CH 628 760 A5

(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
BUNDESAMT FÜR GEISTIGES EIGENTUM

(51) Int. Cl.³: H 04 K 1/00

ETH-BIBLIOTHEK ZÜRICH

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

(12) PATENTSCHRIFT A5

(11) **628 760**

(21) Gesuchsnummer: 14066/77

(22) Anmeldungsdatum: 17.11.1977

(30) Priorität(en): 19.11.1976 DE 2652607
03.06.1977 DE 2725065

(24) Patent erteilt: 15.03.1982

(45) Patentschrift veröffentlicht: 15.03.1982

(73) Inhaber:
Licentia Patent- Verwaltungs-GmbH, Frankfurt a.M. (DE)

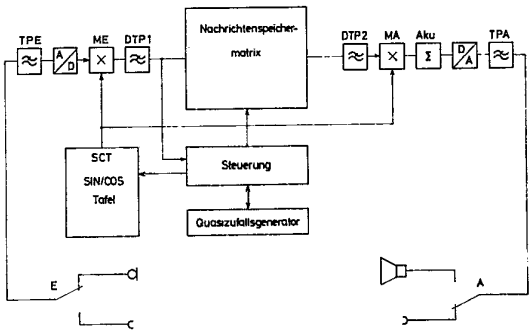
(72) Erfinder:
Dipl.-Ing. Harald Engel, Ulm (DE)
Dipl.-Ing. Ingolf Walz, Erbach (DE)
Reinhard Grünes, Ulm (DE)
Dipl.-Ing. Heinz Rieger, Stuttgart 1 (DE)
Dipl.-Ing. Wolfgang Bitzer, Weissach im Tal (DE)

(74) Vertreter:
Kirker & Cie, Genève

(54) Verfahren zur Verschleierung und nachherigen Entschleierung von Nachrichtensignalen.

(57) Bei diesem Verfahren wird das zu verschleiernde Sprachsignal innerhalb eines Zeitabschnittes in n Zeitelemente und in m gleich breite Frequenzbänder zerlegt wird, so dass eine Matrix von n ∘ m Frequenz-Zeit-Elementen entsteht.

Zwecks Verschleierung werden diese Elemente vor der Übertragung miteinander vertauscht, wobei alle (n • m)! möglichen Vertauschungen, d.h. Permutationen erlaubt sind. Dabei kann die Vertauschung, beispielsweise gesteuert durch einen Quasizufalls-Generator, für jeden der aufeinanderfolgenden Zeitrahmen wieder anders sein.



PATENTANSPRÜCHE

1. Verfahren zur Verschleierung und nachherigen Entschleierung von Nachrichtensignalen, dadurch gekennzeichnet, dass Zeitverwürfelung und Frequenzbandvertauschung miteinander verwendet werden, dass hierzu die Nachrichtensignale sendeseitig innerhalb eines sich wiederholenden Zeitabschnittes in n Zeitelemente und innerhalb eines Frequenzbandausschnittes in m Teilfrequenzbänder unterteilt werden, wobei n und m natürliche Zahlen sind, dass der durch den sich wiederholenden Zeitabschnitt charakterisierte Nachrichtenblock eine (n·m)-Matrix mit n·m-Teilfrequenzband-Zeitelementen bildet, dass mit Hilfe eines Quasizufallsgenerators die einzelnen Teilfrequenzband-Zeitelemente innerhalb der (n·m)-Matrix quasizufällig ihren Platz wechseln, wobei jeder der n·m-Plätze nur von einem der Teilfrequenzband-Zeitelementen eingenommen werden kann, dass auf der Empfangsseite mit Hilfe eines gleichen Quasizufallsgenerators die Platzvertauschung innerhalb der (n·m)-Matrix wieder rückgängig gemacht wird und der natürliche Nachrichtenfluss hergestellt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Nachrichtensignale in Zeitelemente gleicher Dauer (T) unterteilt werden, dass die Zeitelemente in Teilfrequenzbänder gleicher Bandbreite (B) unterteilt werden und dass Teilfrequenzbänder mehrerer Zeitelemente gleichzeitig zur Empfangsseite übertragen werden.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Anzahl m der Teilfrequenzbänder gleich 5 ist.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Anzahl n der Zeitelemente gleich 8 ist.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Nachrichtensignal zur Zerlegung in die Teilfrequenzbänder mit Hilfe mehrerer Trägerfrequenzen so umgesetzt wird, dass das jeweilige Teilfrequenzband durch jeweils gleiche Filter in der jeweils gleichen Frequenzlage gewonnen wird, dass das Teilfrequenzband in einem Speicher zwischengespeichert wird und nach dem Auslesen aus dem Speicher durch erneute Frequenzumsetzung mit Hilfe mehrerer Trägerfrequenzen in eine neue Frequenzlage gebracht wird.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Informationsinhalt der Teilbänder zur Speicherung in einem Speicher digitalisiert und nach dem Auslesen aus dem Speicher in ein Analogsignal zurückverwandelt wird.

