmaschine zugeleitet.

Es werde angenommen, daß die elektronische Herstellung eines Schlüsselimpulses in einer gegenüber der Dauer eines Informationsstromschrittes vernachlässigbar kleinen Zeit geschieht. Klarimpuls von Schlüsselimpuls treten dann im Mischgerät gleichzeitig auf. Ferner werde angenommen, daß der Taktgeber für die Schlüsselimpulserzeugung durch die Fernschreibzeichenschritte synchronisiert ist und daß er Impulse im Takt dieser Schritte liefert, auch wenn der Eigenart der Fernschreibzeichen entsprechend zwischen einzelnen Stromschritten keine Polaritätswechsel eintreten. Diese Voraussetzungen werden gemacht, damit die Anlage funktionsfähig ist; sie berühren nicht den Gegenstand der Erfindung.

In der Schaltungsanordnung nach Fig. 1 liefert der Taktimpulsgeber 3 nadelförmige Taktimpulse an die Leitung 4. Der erste dieser Taktimpulse schaltet den Schalter 5 in seine Arbeitsstellung, wodurch über die Leitung 6 der Zählimpulsgeber 7 in Gang gesetzt wird. Dieser gibt nadelförmige Zählimpulse hoher Frequenz (etwa 50 kHz) über die Leitung 8 an die Eingänge der fünf elektronischen Ringzähler 9 bis 13 und an den Zähler 41. Jeder dieser Zählimpulse schaltet alle Ringzähler 9 bis 13 um jeweils einen Schritt weiter. Nach jedem vollen Umlauf beginnt jeder Zähler ohne Unterbrechung wieder von neuem zu zählen. Die Zählperioden für je einen Umlauf der einzelnen Ringzähler 9 bis 13 sind verschieden und so gewählt, daß deren keine zwei einen gemeinschaftlichen Teiler haben. Den einzelnen Ringzähler 9 bis 13 sind Programme zugeordnet, welche aus je einer parallel zu dessen Längsausdehnung angeordneten Lochreihe des Ur- oder Programmlochstreifens 14 bestehen. Jede Lochreihe ordnet entsprechend der An- und Abwesenheit von Löchern den einzelnen Zählstufen des zugeordneten Ringzählers eine positive oder negative Wertigkeit zu, so daß die ausgangsseitig angeschlossenen Leitungen 15 bis 19 entsprechend diesen Programmen zwischen Positiv und Negativ unregelmäßig wechselnde Potentiale annehmen. Die Leitungen 15 bis 19 sind an die ersten Steuereingänge der Koinzidenzspeicher 20 bis 24 geführt, während die Leitung 4 mit deren zweiten Steuereingängen verbunden ist. Ein Koinzidenzspeicher ist eine Vereinigung von einem Und-Tor und einem bistabilen Schalter, welcher in die Arbeitsstellung geht, wenn an seinen beiden Steuereingängen gleichzeitig Spannung auftritt. Der Taktimpuls auf der Leitung 4 schaltet deshalb nur diejenigen Koinzidenzspeicher 20 bis 24 um, an deren ersten Steuereingängen 15 bis 19 eine positive Spannung liegt.

Im Zeitpunkt des ersten Taktimpulses, also noch bevor der Schalter 5 umgeschaltet hat und der Zählimpulsgeber 7 eingeschaltet worden ist, stehen die Ringzähler 9 bis 13 in gewissen verabredeten Anfangsstellungen. Dabei wird eine bestimmte Konfiguration von Löchern des Lochstreifens 14 abgetastet, wodurch entsprechende Polaritäten der Ringzählerausgänge bestimmt werden. So können beispielsweise die Ringzähler 9, 10 und 13 von ihren Ausgängen positives Potential an die Leitungen 15, 16 und 19 und die Ringzähler 11 und 12 von ihren Ausgängen negatives Potential an die Leitungen 17 und 18 führen. Dadurch sind die Koinzidenzspeicher 20, 21 und 24 vorbereitet, 22 und 23 dagegen gesperrt. Der erste Taktimpuls auf der Leitung 4 schaltet deshalb die Koinzidenzspeicher 20, 21 und 24 in ihre Arbeitsstellung, während die Koinzidenzspeicher 22 und 23 in der Ruhestellung bleiben.

