(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
20. Februar 2003 (20.02.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/015328 A2

(51) Internationale Patentklassifikation[7]: H04K 1/06

(21) Internationales Aktenzeichen: PCT/EP02/08661

(22) Internationales Anmeldedatum:
2. August 2002 (02.08.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 38 650.8 7. August 2001 (07.08.2001) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E. V.** [DE/DE]; Leonrodstrasse 54, 80636 München (DE).

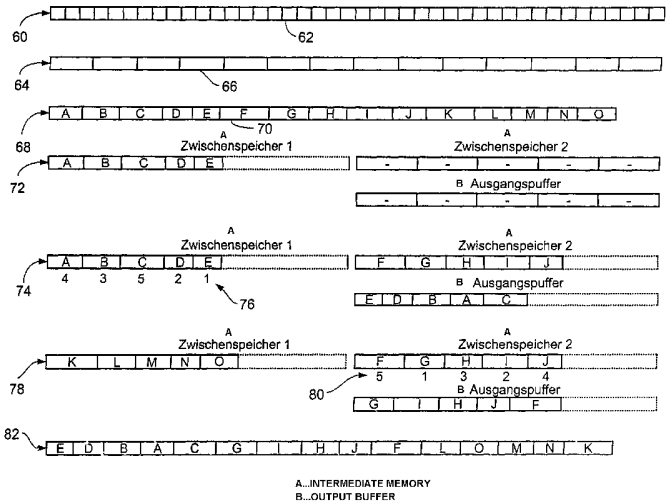
(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **DISCH, Sascha** [DE/DE]; Spinnereistrasse 28, 91052 Erlangen (DE). **HILPERT, Johannes** [DE/DE]; Herrnhüttestrasse 46, 90411 Nürnberg (DE). **LUTZKY, Manfred** [DE/DE]; Heinrich-von-Brentano-Strasse 9, 90427 Nürnberg (DE). **GAYER, Marc** [DE/DE]; Haagstrasse 32, 91054 Erlangen

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR ENCRYPTING A DISCRETE SIGNAL AND METHOD AND DEVICE FOR DECRYPTING THE SAME

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUM VERSCHLÜSSELN EINES DISKRETEN SIGNALS SOWIE VERFAHREN UND VORRICHTUNG ZUR ENTSCHLÜSSELUNG



(57) Abstract: The invention relates to a method for encrypting a discrete signal that consists of subsequent scanned values (62), according which subsequent scanned values (62) are divided up into subsequent time blocks (66) and the subsequent time blocks (66) are then encoded in encoded data blocks (70) having a predetermined order. The predetermined order of the encoded data blocks (70) is then modified in accordance with a predetermined exchange instruction (76, 80). Due to the integration of a time discontinuity, the inventive method allows a very high security of encryption. Mistakes that occur when signals encrypted in this manner are processed without authorization can be prevented and the compatibility with standard codings can be ensured by carrying out the modification of the chronological order after the discrete signal has been encoded, that is with respect to encoded data blocks into which an encoder encodes the discrete signal.

(57) Zusammenfassung: Bei einem erfindungsgemäßen Verfahren zum Verschlüsseln eines diskreten Signals, das aus aufeinanderfolgenden Abtastwerten (62) besteht, werden die aufeinanderfolgenden Abtastwerte (62) in aufeinanderfolgende Zeitblöcke (66) eingeteilt und die aufeinanderfolgenden

[Fortsetzung auf der nächsten Seite]

WO 03/015328 A2

(DE). **BARTHOLOMÄUS, Reinfried** [DE/DE]; Engelstrasse 18, 91054 Erlangen (DE).

(74) Anwälte: SCHOPPE, Fritz usw.; Schoppe, Zimmermann, Stöckeler & Zinkler, Postfach 71 08 67, 81458 München (DE).

(81) Bestimmungsstaat *(national)*: US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Zeitblöcke (66) daraufhin in kodier-te Datenblöcke (70) mit einer vorbestimmten Reihenfolge ko-diert. Anschließend wird die vorbestimmten Reihenfolge der kodierten Datenblöcke (70) gemäß einer vorbestimmten Vertau-schungsvorschrift (76, 80) geändert. Die zugrundeliegende Er-kenntnis besteht darin, daß eine sehr hohe Sicherheit der Verschlüsselung durch Einführung einer zeitlichen Diskonti-nuität erzielt werden kann, und daß das Auftreten von Fehlern bei einer unauthorisierten Verarbeitung derartig verschlüs-selter Signale dadurch verhindert und die Verträglichkeit mit Standardkodierungen dadurch gewährleistet werden kann, daß die Änderung der zeitlichen Reihenfolge nach einer Kodierung des diskreten Signals , d.h. bezüglich kodierter Datenblöcke, in die ein Kodierer das diskrete Signal kodiert, durchgeführt wird.

Verfahren und Vorrichtung zum Verschlüsseln eines diskreten Signals sowie Verfahren und Vorrichtung zur Entschlüsselung

Beschreibung

Die vorliegende Erfindung bezieht sich auf die Verschlüsselung diskreter Signale, wie z.B. auf die Verschlüsselung von Sprachinformationen, bzw. die entsprechende Entschlüsselung.

Bei der Nutzung, Übertragung, Verwaltung und Archivierung von Audiomaterial ist es häufig wünschenswert, die entsprechenden Inhalte vor einem unbefugten Zugriff zu schützen. Besonders im Bereich der Sprachaufzeichnung besteht die Notwendigkeit, daß ein unbefugtes Abspielen oder heimliches Abhören bei der Übertragung verhindert werden kann. Gleichzeitig soll jedoch das verwendete Datenformat weiterhin gültig bleiben, damit die zum Abspielen verwendeten Geräte auch bei einem unberechtigten Zugriff nicht in Fehlerzustände übergehen. Dies gilt insbesondere für komprimierende Datenformate wie z.B. die Datenformate gemäß den Standards MPEG2 Layer 3 und MPEG2/4 AAC (AAC = Advanced Audio Coding = fortgeschrittene Audiokodierung).

Bei den Audioanwendungen kommt hinzu, daß die verschlüsselten Signale beim Abhören ohne Entschlüsselung der Abhöranlage keinen Schaden zufügen dürfen. Die verschlüsselten Signale sollten deshalb derart verschlüsselt sein, daß sie bei Abspielen ohne Entschlüsselung kein Knacksen, Krachen oder andere extreme Dynamiksprünge erzeugen. Während es bei der Verschlüsselung von Musikdaten häufig genügt, die Qualität der unauthorisierten Wiedergabe stark einzuschränken, wird bei Sprachinhalten insbesondere gefordert, daß bei unauthorisierter Nutzung die Wiedergabequalität der verschlüsselten Daten eine Verständlichkeit der Sprachinformationen, die beispielsweise Interviews, Reportagen usw. sein können, nicht mehr gestatten soll.

In der Patentanmeldung WO99/51279 mit dem Titel „Vorrichtung und Verfahren zum Erzeugen eines verschlüsselten Audio- und/oder Videostroms", deren Anmelderin ebenfalls die Fraunho-

fer-Gesellschaft ist, wird ein Verfahren zur Verwürfelung von kodierten Audiodaten beschrieben, das auf Vertauschungen von Linien im Frequenzbereich basiert. Mit diesem Verfahren gelingt es, Musiksignale weitgehend unkenntlich zu machen. Bei Sprachinhalten jedoch ist die genaue spektrale Zusammensetzung des Signals für die Verständlichkeit von geringem Belang, so daß, obwohl die Stimme eines Sprechers stark verfremdet wird, der Inhalt des Gesprochenen bzw. die Sprachinformationen verständlich bleiben.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein Verfahren und eine Vorrichtung zum Verschlüsseln eines diskreten Signals sowie ein Verfahren und eine Vorrichtung zur entsprechenden Entschlüsselung zu schaffen, so daß die Verschlüsselung einerseits möglichst sicher und andererseits keine Fehler bei einer unauthorisierten Verarbeitung hervorruft und mit bisherigen Kodierungen verträglich ist.