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Nachrichtensignal mit Hilfe eines Analog/Digitalwandlers in durch Dualzahlen dargestellte Abtastwerte digitalisiert wird, dass die Frequenzumsetzung durch Multiplikation dieser Zahlenfolgen mit Abtastwerten der entsprechenden Trägerschwingungen darstellenden Zahlenfolgen durchgeführt werden, dass zur Gewinnung der Teilfrequenzbänder digitale Filter eingesetzt werden, wobei diese Teilfrequenzbänder als Folge von Abtastwerten in Form von Dualzahlen entstehen, dass die Teilfrequenzbänder zur Vertauschung in einem Speicher gespeichert werden, dass die Teilfrequenzbänder nach dem Auslesen aus dem Speicher durch Multiplikation mit Trägerschwingungen darstellenden Binärzahlenfolgen umgesetzt werden, dass die als Binärzahlenfolgen vorliegenden Teilfrequenzbänder nur addiert werden und deren Summe in einem Digital/Analogwandler wieder in ein Analogsignal zurückverwandelt wird, das zum Empfänger übertragen wird.

8. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass bei der Speicherung der Teilfrequenzband-Zeitelemente die Speicheradressansteuerung einer monoton steigenden natürlichen Zahlenfolge entspricht, so dass die Teilfrequenzband-Zeitelemente in einer natürlichen zeitlichen Folge am Signalausgang erscheinen.

9. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass bei der Speicherung der Teilfrequenzband-Zeitelemente die Speicheradressansteuerung einer monoton fallenden natürlichen Zahlenfolge entspricht, so dass die Teilfrequenzband-Zeitelemente zeitinvertiert am Signalausgang erscheinen.

10. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass die Speicherung der Teilfrequenzband-Zeitelemente im Wechsel einmal in ihrer natürlichen zeitlichen Folge und dann wieder verwürfelt erfolgt.

11. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass in einem ersten Verarbeitungsschritt für jede Spalte/Zeile der Matrix aus einer vorbestimmten Menge wirksamer Frequenzvertauschungen/Zeitverwürfelungen je eine ausgewählt wird, nach der die Elemente der jeweiligen Spalte/Zeile entsprechend umgestellt werden, dass danach in einem zweiten Verarbeitungsschritt für jede Zeile/Spalte der so entstandenen Matrix ebenfalls aus einer vorbestimmten Menge wirksamer Zeitverwürfelungen/Frequenzbandvertauschungen je eine ausgewählt wird, nach der die Elemente der jeweiligen Zeile/Spalte der Matrix vertauscht werden, dass diese zweimalige Umformung der Matrix für jeden Nachrichtenblock neu gewählt wird und dass diese zweimal umgeformte Matrix spaltenweise ausgelesen wird.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass die Matrixumformung mehrfach vorgenommen wird.

13. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass die Matrixumformung in einem Schritt vorgenommen wird.

14. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass als Anfangsmatrix zur Verwürfelung des nächsten Nachrichtenblocks die Endmatrix des vorhergehenden Nachrichtenblocks verwendet wird.

15. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass für jeden Nachrichtenblock neu gewählt wird, ob im ersten Verarbeitungsschritt die Zeilen und im zweiten Verarbeitungsschritt die Spalten vertauscht werden oder umgekehrt.

Für die Verschleierung und nachherigen Entschleierung von Nachrichtensignalen sind die Verfahren der Zeitverwürfelung und der Frequenzbandvertauschung bekannt.