Die Ausgänge der Koinzidenzspeicher 20 bis 24 sind über die Leitungen 25 bis 29 an die Überlagerungsstufe 30 und gleichzeitig an die Ringzählersteuerstufe 31 angeschlossen. Die Überlagerungsstufe 30 hat die Aufgabe, aus der in jeder Taktzeit abgefragten Lochreihenkonfiguration die Polarität des Schlüsselimpulses zu ermitteln. Dies geschieht im Ausführungsbeispiel durch aufeinanderfolgende paarweise Mischungen der fünf Ausgangspotentiale aller Koinzidenzspeicher. Die Potentiale irgendeines Eingangsleitungspaares, z .B. 25 und 26, werden nach den Vernamschen Mischregeln gemischt, so daß bei gleichen Potentialen das Mischergebnis negativ und bei ungleichen positiv ist. Das Potential dieser Mischung wird mit dem Potential einer dritten Eingangsleitung, z. B. 27, auf gleiche Weise gemischt, das Ergebnis dieser Mischung mit dem Potential der vierten Eingangsleitung 28 und schließlich auf gleiche Weise das dabei entstandene Mischergebnis mit dem Potential der fünften Eingangsleitung 29. Die Reihenfolge der aufeinanderfolgenden Überlagerungen ist gleichgültig, da die Vernamschen Mischregeln kommutativ und assoziativ sind. Um Störungen in der statistischen Gleichverteilung von positivem und negativem Potential zu beseitigen, die wegen der Teilerfremdheit der Zählerperioden auftreten können, da ja mindestens vier der fünf Zählzyklen ungeradzahlige Perioden haben, wird das aus den fünf Eingängen durch Mischung ermittelte Potential noch mit einem über die Leitung 32 zugeführten sechsten Potential gemischt, welches mit jedem Takt regelmäßig abwechselnd positiv oder negativ ist. Dieses alternierende Potential liefert der bistabile Schalter 33, welcher, durch die Taktimpulse auf der Leitung 4 gesteuert, mit jedem Takt seine Stellung wechselt. Das Ergebnis der Mischung aller sechs Eingänge ergibt Spannung oder keine Spannung an dem Ausgang der Überlagerungsstufe 30 und damit auf der Leitung 34, und stellt das Potential des Schlüsselimpulses dar, der über die Leitung 34 zur Mischstufe 35 geleitet wird. Hier wird er mit dem von der Fernschreibmaschine über die Leitung 2 zugeführten Klarimpuls gemischt, und der dabei entstandene Geheimimpuls wird auf die Fernleitung 36 gegeben.

Die Ringzählersteuerstufe besteht aus dem Dual-Trigintadual-Umsetzer 37, den Und-Toren 38 ... 39 ... 40 und dem Zähler 41. Die sämtlichen möglichen binären Potentialkonfigurationen an den fünf Leitungen 25 bis 29 stellen, als duale Schreibweisen der natürlichen Zahlen aufgefaßt, die ersten einunddreißig natürlichen Zahlen einschließlich der Null dar, wenn man etwa + mit 1 und − mit 0 identifiziert. Entsprechend diesen zweiunddreißig möglichen Potentialkonfigurationen hat der Umsetzer 37 zweiunddreißig Ausgänge 42 ... 43 ... 44, welche an die zweiunddreißig Und-Tore 38 ... 39 ... 40 angeschlossen sind. Im Augenblick der Betrachung, also im Anfang der ersten Taktzeit, möge an den Leitungen 25 bis 29 die Spannungskonfiguration + + − − + = 11001 = 25 bestehen, und diese möge an der 25. Ausgangsleitung 43 des Umsetzers 37 Spannung erzeugen. Dadurch wird das 25. Und-Tor 39 vorbereitet. Die zweiten Eingänge 45 ... 46 ... 47 der Und-Tore sind die Ausgänge des Zählers 41. Durch die Zählimpulse des Zählimpulsgebers 7 auf der Leitung 8 zählt der Zähler 41, von seiner Null-Stellung ausgehend, mit jedem Zählimpuls einen Schritt weiter und legt dabei nacheinander an seine Ausgangsleitungen

45 ... 46 ... 47 Spannung. Ist der 25. Ausgang erreicht, so liegt Spannung an der Leitung **46**, welche zum zweiten Eingang des 25. Und-Tores **39** führt. Für dieses Tor ist die Durchlaßbedingung erfüllt, da an seinem ersten Eingang über die Leitung **43** Spannung liegt, so daß auch Spannung an die Leitung **48** gelangt und den Schalter **5** in die Ruhestellung schaltet. Damit wird die Leitung **6** stromlos, und der Zählimpulsgeber **7** hält an. Der Zählimpulsgeber **7** hat also ebenso viele Zählimpulse, nämlich 25 Zählimpulse erzeugt, wie die Anzahl der Schritte des Zählers **41**, nämlich 25 Schritte, beträgt, welche notwendig waren, um diejenige Stellung zu erreichen, bei der an der Ausgangsleitung **46** Spannung liegt. Diese Anzahl ist gleich der Ordnungszahl der spannungsführenden Ausgangsleitung des Umsetzers **37** und wird bestimmt durch die Konfiguration der Potentiale an den Leitungen **25** bis **29**. Auch die Ringzähler **9** bis **13** haben um ebenso viele Schritte, nämlich um 25 Schritte, weitergezählt, wie die Anzahl der Zählimpulse an der Leitung **8** betragen hatte. Sie bleiben in den eingenommenen Stellungen stehen und halten durch die diesen Stellungen entsprechenden Potentiale an ihren Ausgangsleitungen positive bzw. negative Spannung bereit, welche die Koinzidenztore vorbereiten bzw. nicht vorbereiten, bis ein weiterer Taktimpuls auf der Leitung **4** das zweite Taktintervall einleitet. Zu erwähnen ist noch, daß jedem Taktimpuls ein Steuerimpuls unmittelbar vorangeht, welcher über die Leitung **49** die Koinzidenzspeicher **20** bis **24** in die Ruhestellung und den Zähler **41** in die Null-Stellung bringt.