Diese Aufgabe wird durch ein Verfahren gemäß Anspruch 1 oder 8 und eine Vorrichtung gemäß Anspruch 2 oder 9 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß eine sehr hohe Sicherheit der Verschlüsselung durch Einführung einer zeitlichen Diskontinuität erzielt werden kann, und daß das Auftreten von Fehlern bei einer unauthorisierten Verarbeitung derartig verschlüsselter Signale dadurch verhindert und die Verträglichkeit mit Standardkodierungen dadurch gewährleistet werden kann, daß die Änderung der zeitlichen Reihenfolge nach einer Kodierung des diskreten Signals , d.h. bezüglich kodierter Datenblöcke, in die ein Kodierer das diskrete Signal kodiert, durchgeführt wird. Auf diese Weise wird einerseits verhindert, daß ein Dekodierer, der das verschlüsselte Signal empfängt, nicht in undefinierte Zustände gelangt, da bei der Verschlüsselung die zeitliche Diskontinuität in Einheiten von kodierten Datenblöcken erzeugt wird. Andererseits wird verhindert, daß beim Zusammenspiel mit einem beliebigen Kodierverfahren, wie z.B. bei einem komprimierenden Kodierverfahren, die demselben zugrunde liegenden zeitlichen Annahmen, wie z.B.

die zeitliche und spektrale Verdeckung in dem Fall von psychoakustischen Audioverfahren, weiterhin gültig bleiben und somit die erfindungsgemäße Verschlüsselung mit solchen Kodierungen verträglich und die Implementierung der erfindungsgemäßen Verschlüsselung vereinfacht ist.

Bei einer Verschlüsselung gemäß der vorliegenden Erfindung werden die aufeinanderfolgenden Abtastwerte eines diskreten Signals in aufeinanderfolgende Zeitblöcke eingeteilt, die daraufhin in kodierte Datenblöcke mit einer vorbestimmten Reihenfolge kodiert werden. Anschließend wird die vorbestimmte Reihenfolge der kodierten Datenblöcke gemäß einer vorbestimmten Vertauschungsvorschrift geändert.

Bei der Entschlüsselung gemäß der vorliegenden Erfindung wird die Reihenfolge der kodierten Datenblöcke eines verschlüsselten Signals, das einem diskreten Signal, das aus aufeinanderfolgenden Abtastwerten besteht, in verschlüsselter Form entspricht, gemäß einer vorbestimmten Vertauschungsvorschrift bzw. einer inversen Vertauschungsvorschrift geändert, woraufhin die kodierten Datenblöcke in geänderter Reihenfolge in aufeinanderfolgende Zeitblöcke mit einer vorbestimmten Reihenfolge dekodiert werden. Dadurch werden aus den aufeinanderfolgenden Zeitblöcken die aufeinanderfolgenden Abtastwerte des diskreten Signals erzeugt.

Gemäß einem Ausführungsbeispiel der vorliegenden Erfindung wird die Änderung der vorbestimmten Reihenfolge der kodierten Datenblöcke bei der Verschlüsselung durch Permutieren einer vorbestimmten Anzahl von aufeinanderfolgenden Datenblöcken der kodierten Datenblöcke erreicht, wobei hierzu ein Permutationsvektor als Vertauschungsvorschrift erzeugt wird. Die Permutation kann bezüglich aufeinanderfolgender Gruppen von kodierten Datenblöcken mit gleicher Größe bzw. Länge durchgeführt werden. Für jede Permutationsgruppe kann ein anderer Permutationsvektor erzeugt und verwendet werden. Die Erzeugung der Permutationsvektoren findet bei der Dekodierung auf eine vorbestimmte Weise statt, wobei eine korrekte Entschlüsselung da-

durch gewährleistet wird, daß bei der Entschlüsselung zur Rückpermutation der Gruppen von kodierten Datenblöcken entsprechende inverse Permutationsvektoren erzeugt und verwendet werden.

Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend bezugnehmend auf die beiliegenden Zeichnungen näher erläutert. Es zeigen:

Fig. 1 ein Blockschaltbild einer Verschlüsselungsvorrichtung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung;

Fig. 2 ein Blockschaltbild einer Entschlüsselungsvorrichtung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung;

Fig. 3 eine schematische Skizze, die ein exemplarisches Ausführungsbeispiel einer Verschlüsselung zeigt; und

Fig. 4 eine schematische Skizze, die ein exemplarisches Ausführungsbeispiel einer Entschlüsselung zeigt.

Bevor im folgenden die vorliegende Erfindung anhand der Fig. 1 bis 4 näher erläutert wird, wird darauf hingewiesen, daß, obwohl sich die nachfolgende Beschreibung auf die Verschlüsselung von Audiosignalen bezieht, die vorliegende Erfindung ferner auch auf andere diskrete Signale anwendbar ist, wie z.B. auf die Verschlüsselung von Bild- und Videosignalen.

In Fig. 1 ist eine Verschlüsselungsvorrichtung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung gezeigt, die ein diskretes Zeitsignal bzw. ein Audiosignal in kodierte Datenblöcke in verschlüsselter Form umwandelt. Die Vorrichtung von Fig. 1 umfaßt im wesentlichen einen psychoakustischen Kodierer 10, der das Zeitsignal empfängt und in kodierte Datenblöcke umwandelt bzw. kodiert, und eine Einrichtung 12 zur Änderung der Reihenfolge der kodierten Datenblöcke.

Der psychoakustische Kodierer 10 umfaßt eine Einrichtung 14 zur Einteilung der aufeinanderfolgenden diskreten Abtastwerte, aus denen das Zeitsignal besteht, in Zeitblöcke und eine Einrichtung 16 zur Kodierung der Zeitblöcke in kodierte Datenblöcke.

Die Einrichtung 12 zur Änderung der Reihenfolge umfaßt eine Einrichtung 18 zur Erzeugung eines Permutationsvektors, eine Schreibeinrichtung 20, einen ersten Zwischenspeicher 22, einen zweiten Zwischenspeicher 24 und eine Ausleseeinrichtung 26. Ein Eingang der Schreibeinrichtung 20 ist mit einem Ausgang des psychoakustischen Kodierers 10 bzw. der Einrichtung 16 zur Kodierung verbunden, während zwei Ausgänge derselben mit jeweils einem Eingang des ersten und zweiten Zwischenspeichers 22 und 24 verbunden sind. Ein Ausgang der Einrichtung 18 zur Erzeugung eines Permutationsvektors ist mit einem Eingang der Ausleseeinrichtung 26 verbunden, um einen Permutationsvektor an dieselbe auszugeben, wobei die Ausleseeinrichtung zwei weitere Eingänge aufweist, die mit den Ausgängen der Zwischenspeicher 22 und 24 verbunden sind. Die Ausleseeinrichtung 26 ist an einem Ausgang mit einem Ausgangspuffer 28 verbunden, um an denselben kodierte Datenblöcke in verschlüsselter Form auszugeben.

Nachdem im vorhergehenden der Aufbau der Verschlüsselungsvorrichtung von Fig. 1 beschrieben worden ist, wird nachfolgend die Funktionsweise desselben beschrieben.

Das Zeitsignal ist ein diskretes Audiosignal, das aus aufeinanderfolgenden Abtastwerten besteht. Der psychoakustische Kodierer 10 basiert beispielsweise auf einem Kodierverfahren des AAC-Standards. Die Einrichtung 14 teilt die aufeinanderfolgenden Abtastwerte beispielsweise in Zeitblöcke mit einer Anzahl aufeinanderfolgender Abtastwerte ein, die gleich einer Potenz von 2 ist. Zur Handhabung von Aliasingeffekten kann es vorgesehen sein, eine Einteilung in sich gegenseitig überschneidende Zeitblöcke vorzusehen, so daß jeder Abtastwert zwei Zeit-

blöcken zugeteilt wird, wie es beispielsweise bei der AAC-Kodierung der Fall ist.