Bei der Frequenzbandvertauschung ist z. B. die Übertragungsbandbreite der Signale in eine Anzahl gleich breiter Teilkanäle unterteilt. Durch eine quasistatistische Zeichenfolge werden durch Frequenzumsetzer in bestimmten Zeitabständen die Frequenzplätze der Teilkanäle vertauscht. Es sind dabei die Vertauschungen den Binärzeichen des Quasizufallsgenerators fest zugeordnet. Die empfangsseitige Rückvertauschung der Teilkanäle in ihre natürliche Lage erfolgt durch die umgekehrte Anwendung einer der sendeseitigen Zeichenfolge identischen Quasizufallsfolge.

Bei Zeitverwürfelungsverfahren werden innerhalb eines periodischen Zeitabschnitts einzelne Zeitelemente entsprechend den Anweisungen eines Quasizufallsgenerators vertauscht und empfangsseitig zurückvertauscht.

Ein wesentlicher Nachteil der bekannten Verschleierungsverfahren besteht in der verhältnismässig leichten Erkennbarkeit des Klartextes aus dem verschleierten Signal.

Dies gilt insbesondere dann, wenn in einem schmalbandigen Übertragungskanal übertragen werden muss, weil hier die Anzahl der Teilkanäle nicht ausreichend gross gewählt werden kann. Bei der Zeitverwürfelung setzt die noch zumutbare Zwischenspeicherzeit der Anzahl der Zeitelemente eine klare Grenze.

Die zu der Erfindung führende Aufgabe war es, ein Verfahren zur Nachrichtenverschleierung und nachherigen Entschleierung anzugeben, das die beiden bisher bekannten Verfahren, Zeitverwürfelung und Frequenzbandvertauschung derart miteinander kombiniert, dass ein Vielfaches an Sicherheit

gegen unbefugtes Entschleiern erreicht wird.

Die Lösung der Aufgabe erfolgt, wie im Anspruch 1 beschrieben. Zweckmässige Ausführungen sind in den abhängigen Ansprüchen beschrieben.

Nachstehend werden anhand der Figuren Ausführungsformen des erfindungsgemässen Verfahren näher erläutert. Es zeigen:

Figur 1a die mögliche Einteilung der zu übertragenden Nachricht in n Zeitelemente der Dauer T und m gleiche Teilfrequenzbänder der Bandbreite B in der Frequenz-Zeitebene.

Figur 1b die mögliche Verwürfelung der (n·m)-Teilfrequenzband-Zeitelemente bei nacheinander angewendeter Zeitverwürfelung und Frequenzbandvertauschung.

Figur 1c die mögliche Verwürfelung der (n·m)-Teilfrequenzband-Zeitelemente nach dem erfindungsgemässen Verschleierungsverfahren.

Figur 2 schematisch ein nicht voll digital arbeitendes Ausführungsbeispiel eines Verschleierungsgerätes nach dem erfindungsgemässen Mischverfahren, das zum Senden und Empfangen benutzt werden kann.

Figur 3 schematisch ein voll digital arbeitendes Ausführungsbeispiel eines Verschleierungsgerätes nach dem erfindungsgemässen Mischverfahren, das zum Senden und Empfangen benutzt werden kann.

Wird nun auf einen Nachrichtenblock nach Figur 1a sowohl das Zeitverwürfelungsverfahren und anschliessend die Frequenzbandvertauschung oder umgekehrt angewendet, so entspricht der zur Übertragung gelangende transformierte Nachrichtenblock der Darstellung in Figur 1b. Alle Bandelemente m innerhalb eines Zeitelementes der Dauer T sind nach der Verwürfelung wieder Bandelemente eben dieses, wenngleich zeitverwürfelten Zeitelementes. Ein Austausch der Bandelemente mit solchen anderer Zeitelemente findet nicht statt, bedingt durch die additive Überlagerung beider Verfahren.

Durch das erfindungsgemässe Verfahren wird eine vollständige Verwürfelung der Teilfrequenzband-Zeitelemente innerhalb des Nachrichtenblocks erreicht. Der Nachteil der additiven Überlagerung (Figur 1b) wird durch die vorteilhafte vollständige Mischung ersetzt, wie in Figur 1c dargestellt.

Das erfindungsgemässe Verfahren wird nun anhand eines Ausführungsbeispiels nach Figur 2 näher erläutert.