Mit dem zweiten Taktimpuls auf der Leitung **4** beginnt das zweite Taktintervall. Die vorbereiteten Koinzidenzspeicher schalten um, und es entstehen an den entsprechenden Ausgangsleitungen **25** bis **29** wiederum Spannungen oder keine. Das durch die Überlagerungsstufe **30** ermittelte Mischpotential, welches in der An- oder Abwesenheit von positiver Spannung besteht, liefert den Schlüsselimpuls, der über Leitung **34** zur Mischstufe **35** gelangt.

Die durch die Spannungskonfiguration an den Leitungen **25** bis **29** in dualer Schreibweise dargestellte und durch den Umsetzer **37** ermittelte natürliche Zahl bestimmt die gemeinschaftliche Anzahl der Schritte, um welche alle Ringzähler **9** bis **13** weitergeschaltet werden, um die für den Schlüsselimpuls des dritten Taktintervalls zu verwertende Potentialkonfiguration zu ermitteln.

Die Einspeicherung der durch die Ringzählerzustände bestimmten Potentialkonfiguration in die Koinzidenzspeicher am Anfang jedes Taktintervalls und die Überlagerung in der Überlagerungsstufe gehen in einer Zeit vor sich, welche in der Größenordnung der Dauer (Länge) des Taktimpulses liegt, so daß der Schlüsselimpuls für das laufende Taktzeitintervall in der Mischstufe bereits zur Verfügung steht. Die Weiterschaltung der Ringzähler und die Abtastung einer neuen Potentialkonfiguration geschieht in dem ersten Zeitteil des Taktintervalls und ist mit Sicherheit beendet, bevor eine neue Taktzeit beginnt, da der Impulsgeber **7** eine sehr viel höhere Frequenz hat, als die Frequenz der Informationsimpulse beträgt.

Zu erwähnen ist noch, daß sowohl zur Bestimmung der Polarität der Schlüsselimpulse in der Überlagerungsstufe **30** als auch zur Bestimmung der Schrittanzahl, um welche die Ringzähler **9** bis **13** weitergeschaltet werden, nicht alle fünf Ringzähler **9** bis **13** bzw. alle fünf Koinzidenzspeicher **20** bis **24** benutzt werden müssen. Aus besonderen Gründen, z. B. um Schaltmittel einzusparen und um nicht allzu viele Lochkombinationen unbenutzt zu lassen, könnte man z. B. nur eine Kombination von zwei, drei oder vier der Potentiale der Leitungen **25** bis **29** zur Überlagerung und die gleiche oder eine andere Kombination zur Steuerung der Ringzähler **9** bis **13** verwenden. Die fünfstelligen dualen Schreibweisen stellen insgesamt zweiundreißig verschiedene ganze aufeinanderfolgende Zahlen (einschließlich der Null) dar. Alle Zahlen von Null bis Zweiunddreißig kommen mit gleicher Wahrscheinlichkeit vor, so daß die mittlere Schrittanzahl der Ringzähler **9** bis **13** sechzehn beträgt.

Im Durchschnitt wird also nur jede sechzehnte Lochkombination benutzt. Werden aber z. B. nur drei der Potentiale an den Eingangsleitungen **25** bis **29** verwertet, so beträgt die mittlere Schrittanzahl der Ringzähler **9** bis **13** nur acht, und es wird im Mittel jede vierte Lochkombination ausgenutzt. Die Ergiebigkeit des Lochstreifens ist also viermal so groß und damit die gesamte mit einem Lochstreifen erzielbare Schlüssellaufzeit viermal größer.

Fig. 2 zeigt eine Variante der soeben beschriebenen Schaltungsanordnung. Die mit Hilfe des Umsetzers **37** und des Zählers **41** ermittelte Anzahl von Impulsen wird nicht allen, sondern nur denjenigen Ringzählern zugeführt, welche z. B. positive Ausgangsspannung haben. Um dies zu erreichen, sind die Tore **50** bis **54** zwischen die Leitung **8** und die Eingänge der Ringzähler **9** bis **13** geschaltet, deren Steuereingänge mit den Ausgängen der Koinzidenzspeicher **20** bis **24** verbunden sind. Die Tore **50** bis **54** sind im Ruhezustand gesperrt, und nur wenn Spannung an ihre Steuereingänge gelangt, werden sie durchlässig. Ist z. B. die Potentialkonfiguration an den Leitungen **25** bis **29** + − − + −, so sind die Tore **50** und **53** durchlässig, die Tore **51, 52** und **54** hingegen sind gesperrt. Die durch die Ringzählersteuerstufe **31** bestimmten Impulse gelangen also nur zu den Ringzählern **9** und **12** und schalten diese weiter, während die übrigen in der eingenommenen Stellung stehenbleiben. Damit aber nicht die gesperrten Ringzähler **10, 11** und **13** für weitere Taktintervalle gesperrt bleiben, wird der an der Leitung **48** auftretende Impuls, der zur Rückstellung des Schalters **5** benutzt wird, auch an die Eingänge aller Ringzähler geleitet, so daß die gesperrten Ringzähler **10, 11** und **13** einen und die übrigen noch einen zusätzlichen Schritt weiterschalten.