Die Einrichtung 16 zur Kodierung der Zeitblöcke in kodierte Datenblöcke empfängt die Zeitblöcke von der Einrichtung 14 in zeitlicher Reihenfolge und führt daraufhin die Kodierung derselben durch. Die Kodierung eines Zeitblocks kann entweder einzeln bzw. isoliert Zeitblock für Zeitblock oder abhängig von vorhergehenden und nachfolgenden Zeitblöcken durchgeführt werden, um beispielsweise psychoakustische Modelle, wie z.B. die zeitliche und spektrale Verdeckung, zu berücksichtigen. Die Einrichtung 16 zur Kodierung der Zeitblöcke gibt die kodierten Datenblöcke an die Schreibeinrichung 20 in einer vorbestimmten, von dem Kodierverfahren abhängigen Reihenfolge aus. Die Datenblöcke können entweder alle dieselbe Länge oder unterschiedliche Längen aufweisen, wie z.B. in dem Fall, daß die Datenblöcke einen MPEG2/4 AAC konformen Aufbau aufweisen.

Die Schreibeinrichtung 20 empfängt die kodierten Datenblöcke und schreibt die kodierten Datenblöcke nacheinander in einen aktuellen der Zwischenspeicher 22 und 24, wobei dieselben zusammen als ein Wechselpuffer wirken, wie es im folgenden beschrieben wird. Die Größe der Zwischenspeicher 22 und 24 ist ausreichend bemessen, um N kodierte Datenblöcke zu speichern, wobei N eine Ganzzahl größer 1 ist (N>1). Die Schreibeinrichtung 20 beschreibt den aktuellen der Speicher 22 und 24 in der Reihenfolge, in der die kodierten Datenblöcke von der Einrichtung 16 übertragen werden so lange, bis sich N kodierte Datenblöcke in dem aktuellen der Zwischenspeicher 22 und 24 befinden. Wenn der aktuelle der Zwischenspeicher 22 und 24 voll ist, d.h. N gespeicherte kodierte Datenblöcke aufweist, liest die Ausleseeinrichtung 26 den gerade gefüllten Zwischenspeicher 22 und 24 aus, während die Schreibeinrichtung 20 den anderen der beiden Zwischenspeicher 22 bzw. 24 mit den kodierten Datenblöcken von der Einrichtung 16 in der Reihenfolge ihres Empfangs beschreibt.

Die Ausleseeinrichtung 26 liest den zuletzt vollständig beschriebenen Zwischenspeicher 22 bzw. 24 in einer anderen Reihenfolge aus, als derselbe beschrieben wurde. Genauer ausgedrückt liest die Ausleseeinrichtung 26 den jeweiligen Zwischenspeicher 22 bzw. 24 in einer permutierten Reihenfolge aus, die durch einen Permutationsvektor der Größe N festgelegt wird, der durch die Einrichtung 18 zur Erzeugung eines Permutationsvektors erzeugt und zugeführt wird, wie es im folgenden beschrieben werden wird. Durch das permutierte Auslesen wird die Reihenfolge der N kodierten Datenblöcke gemäß einer Vertauschungsvorschrift geändert, die durch den Permutationsvektor festgelegt wird. Die in permutierter Reihenfolge ausgelesenen kodierten Datenblöcke bilden zusammen eine Permutationsgruppe von kodierten Datenblöcken, die die Ausleseeinrichtung 26 an den Ausgangspuffer 28 ausgibt, an den sich beispielsweise eine Computerschnittstelle (nicht gezeigt) anschließt.

Die Einrichtung 18 erzeugt den Permutationsvektor der Größe N, der die Vertauschungsvorschrift festlegt, basierend auf welcher die kodierten Datenblöcke einer Permutationsgruppe permutiert werden, für jede Permutationsgruppe neu. Die Erzeugung eines Permutationsvektors basiert auf N Pseudozufallszahlen, die durch den Pseudozufallszahlengenerator 30 erzeugt werden. Der Pseudozufallszahlengenerator 30 erzeugt für die Erzeugung jedes Permutationsvektors der Länge N nacheinander N Pseudozufallszahlen und gibt dieselben an den Sortierer 34 aus, wobei der Zähler 32 bei der Ausgabe jeder Pseudozufallszahl einen Zählerwert inkrementiert und an den Umordner 36 ausgibt, wobei der Zähler 32 mit einem Wert von 0 beginnt, um bei der ersten Pseudozufallszahl einen Wert von 1 auszugeben. Auf diese Weise werden die Pseudozufallszahlen, die von dem Pseudozufallszahlengenerator 30 ausgegeben werden, parallel zur Erzeugung nummeriert bzw. mit Indices in der Reihenfolge ihrer Generierung versehen. Die durch den Pseudozufallszahlengenerator 30 erzeugten Pseudozufallszahlen bilden zusammen einen Zufallszahlenvektor bzw. ein Zufallszahlenarray aus N Pseudozufallszahlen, während die durch den Zähler 32 erzeugten Zahlen ein Indexvektor bzw. ein Indexarray bilden, der bzw. das aus anstei-

genden Zahlen von 1 bis N besteht. Der Sortierer 34 empfängt den Zufallszahlenvektor und sortiert denselben mit einem geeigneten Sortierverfahren zum Beispiel in ansteigender Reihenfolge. Der Sortierer 34 ist mit dem Umordner 36 gekoppelt, um es zu ermöglichen, daß der Umordner 36 den von dem Zähler 32 empfangenen Indexvektor parallel zu der Sortierung des Zufallszahlenvektors umordnet. Das umgeordnete bzw. permutierte Indexarray, das von dem Umordner 36 erzeugt wird, stellt die Vertauschungsvorschrift für die N kodierten Datenblöcke dar, die von der Ausleseeinrichtung als nächstes gelesen werden, und wird durch den Umordner 36 als Permutationsvektor an die Ausleseeinrichtung 26 ausgegeben, die dasselbe, wie es im vorhergehenden beschrieben wurde, zur Definition der Auslesereihenfolge bezüglich des entsprechenden Zwischenspeichers 22 bzw. 24 verwendet.

Nachdem die Ausleseeinrichtung 26 die N kodierten Datenblöcke aus dem einen Zwischenspeicher 22 bzw. 24 gelesen hat, und gleichzeitig die Schreibeinrichtung den anderen Zwischenspeicher mit den nächsten N kodierten Datenblöcken von dem Kodierer 10 gefüllt hat, wechseln die Schreibeinrichtung 20 und die Ausleseeinrichtung 26 zu dem jeweils anderen Zwischenspeicher 22 bzw. 24, wobei der Auslesevorgang bezüglich der neuen in den Wechselpuffer geschriebenen kodierten Datenblöcken durchgeführt wird, die daraufhin in permutierter Reihenfolge an den Ausgangspuffer ausgegeben werden. Insgesamt ergibt sich am Ein- und Ausgang des Ausgangspuffers somit ein verschlüsseltes Signal aus kodierten Datenblöcken in permutierter Reihenfolge, das bei unauthorisierter Verarbeitung ohne Entschlüsselung und in dem Fall von Sprache eine Verständlichkeit der Sprachinformationen verhindert, wie es in Bezug auf Fig. 3 und 4 näher beschrieben werden wird.

Im folgenden wird bezugnehmend auf Fig. 2 eine Entschlüsselungsvorrichtung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung erläutert. Die Entschlüsselungsvorrichtung von Fig. 2 ist vorgesehen, um die in verschlüsselter Form ausgegebenen kodierten Datenblöcke der Verschlüsselungsvorrich-

tung von Fig. 1 wieder in ein Zeitsignal umzuwandeln, und zwar je nach der verwendeten Kodierung auf verlustbehaftete oder verlustlose Weise.

Die Vorrichtung von Fig. 2 umfaßt eine Einrichtung 38 zum Ändern der Reihenfolge der empfangenen kodierten Datenblöcke, die das verschlüsselte Signal darstellen, sowie einen Dekodierer 40, der mit der Einrichtung 38 verbunden ist und die Dekodierung der kodierten Datenblöcke vornimmt.