Das zu übertragende Nachrichtensignal wird dem in Figur 2 dargestellten Gerät bei E dem Eingangstiefpass ETP zugeführt und ausgangsseitig an die Eingänge der zur Bildung der m Teilfrequenzbänder erforderlichen Ringmodulatoren ME1 bis MEm weitergeleitet. Jedem der Ringmodulatoren ist ein Bandfilter BFE1 bis BFEm nachgeschaltet, wodurch die m Teilfrequenzbänder in identischer Frequenzlage an m Eingangsleitungen eines Analogmultiplexers AMX anliegen. Am Ausgang des dem Analogmultiplexer nachgeschalteten Analog/Digitalwandlers A/D erscheint somit das mit der Abtastfrequenz multiplizierte Zeitmultiplexsignal der Teilfrequenzbänder in digitalisierter Form. In einem ersten Zwischenspeicherschritt wird die Nachrichtenspeichermatrix gemäss Figur 1a gefüllt. In einem zweiten Zwischenspeicherschritt für den nun folgenden Nachrichtenblock erfolgt das Zwischenspeichern gemäss Figur 1c, wobei vor dem Einschreiben in die Speicherzellen derart Inhalt abgefragt und an den Digital/Analogwandler D/A weitergeleitet wird. In dem nun folgenden Zwischenspeicherschritt erfolgt die Eingabe wieder gemäss Figur 1a, dann wieder gemäss Figur 1c usw.

Das Einlese-Ausleseschema gemäss Figur c wird von einem Quasizufallsgenerator gesteuert, welcher für eine quasizufällige Verteilung der Teilfrequenzbandelemente innerhalb der Matrix sorgt, was bezogen auf die Signalausgabe zu einer vollständigen Mischung der Verfahren Frequenzbandvertauschung und Zeitverwürfelung führt.

Der dem Digital/Analogwandler D/A nachgeschaltete Analogdemultiplexer ADMX läuft synchron mit dem Analogmultiplexer AMX und führt die Abtastwerte den den Teilfrequenzbändern zugeordneten Bandpässen BFA1 bis BFAm zu, ihnen nachgeschaltet sind die Ringmodulatoren MA1 bis MAm, deren ausgangsseitige Zusammenfassung über den Ausgangstiefpass im Sendeteil das Sendesignal erzeugt.

Im Empfangsbetrieb wird nun ein so erzeugtes Sendesignal einem anderen Gerät in Punkt E eingespeist, wobei die Signalverarbeitung wie im Sendebetrieb verläuft, nur dass der Quasizufallsgenerator des Empfängers anstatt der Vertauschungsmatrix gemäss Figur 1c die hierzu Inverse anliefert, welche zusätzlich um einen Zwischenspeicherschritt verzögert (bezogen auf Sendebetrieb) die Adressierung des Nachrichtenzwischenspeichers steuert. Beim Empfangsbetrieb sind die beiden Schalter auf Figur 2 umzuschalten, ferner muss davon ausgegangen werden, dass die Quasizufallsgeneratoren synchron laufen. Dies wird z. B. durch eine Präambelsynchronisation bei jedem Gesprächsrichtungswechsel bewirkt.

Durch entsprechende Adressinvertierung am Nachrichtenzwischenspeicher und durch Umschaltung der Träger an den Ringmodulatoren ist auch die Aussendung von bandinvertierten und zeitinvertierten Nachrichtenelementen möglich.

Das in Figur 3 dargestellte erfindungsgemässe Ausführungsbeispiel eines Verschlüsselungsgerätes nach dem Mischverfahren unterscheidet sich im Ergebnis nicht von dem in Figur 2 dargestellten Gerät. Die Realisierung bedient sich hier statt einzelner Ringmodulatoren und Bandpässe eines digitalen Multiplizierers ME und eines digitalen Tiefpasses DTP1, weshalb der Analog/Digitalwandler A/D sofort im Anschluss an den analog ausgebildeten Eingangstiefpas TPE angeschlossen ist. Der Multiplizierer ME dient als Modulator, an welchen der digitale Tiefspass DTP1 angeschlossen ist. Die digitale Realisierung hat den Vorteil, dass der Mischer ME und der digitale Tiefpass DTP1 im Zeitmultiplex mehrfach genutzt werden können, weshalb am Ausgang des digitalen Tiefpasses DTP1 die Teilfrequenzbänder im Zeitmultiplex in gleicher Frequenzlage vorliegen. Die einzelnen digitalisierten Träger für den Multiplizierer ME sind in der sin/cos-Tafel SCT abgespeichert.