Fig. 3 zeigt ein anderes Ausführungsbeispiel zur Durchführung der Erfindung. Die Aufgabe der Ringzählersteuerstufe **31** war es, eine Zahl zu ermitteln, um welche die einzelnen Ringzähler **9** bis **13** weitergeschaltet werden. In den bisher beschriebenen Anordnungen geschah dieses durch Errechnen der als duale Schreibweisen der Trigintadualzahlen aufgefaßten Potentialkonfigurationen an den Eingangsleitungen der Ringzählersteuerstufe **31**. In der Anordnung nach Fig. 3 ist jedem der Ringzähler **9** bis **13** eine höchstens zweistellige ganze Zahl unter **20** fest zugeordnet, von diesen Zahlen sowie von den Zählperioden der Ringzähler **9** bis **13** sollen keine zwei einen gemeinschaftlichen Teiler haben. Die Erfüllung dieser Forderung trägt dazu bei, die Schlüsselperiode zu vergrößern. Als Beispiel seien dem Ringzähler **9** die Zahl drei, dem Ringzähler **10** die Zahl fünf und den Ringzählern **11, 12** und **13** die Zahlen sieben, neun und elf zugeordnet. Von diesen Zahlen werden in jedem Taktintervall diejenigen addiert, welche denjenigen Ringzählern zugeordnet sind, deren Ausgänge positive Spannung führen. Es werde angenommen, daß die Ringzählerausgänge **15**

und 19 positive Spannung haben, was der Potentialkonfiguration + − − − + entspricht; dann werden durch einen Taktimpuls auf der Leitung 4 die Leitungen 25 und 29 spannungsführend, während die Leitungen 26, 27 und 28 ohne Spannung bleiben. Über das Tor 56, das in Durchlaßstellung steht, wird das Tor 61 gesperrt und das Tor 66 geöffnet. Die nach der Umschaltung des Schalters 5 und der Einschaltung des Zählimpulsgebers 7 auf der Leitung 8 auftretenden Zählimpulse erreichen über das Tor 66 den Zähler 71. Die Schrittanzahl dieses dem Ringzähler 9 zugeordneten Zählers ist der Annahme entsprechend gleich drei.

Nach drei Impulsen auf der Leitung 8 ist deshalb seine Endstellung erreicht, und es gelangt Spannung an die Leitung 76, welche das Tor 56 sperrt. Dadurch verschwindet die Spannung an der Leitung 81, und die Tore 61 und 66 gehen wieder in ihre Ruhestellung. Weitere Zählimpulse von der Leitung 8 gelangen nicht mehr zum Zähler 71, sondern über das Tor 61 an die Leitung 86. Da die Leitung 26 spannungslos ist, ist das Tor 62 durchlässig und das Tor 67 ist gesperrt. Die Zählimpulse von der Leitung 8 und der Leitung 86 erreichen somit den Zähler 72 nicht, sondern gelangen über das geöffnete Tor 62 zur Leitung 87 und weiter zu den nichtgezeichneten Toren 63 und 68. Da auch die Leitungen 27 und 28 ohne Spannung sind, gelangen die Impulse über das Tor 63 und das ebenfalls nichtgezeichnete Tor 64 zu den Toren 65 und 70. Die Leitung 29 führt jedoch voraussetzungsgemäß Spannung, so daß über das Tor 60 und die Leitung 85 das Tor 65 gesperrt ist und das Tor 70 durchlässig ist.

Die Zählimpulse von der Leitung 8 gelangen also nach dem Zähler 71 seine Endstellung erreicht hat, über alle Tore 61 bis 65 an den Zähler 75. Dieser schaltet mit jedem Zählimpuls um einen Schritt weiter, bis nach elf Schritten — das ist die dem Zähler 75 zugeordnete Schrittanzahl — die Endstellung erreicht ist. Dadurch gelangt Spannung an die Leitung 80, welche das Tor 60 sperrt. Damit verschwindet die Spannung an der Leitung 85, wodurch das Tor 65 durchlässig und das Tor 70 gesperrt wird.

Der nächste Zählimpuls des Zählimpulsgebers 7 gelangt deshalb über alle Tore 61 bis 65 zur Leitung 48 und zum Schalter 5 und schaltet diesen in die Ruhestellung zurück, wodurch die Leitung 6 stromlos und der Zählimpulsgeber 7 angehalten wird; somit werden weitere Zählimpulse auf der Leitung 8 unterbunden.

An der Leitung 8 sind also nacheinander drei, elf und ein weiterer Zählimpuls aufgetreten, nämlich die Summe der Schrittanzahlen der Zähler 71 und 75 und außerdem ein zusätzlicher Impuls zur Rückschaltung des Schalters 5, so daß die gesamte Schrittanzahl, um welche die Ringzähler 9 bis 13 weitergeschaltet worden sind, fünfzehn beträgt. Der zusätzliche Impuls wird gegeben, damit die Ringzähler 9 bis 13 immer wenigstens einen Schritt weiterschalten, auch wenn während eines Taktintervalls zufällig alle fünf Leitungen 25 bis 29 ohne Spannung sein sollten. Der Impuls auf der Leitung 48 wird auch zu den Zählern 71 bis 75 geleitet und schaltet die während des abgelaufenen Zählvorganges in Tätigkeit gesetzten Zähler 71 und 75 in die Null-Stellung zurück.

Fig. 4 zeigt eine Variante der Schaltungsanordnung nach Fig. 3. Während in der Anordnung nach Fig. 3 die Summe der mit den Faktoren 0 und 1 versehenen, den Ringzählern 9 bis 13 zugeordneten festen Zahlen gebildet wird, und sodann alle Ringzähler 9 bis 13 um die dieser Summenzahl gleiche Schrittanzahl weitergeschaltet werden, werden im Ausführungsbeispiel nach Fig. 4 nur einzelne Ringzähler weitergeschaltet, z. B. diejenigen, deren Ausgänge im vorangegangenen Taktintervall Spannungen führten.