Die Einrichtung 38 weist eine zu der Einrichtung 12 der Verschlüsselungsvorrichtung von Fig. 1 ähnliche Anordnung auf, und besteht aus einer Schreibeinrichtung 42, einem Zwischenspeicher 1 44, einem Zwischenspeicher 2 46, einer Ausleseeinrichtung 48 und einer Einrichtung 50 zum Erzeugen eines inversen Permutationsvektors, die einen zu der Einrichtung 18 der Verschlüsselungsvorrichtung von Fig. 1 ähnlichen Aufbau aufweist und deshalb aus Übersichtlichkeitsgründen in Fig. 2 nicht detaillierter dargestellt ist. Die Schreibeinrichtung 42 empfängt an einem Eingang die kodierten Datenblöcke, die in der verschlüsselten Form vorliegen, und ist an zwei Ausgängen mit einem Eingang des Zwischenspeichers 44 bzw. des Zwischenspeichers 46 verbunden. Die Ausleseeinrichtung umfaßt drei Eingänge, von denen einer mit einem Ausgang der Einrichtung 50 zum Erzeugen eines inversen Permutationsvektors und die anderen beiden mit jeweils einem Ausgang des Zwischenspeichers 44 bzw. 46 verbunden sind. Ein Ausgang der Ausleseeinrichtung 48 ist mit dem Dekodierer 40 verbunden, um die dekodierten Datenblöcke in vorbestimmter Reihenfolge, d.h. in der für die Dekodierung nach dem jeweiligen Kodierverfahren vorgesehenen Reihenfolge, auszugeben.

Der Dekodierer 40 umfaßt eine Einrichtung 52 zum Dekodieren der kodierten Datenblöcke, die von der Ausleseeinrichtung 48 ausgegeben werden, sowie eine sich an die Einrichtung 52 anschließende Einrichtung 54 zum Bilden der aufeinanderfolgenden Abtastwerte, wobei die Einrichtung 54 das Zeitsignal bei-

spielsweise an einen Digital/Analog-Wandler (nicht gezeigt) oder dergleichen ausgibt.

Nachdem im vorhergehenden der Aufbau der Entschlüsselungsvorrichtung von Fig. 2 beschrieben worden ist, wird im folgenden die Funktionsweise derselben beschrieben.

Die Schreibeinrichtung 42 empfängt die kodierten Datenblöcke, die in verschlüsselter Form vorliegen, und gibt dieselben in der Reihenfolge, in der sie übertragen werden, an einen aktuellen der Zwischenspeicher 44 und 46 aus, die wie bei der Verschlüsselungsvorrichtung von Fig. 1 als Wechselpuffer zusammenwirken. Während die Schreibeinrichtung 42 einen der beiden Zwischenspeicher 44 und 46 nacheinander mit N kodierten Datenblöcken füllt, liest die Ausleseeinrichtung 48 den anderen Zwischenspeicher aus. Während das Befüllen eines Zwischenspeichers mit den kodierten Datenblöcken in der Übertragungsreihenfolge geschieht, wird das Auslesen des anderen Zwischenspeichers in permutierter Reihenfolge ausgeführt, die von dem inversen Permutationsvektor abhängt, der von der Einrichtung 50 erzeugt wird. Ein inverser Permutationsvektor bedeutet hierin, daß die durch den inversen Permutationsvektor erzeugte Vertauschungsvorschrift die Vertauschungen, die durch die Entschlüsselungsvorrichtung von Fig. 1 an einer jeweiligen Vertauschungs- bzw. Permutationsgruppe von N kodierten Datenblökken vorgenommen worden sind, wieder rückgängig macht.

Die Einrichtung 50 erzeugt die inversen Permutationsvektoren pro Auslesevorgang beispielsweise mittels einer gleichen Anordnung von Einrichtungen, wie sie für die Einrichtung 18 in Fig. 1 dargestellt ist, wobei die Einrichtung 50 jedoch aus dem Permutationsvektor, wie er durch die Einrichtung 18 erzeugt wird, durch eine geeignete Einrichtung einen inversen Permutationsvektor erzeugt, indem beispielsweise die durch den Permutationsvektor festgelegte Vertauschungsvorschrift auf einen Vektor angewendet wird, wie er von dem Zähler (siehe 32 in Fig. 1) ausgegeben wird, d.h. einen Vektor aus geordneten Zahlen von 1 bis N.

Die von der Ausleseeinrichtung 48 in permutierter Reihenfolge ausgelesenen N kodierten Datenblöcke werden der Einrichtung 52 zum Dekodieren der kodierten Datenblöcke zugeführt, wobei dieselben nun in der vorbestimmten Reihenfolge vorliegen, die zur Dekodierung der kodierten Datenblöcke gemäß dem dem Dekodierer 44 zugrundeliegenden Kodierverfahren notwendig ist, um ein korrektes Zeitsignal zu erhalten.

Nachdem die Ausleseeinrichtung 48 den jeweiligen Zwischenspeicher ausgelesen hat bzw. die Schreibeinrichtung 42 den anderen Zwischenspeicher vollständig gefüllt hat, liest die Ausleseeinrichtung den gerade von der Schreibeinrichtung 42 befüllten Zwischenspeicher aus, während die Schreibeinrichtung 42 den Zwischenspeicher beschreibt, der von der Ausleseeinrichtung 48 ausgelesen worden ist.

Die Einrichtung 52 dekodiert die kodierten Datenblöcke und gibt Zeitblöcke mit vorbestimmter Reihenfolge aus. Die Einrichtung 54 empfängt die Zeitblöcke und bildet aus denselben die aufeinanderfolgenden Abtastwerte, aus denen das Zeitsignal besteht, und gibt dieselben beispielsweise an einen Analog/Digital-Wandler (nicht gezeigt) aus.

Nachdem im vorhergehenden Ausführungsbeispiele für eine Verschlüsselungs- bzw. Entschlüsselungsvorrichtung beschrieben worden sind, wird im folgenden bezugnehmend auf die Fig. 3 und 4 ein explizites Ausführungsbeispiel beschrieben, bei dem ein diskretes Signal durch die Vorrichtung von Fig.1 in ein verschlüsseltes Signal verschlüsselt und letztgenanntes durch die Vorrichtung von Fig. 2 entschlüsselt wird, wobei zusätzlich auf Fig. 1 und 2 Bezug genommen wird.

In den Fig. 3 und 4 sind mit Rechtecken Abtastwerte des Zeit- bzw. Audiosignals, Zeitblöcke bzw. Datenblöcke dargestellt, wie es in der Beschreibung angegeben ist. Um die Datenblöcke voneinander unterscheiden zu können, sind die Datenblöcke jeweils mit einem großen Buchstaben A - O markiert.

Fig. 3 stellt schematisch einen Verschlüsselungsvorgang gemäß der vorliegenden Erfindung dar. Bei 60 ist eine Aufeinanderfolge von Abtastwerten 62 gezeigt, die das Zeitsignal bzw. das diskrete Signal bilden, wie es der Verschlüsselungsvorrichtung von Fig. 1 zugeführt wird.

Bei 64 ist eine Aufeinanderfolge von Zeitblöcken 66 gezeigt, wie sie von der Einrichtung 14 von Fig. 1 erzeugt wird. Wie es bereits erwähnt worden ist, kann sich jeder Abtastwert in einem oder mehreren der Zeitblöcke 66 befinden, bzw. die Zeitblöcke können sich gegenseitig überschneiden, um Aliasingartefakte auszumerzen.

Bei 68 ist eine Aufeinanderfolge von kodierten Datenblöcken A - N gezeigt, die in der vorbestimmten Reihenfolge vorliegen, wie sie von der Einrichtung 16 von Fig. 1 ausgegeben werden. Wie es zu sehen ist, kann jeder kodierte Datenblock 70 eine individuell unterschiedliche Länge bzw. Größe aufweisen, wie es durch die unterschiedlichen Größen der Blöcke veranschaulicht ist.