Die cos-Tafel ist erforderlich, da bei dieser Realisierung die Einseitenbandgewinnung nach der Phasenmethode von Weaver (D.K. Weaver jr.: «A third method of generation and detection of single sideband signals», Proceedings of IRE, Dez. 1956, Seiten 1703 bis 1705) erfolgt. Hierbei wird das umzusetzende Signal in zwei Kanälen mit je einer cos- bzw. sin-Schwingung derselben Frequenz, die in der Bandmitte liegt, moduliert. Aus dem entstandenen Modulationsprodukt werden anschliessend mittels Tiefpassfilter die Summenfrequenzen entfernt. Die Ausgangssignale dieser Filter werden anschliessend mit je einer sin- bzw. cos-Schwingung derselben Frequenz, die bis jetzt aber in der Mitte des Bandes liegt, in die das Signal umgesetzt werden soll, moduliert. Die Summe der so entstandenen Modulationsprodukte stellt schliesslich das neue Frequenzband dar, in die das ursprüngliche Signal umgesetzt wurde.

Werden bei der ausgangsseitigen Modulation die sin- und cos-Schwingung miteinander vertauscht, so liefert die Summe das neue Frequenzband in invertierter Frequenzlage.

Die Anpassung der Bitrate an den Nachrichtenfluss geschieht hier durch Abspeicherung minimal jedes ½-m-ten Abtastwertes in die Nachrichtenspeichermatrix. Da diese Verminderung der Abtastfrequenz einer neuerlichen Mischung des Signales gleichkommt, muss dies durch Wiederherstellung der Bitrate am digitalen Tiefpass DTP2 rückgängig gemacht werden. An den digitalen Tiefpass DTP2 schliesst sich der digitale Ausgangsmultiplizierer MA an, er multipliziert die Zahlenwerte des digitalen Tiefpasses DTP2 mit denselben Zahlenwerten wie der digitale Eingangsmultiplizierer. Der dem digitalen Ausgangsmultiplizierer MA folgende Akkumulator vereinigt die Teilbänder wieder zum «verwürfelten» oder «entwürfel-

ten» Nachrichtenkanal, welcher durch den Digital-Analogwandler D/A und anschliessenden analogen Ausgangstiefpass TPA wieder als Analogsignal im Punkte A der Schaltung ansteht. Die Teilfrequenzbandinversion geschieht hier im Gegensatz zum Schaltungsbeispiel in Figur 2 durch Rückmischung der durch Multiplikation mit digitalisierten sin-Trägern gewonnenen Teilfrequenzbänder im digitalen Multiplizierer ME mittels digitaler cos-Träger und umgekehrt im digitalen Multiplizierer MA, was über die Ausgabesteuerung der Nachrichtenspeichermatrix einfach realisierbar ist. Alle weiteren Betrachtungen sind analog der Beschreibung zur Realisierung gemäss Figur 2.

Ein weiteres Ausführungsbeispiel vermeidet die kryptologisch unwirksamen Vertauschungen, die bei der Fülle rein statistischer Vertauschungen der Elemente der (n·m)-Matrix vorkommen könnten und erhöht damit die Sicherheit der Verschleierung.

Diese Verbesserung wird dadurch erreicht, dass in einem ersten Verarbeitungsschritt von einem Schlüsselgeber für jede Zeile/Spalte der Matrix je eine Zeitverwürfelung/Frequenzbandvertauschung aus einer vorbestimmten Menge wirksamer, gespeicherter Zeitverwürfelungen/Frequenzbandvertauschungen ausgewählt wird. Die Elemente einer Zeile/Spalte der Matrix werden entsprechend der Reihenfolge der ausgesuchten Vertauschungen umgestellt. In einem zweiten Verarbeitungsschritt werden vom Schlüsselgeber für die Spalten/Zeilen der Zwischenmatrix je eine Frequenzbandvertauschung/Zeitverwürfelung aus einer vorbestimmten Menge wirksamer gespeicherter Frequenzbandvertauschungen/Zeitverwürfelungen ausgewählt. Die Elemente der Spalten/Zeilen der Zwischenmatrix werden entsprechend der Reihenfolge der ausgesuchten Vertauschungen umgestellt.

Werden im ersten Verarbeitungsschritt die Frequenzbandvertauschungen und im zweiten Verarbeitungsschritt die Zeitverwürfelungen vorgenommen, ergibt sich eine andere Matrix als bei umgekehrter Reihenfolge der Verarbeitungsschritte, auch wenn dieselben Frequenzbandvertauschungen und Zeitverwürfelungen ausgewählt wurden.