Die Arbeitsweise ist folgende: Angenommen, die Potentialkonfiguration bei Beginn der Schlüsselimpulserzeugung sei wieder + + − − +. Die Ausgänge der Ringzähler 9, 10 und 13 haben somit positive Spannung, die der Zähler 11 und 12 sind ohne Spannung. Dann sind die Koinzidenzspeicher 20, 21 und 24 vorbereitet. Der erste Taktimpuls an der Leitung 4 bringt diese Speicher in Arbeitsstellung, während die Speicher 22 und 23 in Ruhe bleiben. Es gelangt Spannung an die Leitungen 25, 26 und 29. Die Spannung an der Leitung 25 öffnet das Tor 50, die Spannung an der Leitung 26 das Tor 51 und die Spannung an der Leitung 29 das Tor 54. Die nach der Umschaltung des Schalters 5 und Einschaltung des Zählimpulsgebers 7 auf der Leitung 8 auftretenden Zählimpulse gelangen über die Tore 50, 51 und 54 zu den Ringzählern 9, 10 und 13 und schalten diese weiter, während die Ringzähler 11 und 12 stehenbleiben, da ja die Tore 52 und 53 gesperrt sind. Die Leitung 8 ist außerdem mit dem Eingang des Zählers 90 verbunden, welcher, von seiner Null-Stellung ausgehend, mit jedem Impuls einen Schritt weiterschaltet.

Entsprechend den Zahlen drei, fünf, sieben, neun und elf, welche den einzelnen Ringzählern zugeordnet sind, ist der 3., 5., 7., 9. und 11. Ausgang des Zählers 90 mit den Leitungen 91, 92, 93, 94 und 95 verbunden. Diese Leitungen sind in beliebiger Reihenfolge mit den Koinzidenzspeichern 20 bis 24 verbunden. Beim Weiterschalten des Zählers 90 entsteht der Reihe nach an allen seinen Ausgängen Spannung. Nach dem dritten Impuls befindet sich also Spannung am dritten Ausgang, d. h. an der Leitung 91, welche den Koinzidenzspeicher 21 in die Ruhestellung zurückschaltet. Die Leitung 26 wird stromlos, und das Tor 51 wird gesperrt. Der Ringzähler 10 bleibt fortan stehen, weil keine weiteren Impulse mehr an seinen Eingang gelangen. Beim fünften Taktimpuls entsteht Spannung an der Leitung 92, dem fünften Ausgang des Zählers 90. Diese Spannung bleibt wirkungslos, da der Koinzidenzspeicher 22, entsprechend dem gewählten Beispiel, bereits in Ruhe ist. Der Ringzähler 11 hat also nicht weitergeschaltet. Mit dem 7. Taktimpuls gelangt Spannung an die Leitung 93, welche mit dem Koinzidenzspeicher 20 verbunden ist und diesen in die Ruhestellung zurückschaltet. Dadurch wird die Leitung 25 stromlos, das Tor 50 wird gesperrt, und der Ringzähler 9 bleibt stehen, nachdem er sieben Schritte gemacht hat. Nach dem neunten Taktimpuls wird über die Leitung 94 der Koinzidenzspeicher 24 in die Ruhestellung und durch Sperrung des Tores 54 auch der Ringzähler 13 stillgesetzt. Nach zwei weiteren Impulsen schließlich ist die Endstellung des Zählers 90 erreicht, und es gelangt Spannung an die Leitung 95. Der Koinzidenzspeicher 23 befindet sich nicht in Arbeitsstellung, so daß die Spannung an Leitung 95 ohne Wirkung auf den Speicher 23 bleibt. Sie gelangt aber zum Schalter 5, bringt diesen in die Ruhestellung und hält den Impulsgeber 7 an. Sie schaltet ferner den monostabilen Schalter 96 ein, welcher nach einer im Vergleich zur Taktzeit sehr kuren Zeit selbsttätig in die Ruhestellung zurückgeht. Dadurch wird ein zusätzlicher Impuls an die Leitung 97 gegeben, der den Zähler 90 in die Null-Stellung bringt und ferner allen Ringzählereingängen 9 bis 13 zugeführt wird. Alle Ringzähler 9 bis 13, sowohl diejenigen, welche vorher weitergeschaltet

haben, als auch diejenigen, welche in ihrer Stellung verharrt hatten, werden dadurch um einen zusätzlichen Schritt weitergeschaltet. Dieser zusätzliche Schritt ist notwendig, damit nicht negative Spannung am Ausgang eines Ringzählers oder mehrerer der Ringzähler die Weiterschaltung dieser Zähler für alle Zeiten blockiert, denn die Weiterschaltung der Ringzähler ist nur bei positiver Ausgangsspannung möglich.