Bei 72 ist ein Zustand dargestellt, wie er sich für die aufeinanderfolgenden kodierten Datenblöcke 70 während der Verschlüsselung bei der Verschlüsselungsvorrichtung von Fig. 1 ergibt. Bei dem Zustand 72, wie auch bei den folgenden Zuständen der Fig. 3, sind insbesondere die Inhalte des Zwischenspeichers 1 (22 in Fig. 1), des Zwischenspeichers 2 (24 in Fig. 1) und des Ausgangspuffers (28 in Fig. 1) für den jeweiligen Zustand dargestellt. Bei 72 ist der Zustand für den exemplarischen Fall dargestellt, daß die Vertauschungsgruppengröße bei der Verschlüsselung bzw. Entschlüsselung auf 5 eingestellt ist. Der bei 72 dargestellte Zustand entspricht dem Zustand, wie er sich bei der Vorrichtung von Fig. 1 einstellt, nachdem von den Datenblöcken 70 bei 68 die ersten fünf A - E in den aktiven bzw. aktuellen Zwischenspeicher, in diesem Fall den Zwischenspeicher 1, geschrieben worden sind. Die Werte in dem Zwischenspeicher 2 und dem Ausgangspuffer, die beispiels-

weise dieselbe Länge bzw. Größe wie der Zwischenspeicher 1 aufweisen können, hängen von vorhergehenden kodierten Datenblöcken ab, und sind deshalb mit Bindestrichen dargestellt. Wie es zu sehen ist, sind die kodierten Datenblöcke A - E in ihrer vorbestimmten Reihenfolge in den Zwischenspeicher 1 abgelegt worden.

Bei 74 ist der Zustand dargestellt, wie er sich nach fünf weiteren kodierten Datenblöcken ergibt. Die 5 weiteren kodierten Datenblöcke F - J sind in den Zwischenspeicher 2 geschrieben worden, während die in den Zwischenspeicher 1 abgelegten kodierten Datenblöcke in den Ausgangspuffer ausgelesen worden sind. Zum Auslesen der in den Zwischenspeicher 1 abgelegten kodierten Datenblöcke ist der Permutationsvektor verwendet worden, wie er bei 76 angezeigt ist, d.h. (4,3,5,2,1). Anders ausgedrückt, ordnet der Permutationsvektor 76 jeden kodierten Datenblock in dem Zwischenspeicher 1 eine Zahl zwischen 1 bis 5 bzw. N zu, die die Auslesereihenfolge bzw. die Position angibt, an der dieser kodierte Datenblock in den Ausgangspuffer geschrieben werden soll, so daß in dem Ausgangspuffer die kodierten Datenblöcke A-E in der Reihenfolge EDBAC vorliegen.

Bei 78 ist der Zustand nach weiteren 5 kodierten Datenblöcken dargestellt. Wie es zu sehen ist, sind die 5 nachfolgenden kodierten Datenblöcke K - O wiederum in den Zwischenspeicher 1 geschrieben worden, während in der Zwischenzeit der Zwischenspeicher 2 mittels eines Permutationsvektors 80 (5,1,3,2,4) in den Ausgangspuffer ausgelesen worden ist, wo sich die kodierten Datenblöcke in der Reihenfolge GIHJF ergeben.

Bei 82 ist der Strom bzw. die Aufeinanderfolge von kodierten Datenblöcken in verschlüsselter Form dargestellt, wie sie in den Ausgangspuffer 28 eingegeben bzw. von demselben ausgegeben werden. Wie es zu sehen ist, sind die kodierten Datenblöcke gegenüber der vorbestimmten Reihenfolge, in der dieselben durch die dem Kodierer 10 zugrundeliegende Kodierung üblicherweise ausgegeben werden, verwürfelt bzw. gescrambelt, weshalb in dem Fall, daß die Audiodaten Träger von Sprachinformationen

sind, diese Sprachinformationen bei Dekodierung ohne Entschlüsselung gemäß der vorliegenden Erfindung unverständlich sind. Dennoch wird bei Dekodierung ohne Entschlüsselung verhindert, daß der Dekodierer in ungültige Zustände gerät, da die zeitliche Diskontinuität in Einheiten von kodierten Datenblöcken definiert ist.

Ist die dem psychoakustischen Dekodierer zugrunde liegende Kodierung beispielsweise eine nach dem AAC-Standard, tritt, falls das verschlüsselte Signal von einem standardkonformen Dekoder bzw. Dekodierer dekodiert wird, kein Knacksen an den Blockgrenzen auf, sondern vielmehr äußert sich die zeitliche Diskontinuität aufgrund der vertauschten Rahmen bzw. Datenblöcke im Auftreten von Aliasinganteilen, da die Datenblöcke vermittels der inversen modifizierten diskreten Cosinustransformation (IMDCT = inverse modified discrete cosine transform) in den Zeitbereich rücktransformiert werden und an den Überlappungsbereichen der Transformationsfenster keine Aliasing-Auslöschung mehr stattfindet.

Wird das Signal 82 von einem Decoder bzw. einer Entschlüsselungsvorrichtung gemäß Fig. 2, d.h. mit einer entsprechenden inversen Vertauschung der Eingangsdaten, entschlüsselt, dann liegen in dem Zwischenspeicher wieder die Datenblöcke bzw. die Datenrahmen in der richtigen Reihenfolge vor und die anschließende Dekodierung kann standardkonform erfolgen. Dieser Entschlüsselungsvorgang wird bezugnehmend auf Fig. 4 für das explizite Ausführungsbeispiel von Fig. 3 näher erläutert.

Fig. 4 zeigt bei 84 ein Beispiel für eine Folge von kodierten Datenblöcken in verschlüsselter Form, die in diesem Fall derjenigen von Fig. 3 bei 82 entspricht. Bei 86 ist ein Zustand dargestellt, wie er sich bei der Entschlüsselungsvorrichtung von Fig. 2 ergibt, nachdem dieselbe die ersten fünf der kodierten Datenblöcke von 84 empfangen hat. Insbesondere ist bei dem Zustand 84 sowie bei den folgenden Zuständen in Fig. 4 der Inhalt des Zwischenspeichers 1 (44 in Fig. 2), der Inhalt des Zwischenspeichers 2 (46 in Fig. 2) und die Folge von kodierten

Datenblöcken, die von der Einrichtung 38 an den Kodierer 40 ausgegeben wird, gezeigt. Wie es bei 86 zu sehen ist, werden die dekodierten Datenblöcke in den aktuellen Zwischenspeicher, in diesem Fall den Zwischenspeicher 1, in der Reihenfolge abgelegt, in der dieselben übertragen werden.

Bei 88 ist der Zustand dargestellt, wie er sich nach fünf weiteren kodierten Datenblöcken FGHIJ einstellt. Wie es zu sehen ist, sind die nächsten fünf kodierten Datenblöcke in den Zwischenspeicher 2 geschrieben worden, während mittels eines inversen Permutationsvektors 90 die kodierten Datenblöcke EDBAC aus dem Zwischenspeicher 1 ausgelesen werden, um zu dem Dekodierer 40 in der Reihenfolge ABCDE übertragen zu werden, wobei sich der inverse Permutationsvektor aus dem Permutationsvektor 76 von Fig. 3, der sich auf dieselbe Permutationsgruppe bezog, durch Anwenden des letztgenannten als Vertauschungsvorschrift auf einen Vektor (1,2,3,4,5) ergibt.

Bei 92 ist der Zustand dargestellt, wie er sich nach dem Auslesen weiterer fünf kodierter Datenblöcke aus dem Strom von kodierten Datenblöcken 84 ergibt. Wie es zu sehen ist, ist wieder der Zwischenspeicher 1 mit den nachfolgenden kodierten Datenblöcken K - O befüllt worden, während zu dem Dekodierer die kodierten Datenblöcke GHIJF in dem Zwischenspeicher 2 ausgelesen und in permutierter Reihenfolge bzw. invers permutierter Reihenfolge FGHIJ ausgegeben worden sind. Der Rückpermutation liegt der inverse Permutationsvektor 94 zugrunde, der sich aus dem Permutationsvektor 80 von Fig. 3 durch Anwenden des letztgenannten auf einen Vektor (1,2,3,4,5) ergibt.