Verwendet man als Anfangsmatrix für die Verwürfelung des nächsten Nachrichtenblocks die Endmatrix des vorhergehenden Nachrichtenblocks, dann ergibt sich der Vorteil, dass für das Zwischenspeichern der Nachrichtenelemente nur ein Speicher für die Elemente eines Nachrichtenblocks benötigt wird.

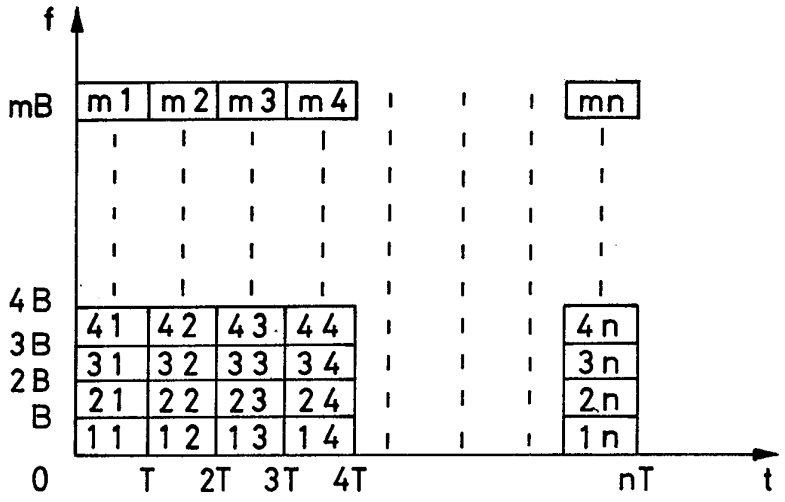


Fig. 1a