Hierzu 4 Blatt Zeichnungen

Nummer: 9 78 066
Int. Cl.²: H 04 L 9/02
Bekanntmachungstag: —

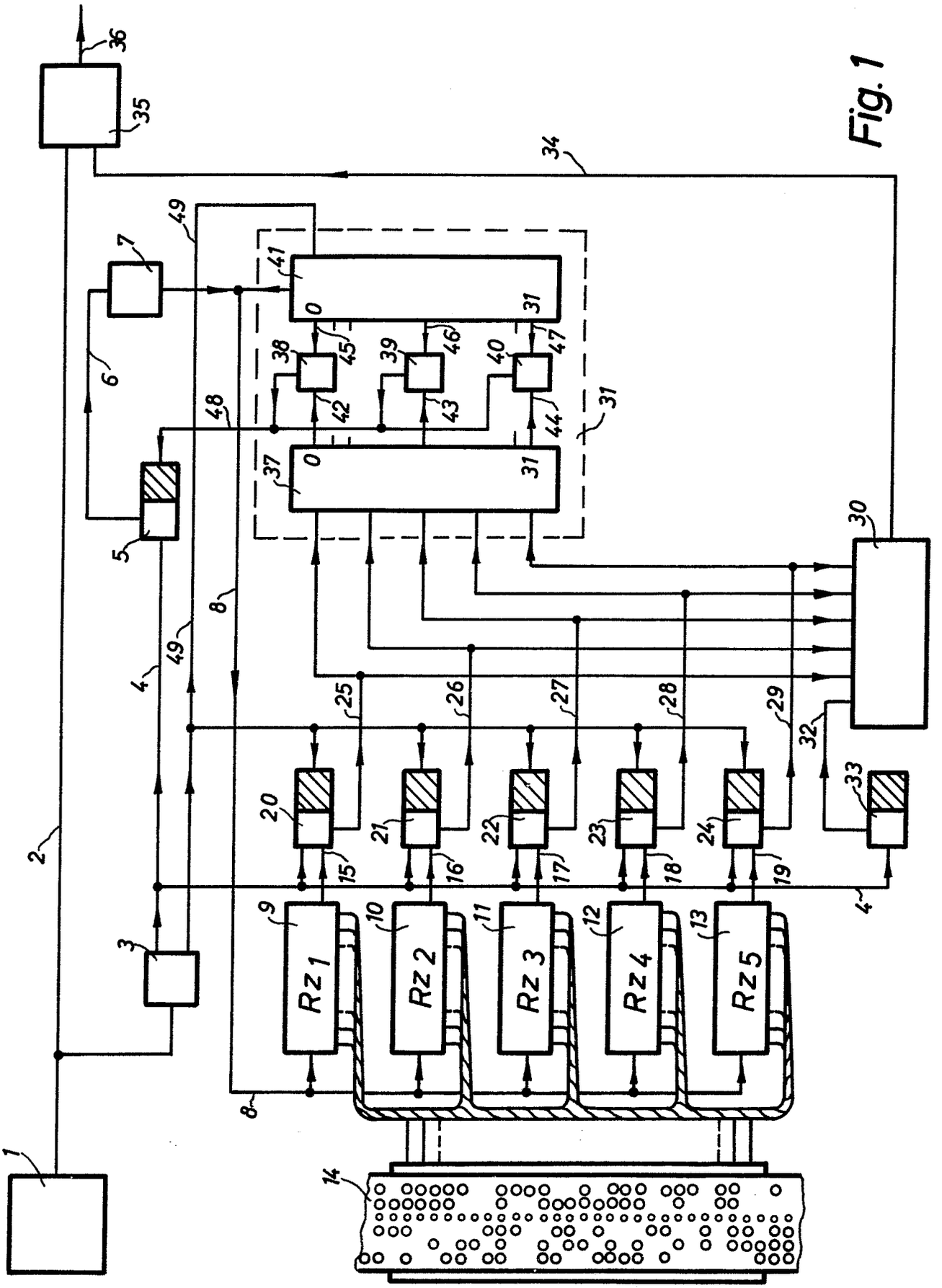
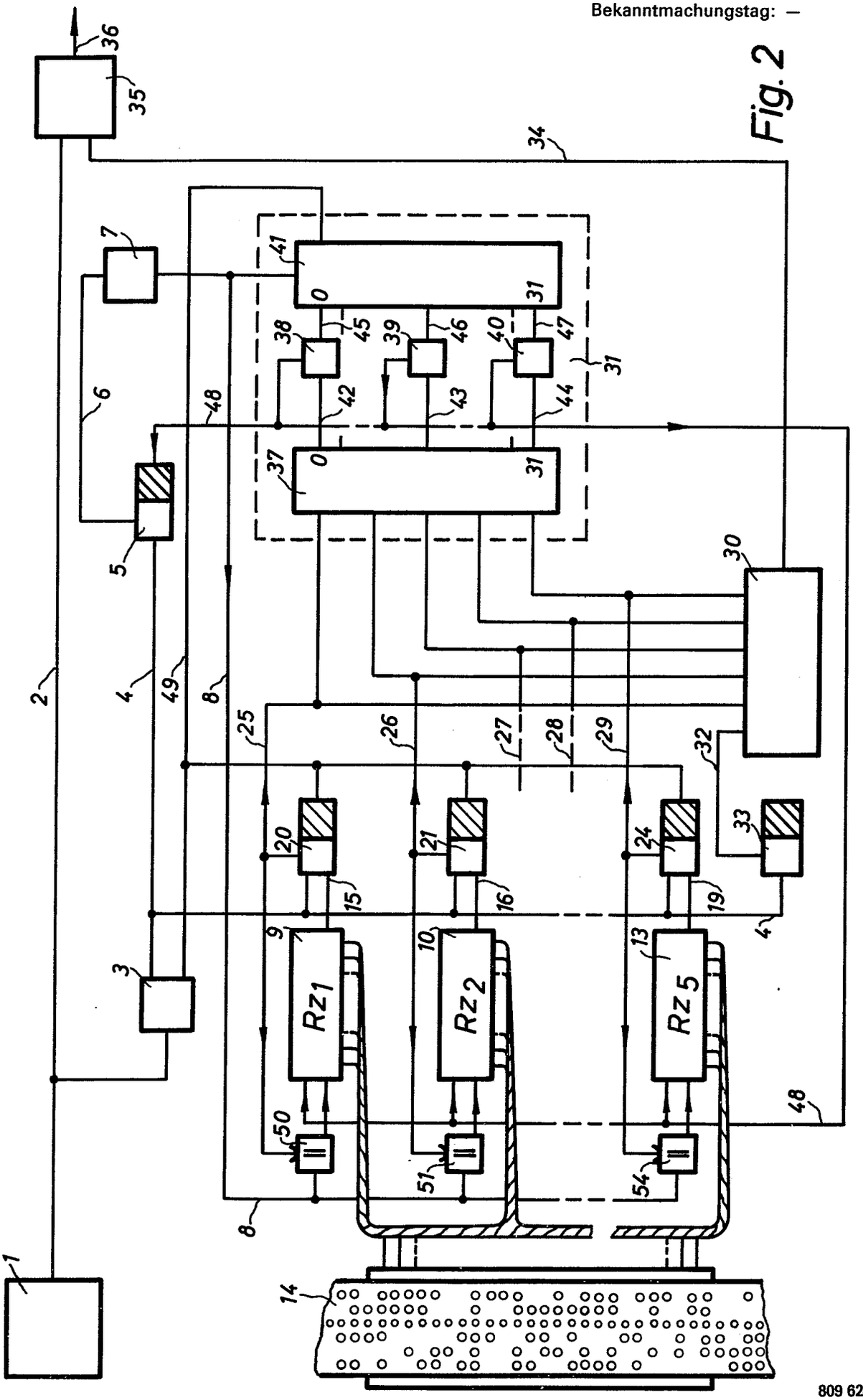