Bei 96 ist schließlich der Strom von aufeinanderfolgenden kodierten Datenblöcken gezeigt, wie er dem Dekodierer zugeführt wird. Wie es zu sehen ist, ist die Reihenfolge wieder hergestellt, in der die kodierten Datenblöcke von dem Kodierer der Verschlüsselungsvorrichtung ausgegeben worden sind, d.h. ABCDEFGHIJKLMN..., so daß die Dekodierung standardkonform erfolgen kann.

Die im vorhergehenden bezugnehmend auf die Fig. 1 bis 4 gelieferte Beschreibung bezog sich auf eine Verschlüsselung, die auf der Vertauschung von Datenblöcken des Zeitsignals innerhalb einer Blockgruppe bzw. Vertauschungsgruppe basiert. Die Blockvertauschung im Zeitbereich zerstört die zeitliche Modulation eines Sprachsignals derart, daß in dem Fall eines Sprachsignals die Verständlichkeit erheblich reduziert wird. Ein Vorteil der obigen Ausführungsbeispiele besteht darin, daß, obwohl bei den vorhergehenden Ausführungsbeispielen zur Kodierung des Zeitsignals ein psychoakustisches Kompressionsverfahren verwendet wird, die diesem psychoakustischen Kompressionsverfahren zugrundeliegenden Annahmen, wie z.B. über die zeitliche und spektrale Verdeckung, weiterhin gültig bleiben, da die zeitliche Diskontinuität erst nach der Komprimierung erzeugt wird, d.h. die zeitliche Reihenfolge der bereits kodierten Datenrahmen vertauscht wird. Die im vorhergehenden beschriebenen Ausführungsbeispiele sind grundsätzlich für alle kodierten Datenströme anwendbar, die auf einer sequentiellen Folge in sich abgeschlossener und nach Kodierung sich überlappender Datenrahmen basieren.

In Bezug auf die im vorhergehenden beschriebenen Ausführungsbeispiele wird insbesondere darauf hingewiesen, daß die Sprachunverständlichkeit des verschlüsselten Signals dadurch verbessert werden kann, daß der psychoakustische Kodierer 10 bzw. eine Einrichtung zwischen demselben und der Einrichtung zur Änderung der Reihenfolge eine Frequenzbereichsverwürfelung gemäß der in der Beschreibungseinleitung erwähnten Patentanmeldung WO99/51279 durchführt.

Nachdem im vorhergehenden die vorliegende Erfindung anhand spezieller Ausführungsbeispiele beschrieben worden ist, wird darauf hingewiesen, daß die vorliegende Erfindung sowohl in Hardware, wie z.B. als eine ASIC, eine integrierte Schaltung oder dergleichen, als auch in Software, wie z.B. als eine auf einem PC lauffähige Software, implementierbar ist. Ferner wird darauf hingewiesen, daß, obwohl im vorhergehenden die vorliegende Erfindung in Bezug auf die Verschlüsselung von Audioda-

ten bzw. Sprachsignalen beschrieben worden ist, die vorliegende Erfindung allgemein auf alle Gebiete anwendbar ist, bei denen diskrete Signale verwendet werden und gegebenenfalls eine Kodierung derselben stattfindet, wie z.B. bei der Bild- und Videoverarbeitung oder der Datenübertragung im allgemeinen. Dementsprechend ist die der Erzeugung der zeitlichen Diskontinuität bei der Verschlüsselung vorangehende Kodierung nicht auf eine psychoakustische Kodierung begrenzt. Beispielsweise ist auch eine JPEG-Kodierung bei Bild- oder Videodaten möglich. Allgemein ist die vorliegende Erfindung mit allen Kodierverfahren implementierbar, die aufeinanderfolgende diskrete Abtastwerte in Zeitblöcke unterteilen und diese in kodierte Datenblöcke bzw. -rahmen kodieren oder direkt bereits existierende Zeitblöcke kodieren.

Ferner wird darauf hingewiesen, daß die genaue Implementierung der Einrichtung zur Erzeugung eines Permutationsvektors eine Einrichtung zur Erzeugung der Reihenfolge der kodierten Datenblöcke auch anders implementiert sein kann, wie z.B. insbesondere im Hinblick auf die Länge der Vertauschungsgruppe N oder der Anzahl und Größe der verwendeten Zwischenspeicher.

Ferner kann die Einrichtung zur Erzeugung eines Permutationsvektors anders implementiert sein als im vorhergehenden beschrieben. Der Permutationsvektor könnte beispielsweise für alle Vertauschungsgruppen gleich sein, in welchem Fall der inverse Permutationsvektor ebenfalls fest wäre. Allgemein wird darauf hingewiesen, daß von dem in dem vorhergehenden Ausführungsbeispielen verwendeten Prinzip der Permutierung aufeinanderfolgender Vertauschungsgruppen abgewichen werden kann, und daß die Änderung der Reihenfolge auch auf andere Weisen durchgeführt werden kann, wie z.B. durch eine Änderung der Reihenfolge bezüglich der gesamten kodierten Datenblöcke, in welchem Fall eine Zwischenspeicherung aller kodierten Datenblöcke vor der Änderung der Reihenfolge bei der Verschlüsselung sowie eine Speicherung der gesamten kodierten Datenblöcke vor der Änderung der Reihenfolge bei der Entschlüsselung erforderlich wäre.

Patentansprüche

1. Verfahren zum Verschlüsseln eines diskreten Signals, das aus aufeinanderfolgenden Abtastwerten (62) besteht, mit folgenden Schritten:

Einteilen der aufeinanderfolgenden Abtastwerte (62) in aufeinanderfolgende Zeitblöcke (66);

Kodieren der aufeinanderfolgenden Zeitblöcke (66) in kodierte Datenblöcke (70) mit einer vorbestimmten Reihenfolge; und

Ändern der vorbestimmten Reihenfolge der kodierten Datenblöcke (70) gemäß einer vorbestimmten Vertauschungsvorschrift (76, 80).

2. Vorrichtung zum Verschlüsseln eines diskreten Signals, das aus aufeinanderfolgenden Abtastwerten (62) besteht, mit

einer Einrichtung (14) zum Einteilen der aufeinanderfolgenden Abtastwerte (62) in aufeinanderfolgende Zeitblöcke (66);

einer Einrichtung (16) zum Kodieren der aufeinanderfolgenden Zeitblöcke (66) in kodierte Datenblöcke (70) mit einer vorbestimmten Reihenfolge; und

einer Einrichtung (12) zum Ändern der vorbestimmten Reihenfolge der kodierten Datenblöcke (70) gemäß einer vorbestimmten Vertauschungsvorschrift (76, 80).

3. Vorrichtung gemäß Anspruch 2, bei der das diskrete Signal ein Audiosignal ist, und die Einrichtung (16) zum Kodieren angepaßt ist, um eine psychoakustische Kodierung durchzuführen.

4. Vorrichtung gemäß Anspruch 2 oder 3, bei der die Einrichtung (12) zum Ändern der vorbestimmten Reihenfolge der kodierten Datenblöcke (70) gemäß einer vorbestimmten Vertauschungsvorschrift (76, 80) ferner folgendes Merkmal aufweist:

eine Einrichtung (12) zum Permutieren einer vorbestimmten Anzahl von aufeinanderfolgenden dekodierten Datenblöcke (70) gemäß der vorbestimmten Vertauschungsvorschrift (76, 80).