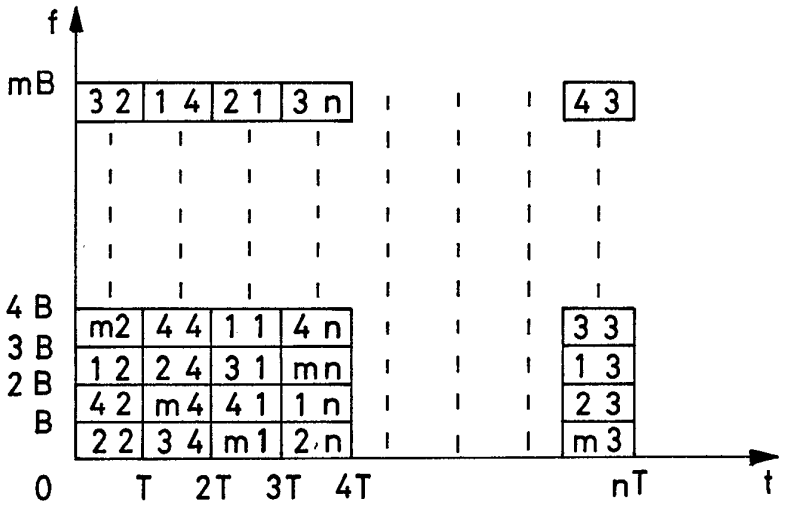


Fig. 1b

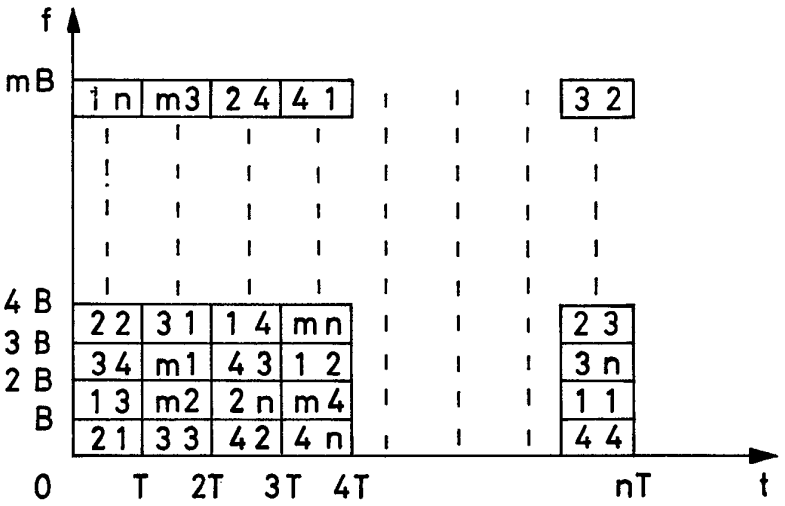


Fig. 1c

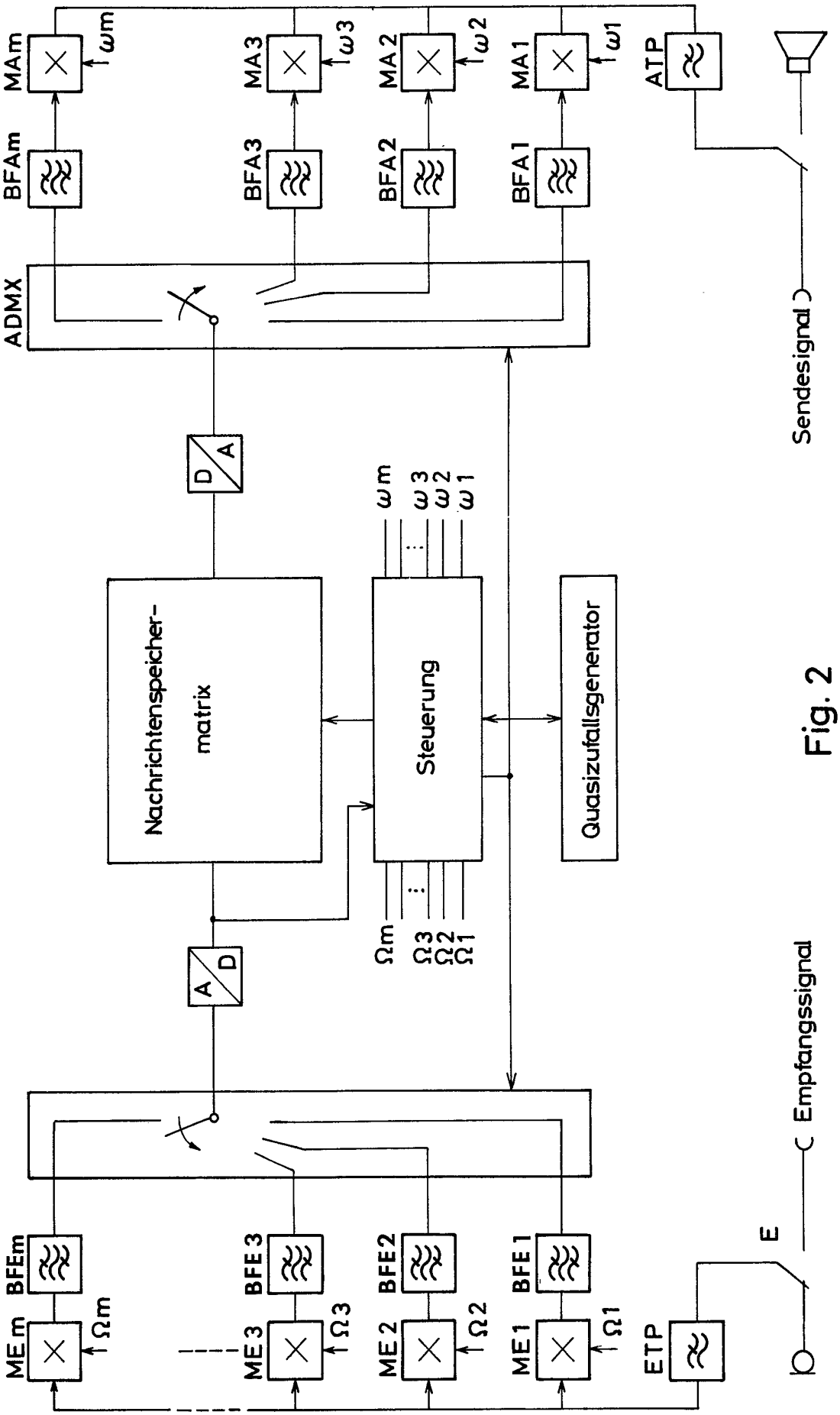

MAm
ωm
MA3
ω3
MA2
ω2
MA1
ω1
ATP
BFAm
BFA3
BFA2
BFA1
ADMX
Sendesignal
D/A
ωm ω3 ω2 ω1
Nachrichtenspeicher-matrix
Steuerung
Quasizufallsgenerator
A/D
Ωm Ω3 Ω2 Ω1
BFEm
BFE3
BFE2
BFE1
E
Empfangssignal
ME m
Ωm
ME 3
Ω3
ME 2
Ω2
ME 1
Ω1
ETP