Fig. 1

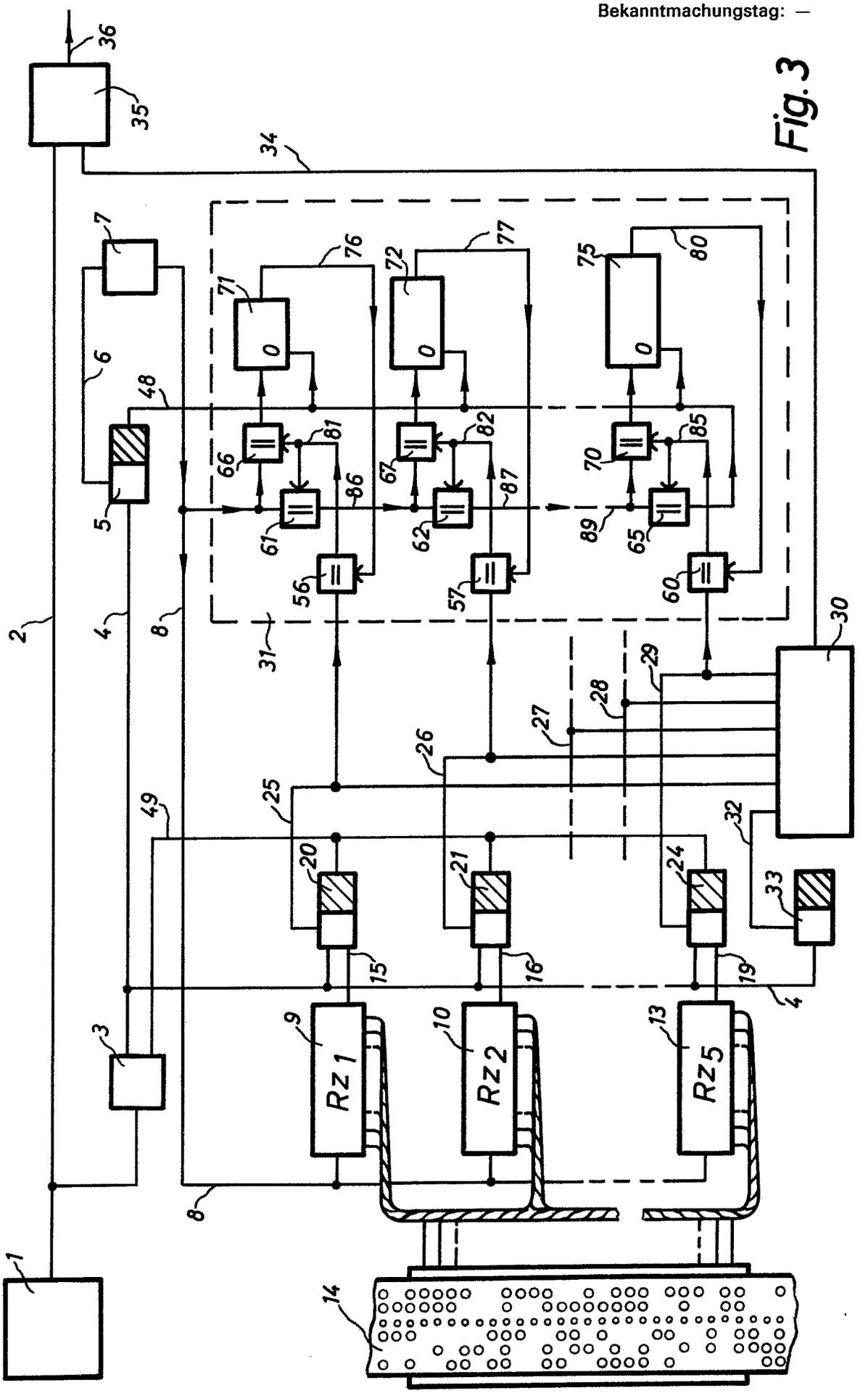
Nummer: 9 78 066
Int. Cl.²: H 04 L 9/02
Bekanntmachungstag: —