5. Vorrichtung gemäß Anspruch 4, bei der die vorbestimmte Vertauschungsvorschrift ein Permutationsvektor (76, 80) der Länge N ist, wobei N der vorbestimmten Anzahl von aufeinanderfolgenden der kodierten Datenblöcke (70) entspricht, wobei die Vorrichtung ferner folgendes Merkmal aufweist:

eine Einrichtung (18) zum Erzeugen des Permutationsvektors mit

einer Einrichtung (30) zum aufeinanderfolgenden Erzeugen von N Pseudozufallszahlen;

einer Einrichtung (32) zum Zuordnen jeder der N Pseudozufallszahlen eine Zahl zwischen 1 und N gemäß der Reihenfolge der Erzeugung der N Pseudozufallszahlen;

einer Einrichtung (34) zum Sortieren der N Pseudozufallszahlen; und

einer Einrichtung (36) zum Umordnen der N zugeordneten Zahlen parallel zu der Sortierung der N Pseudozufallszahlen, um den Permutationsvektor (76, 80) zu erhalten.

6. Vorrichtung gemäß Anspruch 4 oder 5, bei der die Einrichtung (12) zum Permutieren angepaßt ist, um mehrere aufeinanderfolgende Gruppen von aufeinanderfolgenden kodierten Datenblöcken (70) zu permutieren, und die ferner folgende Merkmale aufweist:

einen Ausgangspuffer (28);

einen ersten und einen zweiten Zwischenspeicher (22, 24);

eine Einrichtung (20) zum abwechselnden Speichern der aufeinanderfolgenden Gruppen von aufeinanderfolgenden kodierten Datenblöcken (70) in einen des ersten beziehungsweise zweiten Zwischenspeichers (22, 24); und

eine Einrichtung (26) zum Auslesen des Speicherinhalts des anderen des ersten beziehungsweise zweiten Zwischenspeichers (22, 24), in dem die abwechselnde Speicherung nicht erfolgt, während der abwechselnden Speicherung in den einen des ersten beziehungsweise zweiten Zwischenspeichers (22, 24) und Ausgeben des Speicherinhalts an den Ausgangspuffer (28) gemäß einer der Vertauschungsvorschrift entsprechenden Reihenfolge.

7. Vorrichtung gemäß Anspruch 6, bei der die Vertauschungsvorschrift für zumindest zwei der Gruppen einen unterschiedlichen Permutationsvektor aufweist.

8. Verfahren zum Entschlüsseln eines verschlüsselten Signals, das eine Mehrzahl von kodierten Datenblöcken in einer Reihenfolge aufweist und einem diskreten Signal, das aus aufeinanderfolgenden Abtastwerten besteht, in verschlüsselter Form entspricht, mit folgenden Schritten:

Ändern der Reihenfolge der kodierten Datenblöcke gemäß einer vorbestimmten Vertauschungsvorschrift (90, 94);

Dekodieren der kodierten Datenblöcke in der geänderten Reihenfolge in aufeinanderfolgende Zeitblöcke mit vorbestimmter Reihenfolge; und

Bilden der aufeinanderfolgenden Abtastwerte aus den aufeinanderfolgenden Zeitblöcken.

9. Vorrichtung zum Entschlüsseln eines verschlüsselten Signals, das eine Mehrzahl von kodierten Datenblöcken in einer Reihenfolge aufweist und einem diskreten Signal, das aus aufeinanderfolgenden Abtastwerten besteht, in verschlüsselter Form entspricht, mit

einer Einrichtung (38) zum Ändern der Reihenfolge der kodierten Datenblöcke gemäß einer vorbestimmten Vertauschungsvorschrift (90, 94);

einer Einrichtung (52) zum Dekodieren der kodierten Datenblöcke in der geänderten Reihenfolge in aufeinanderfolgende Zeitblöcke mit vorbestimmter Reihenfolge; und

einer Einrichtung (54) zum Bilden der aufeinanderfolgenden Abtastwerte aus den aufeinanderfolgenden Zeitblöcken.

10. Vorrichtung gemäß Anspruch 9, bei der das diskrete Signal ein Audiosignal ist, und die Einrichtung (52) zum Dekodieren angepaßt ist, um eine inverse modifizierte diskrete Cosinustransformation durchzuführen.

11. Vorrichtung gemäß Anspruch 9 oder 10, bei der die Einrichtung (38) zum Ändern der Reihenfolge der kodierten Datenblöcke gemäß einer vorbestimmten Vertauschungsvorschrift ferner folgendes Merkmal aufweist:

eine Einrichtung (38) zum Permutieren einer ersten vorbestimmten Anzahl von aufeinanderfolgenden kodierten Datenblöcken gemäß der vorbestimmten Vertauschungsvorschrift.

12. Vorrichtung gemäß Anspruch 11, bei der die vorbestimmte Vertauschungsvorschrift ein Permutationsvektor (76, 80) der Länge N ist, wobei N der vorbestimmten Anzahl von aufeinanderfolgenden der kodierten Datenblöcke (70) entspricht, wobei die Vorrichtung ferner folgendes Merkmal aufweist:

eine Einrichtung (50) zum Erzeugen des Permutationsvektors mit

einer Einrichtung zum aufeinanderfolgenden Erzeugen von N Pseudozufallszahlen;

einer Einrichtung zum Zuordnen jeder der N Pseudozufallszahlen eine Zahl zwischen 1 und N gemäß der Reihenfolge der Erzeugung der N Pseudozufallszahlen;

einer Einrichtung zum Sortieren der N Pseudozufallszahlen;

einer Einrichtung zum Umordnen der N zugeordneten Zahlen parallel zu der Sortierung der N Pseudozufallszahlen, um einen permutierten Vektor zu erhalten; und

einer Einrichtung zum Anwenden des permutierten Vektors als eine Permutationsvorschrift auf einen geordneten Vektor von Zahlen von 1 bis N, um den Permutationsvektor zu erhalten.

13. Vorrichtung gemäß Anspruch 11 oder 12, bei der die Einrichtung (38) zum Permutieren angepaßt ist, um mehrere aufeinanderfolgende Gruppen von aufeinanderfolgenden von kodierten Datenblöcken (70) zu permutieren, und die ferner folgende Merkmale aufweist:

einen ersten und einen zweiten Zwischenspeicher (44, 46);

eine Einrichtung (42) zum abwechselnden Speichern der Gruppen von aufeinanderfolgenden kodierten Datenblöcken (70) in einen des ersten und zweiten Zwischenspeichers (44, 46); und

eine Einrichtung (48) zum Auslesen des Speicherinhalts des anderen des ersten und zweiten Zwischenspeichers (44, 46), in dem die abwechselnde Speicherung nicht erfolgt, während der abwechselnden Speicherung in den anderen in des ersten und zweiten Zwischenspeichers (44, 46) und Ausgeben des Speicherinhalts an die Einrichtung (52) zum Dekodieren gemäß einer der Vertauschungsvorschrift entsprechenden Reihenfolge.

14. Vorrichtung gemäß Anspruch 13, bei der die Vertauschungsvorschrift für zumindest zwei der Gruppen einen unterschiedlichen Permutationsvektor aufweist.