Fig. 2

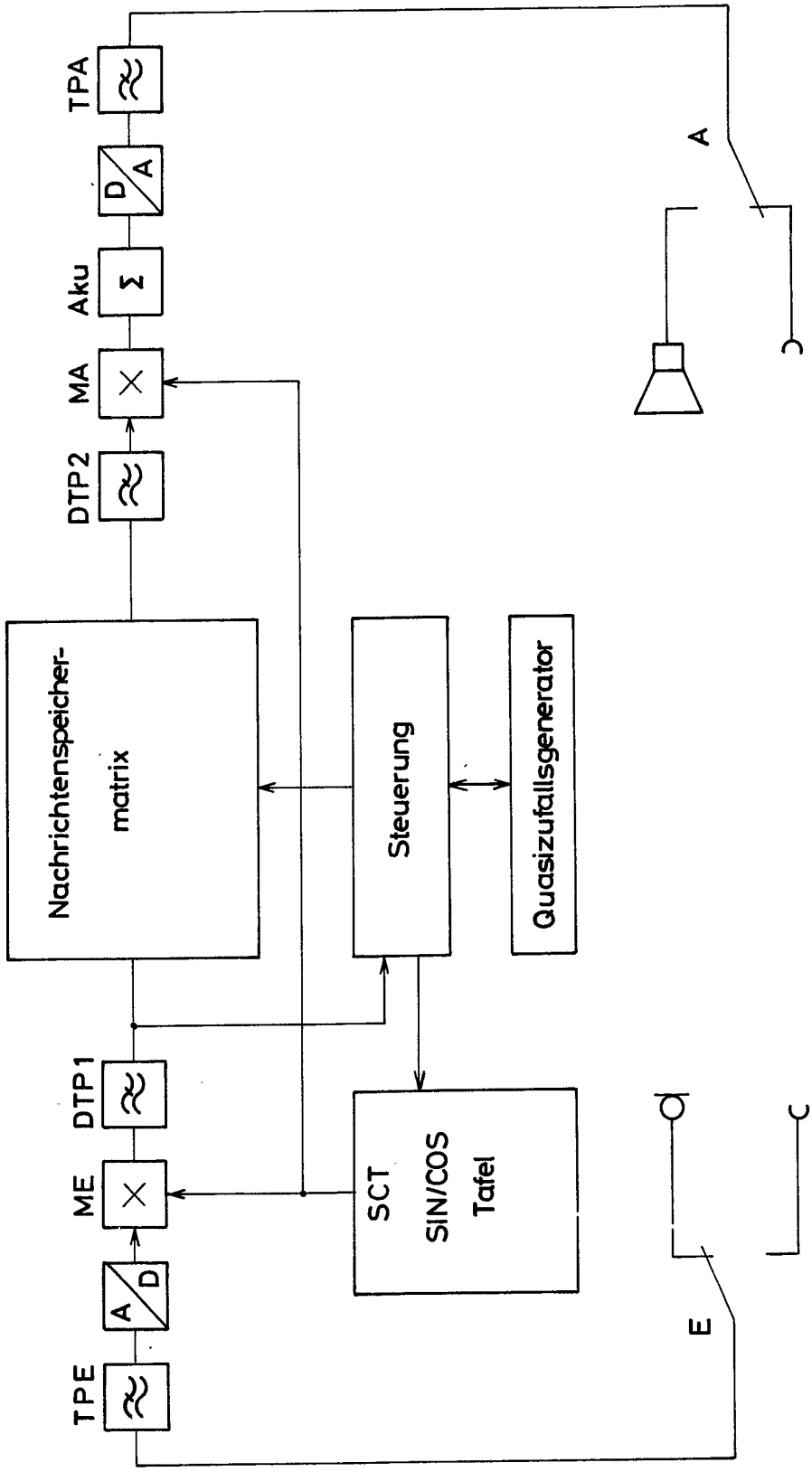

TPA
D/A
Aku
Σ
MA
DTP2
Nachrichtenspeicher-
matrix
Steuerung
Quasizufallsgenerator
DTP1
ME
A/D
TPE
SCT
SIN/COS
Tafel
A
C
d
E

Fig. 3