Fig. 2



Nummer: 9 78 066
Int. Cl.²: H 04 L 9/02
Bekanntmachungstag: —

Fig. 3



Nummer: 9 78 066
Int. Cl.²: H 04 L 9/02
Bekanntmachungstag: —

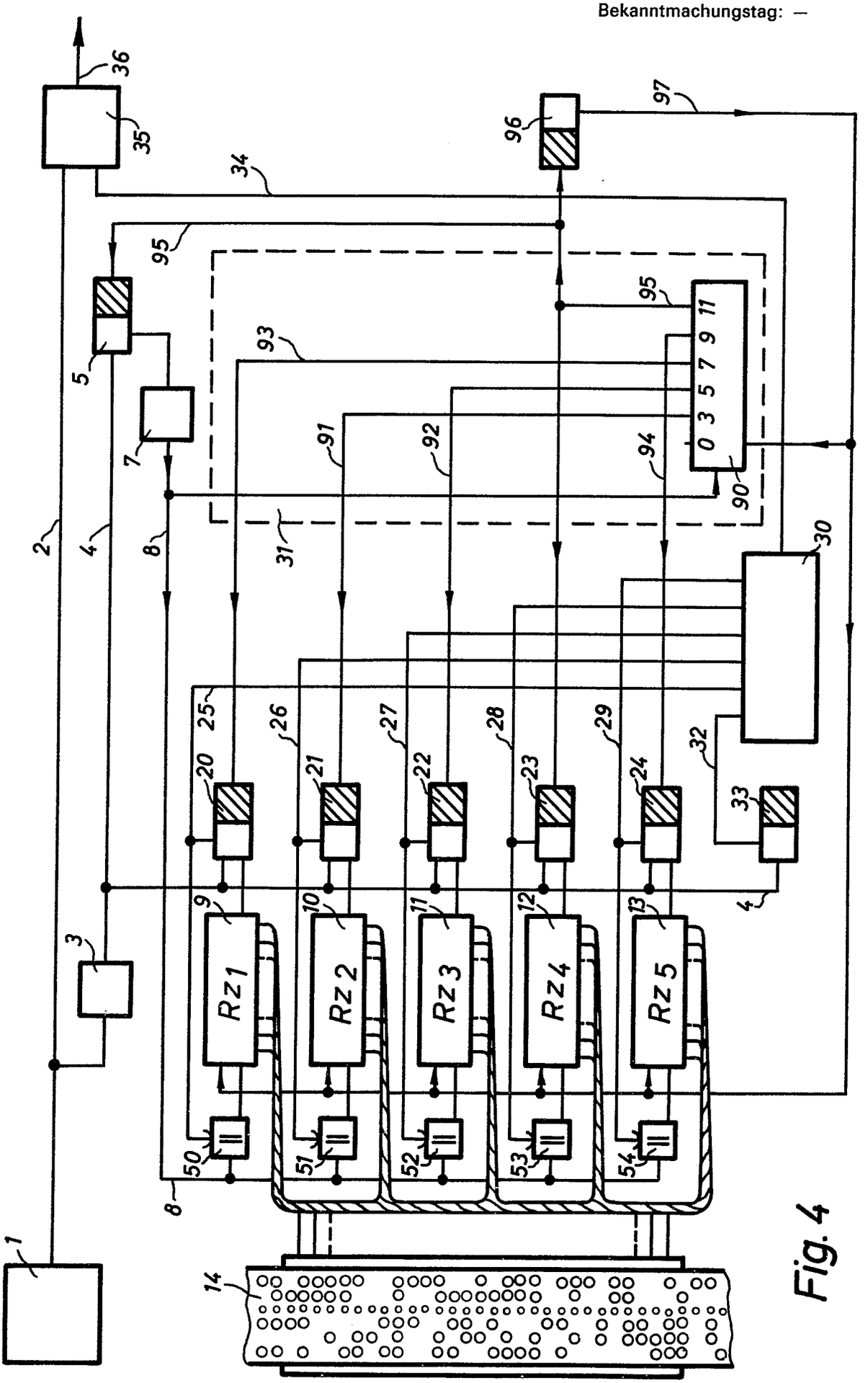


Fig. 4