15. Vorrichtung gemäß Anspruch 9 oder 13, bei dem das Audiosignal Sprachinformationen enthält.

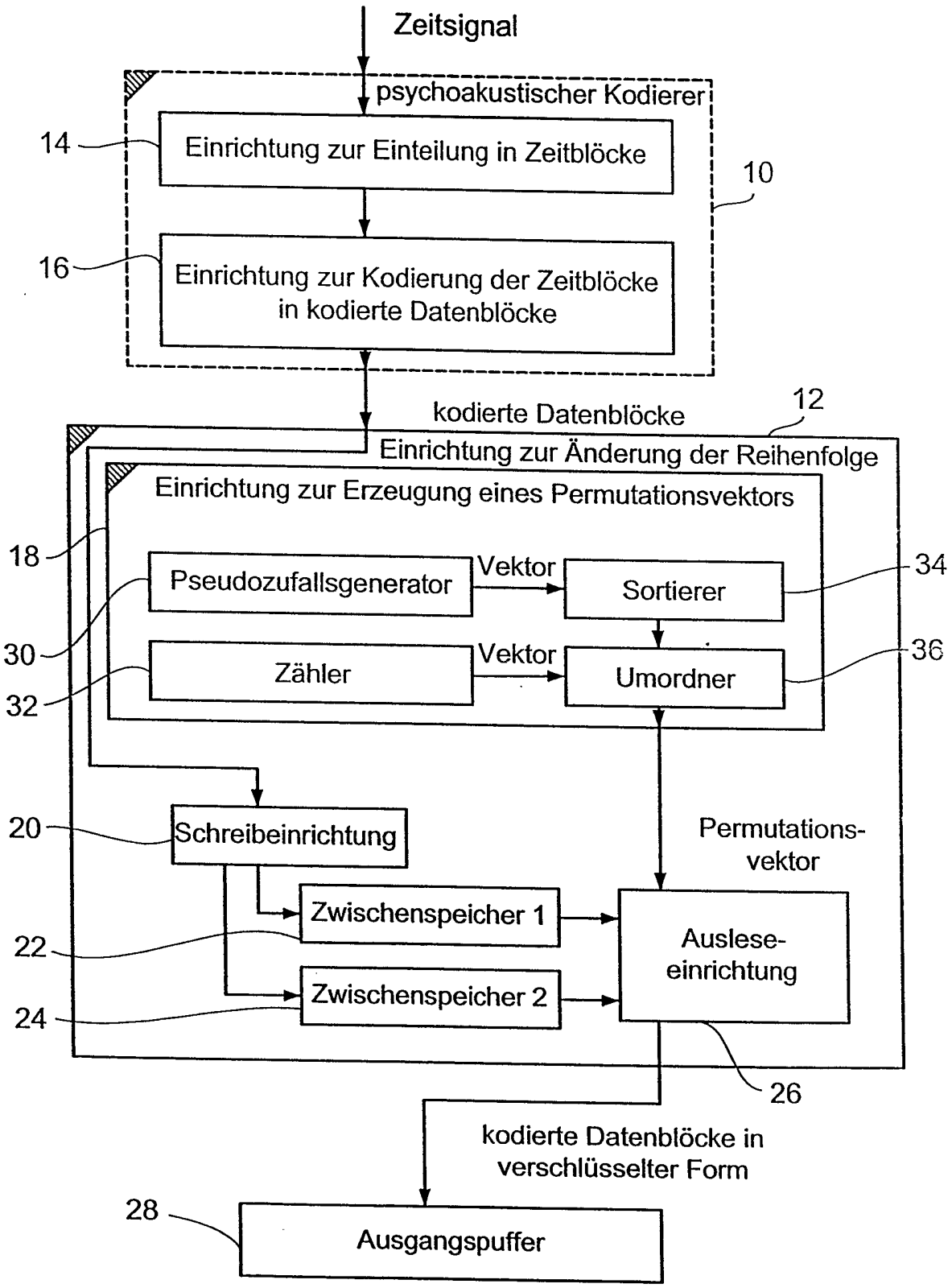

Zeitsignal
psychoakustischer Kodierer
14
Einrichtung zur Einteilung in Zeitblöcke
10
16
Einrichtung zur Kodierung der Zeitblöcke in kodierte Datenblöcke
kodierte Datenblöcke
12
Einrichtung zur Änderung der Reihenfolge
Einrichtung zur Erzeugung eines Permutationsvektors
18
Pseudozufallsgenerator
Vektor
Sortierer
34
30
Zähler
Vektor
Umordner
36
32
20
Schreibeinrichtung
Permutations-vektor
Zwischenspeicher 1
22
Auslese-einrichtung
Zwischenspeicher 2
24
26
kodierte Datenblöcke in verschlüsselter Form
28
Ausgangspuffer

FIG. 1

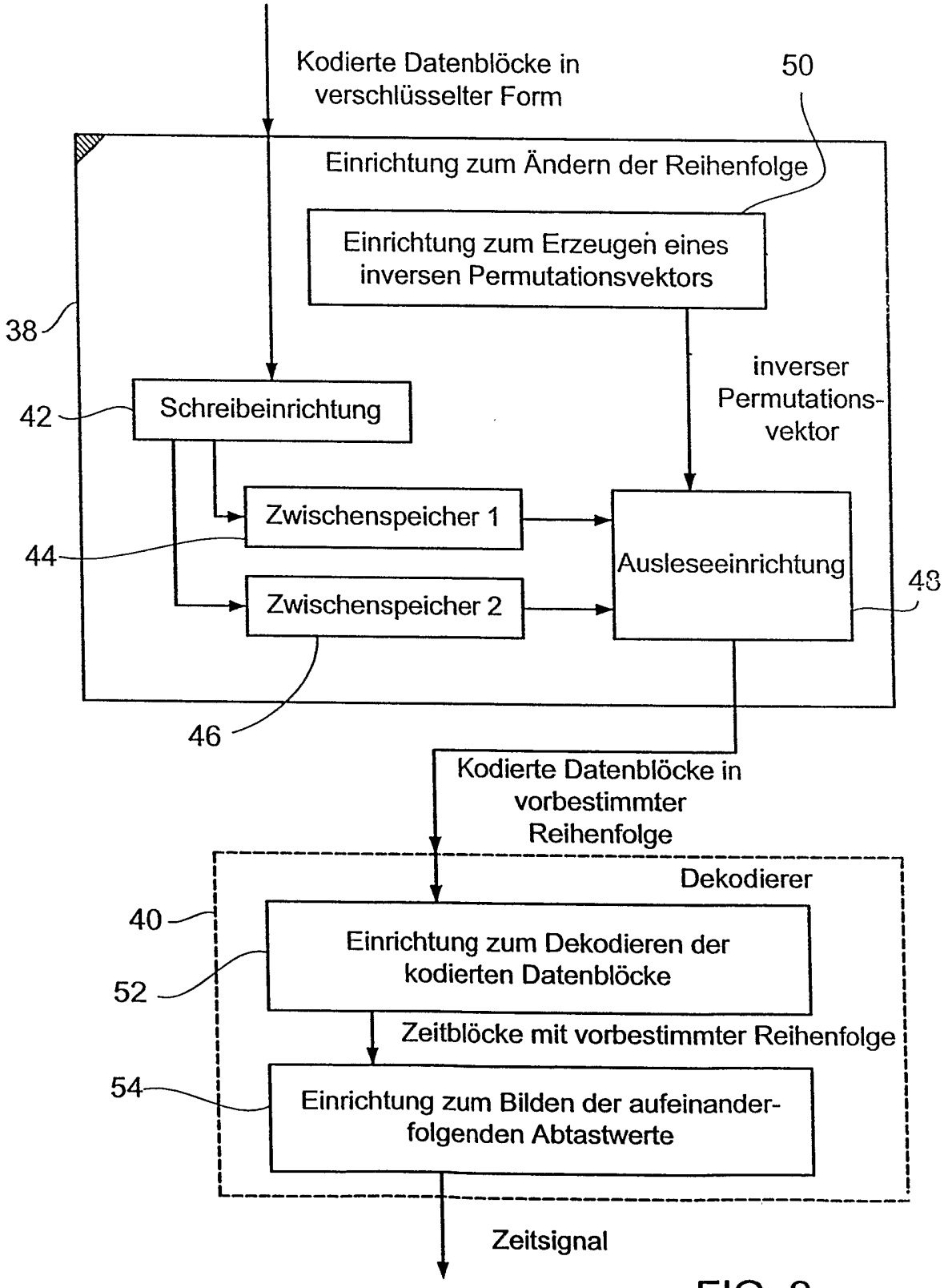

Kodierte Datenblöcke in verschlüsselter Form
50
Einrichtung zum Ändern der Reihenfolge
Einrichtung zum Erzeugen eines inversen Permutationsvektors
38
inverser Permutations-vektor
42
Schreibeinrichtung
Zwischenspeicher 1
44
Ausleseeinrichtung
48
Zwischenspeicher 2
46
Kodierte Datenblöcke in vorbestimmter Reihenfolge
Dekodierer
40
Einrichtung zum Dekodieren der kodierten Datenblöcke
52
Zeitblöcke mit vorbestimmter Reihenfolge
54
Einrichtung zum Bilden der aufeinander-folgenden Abtastwerte
Zeitsignal

FIG. 2

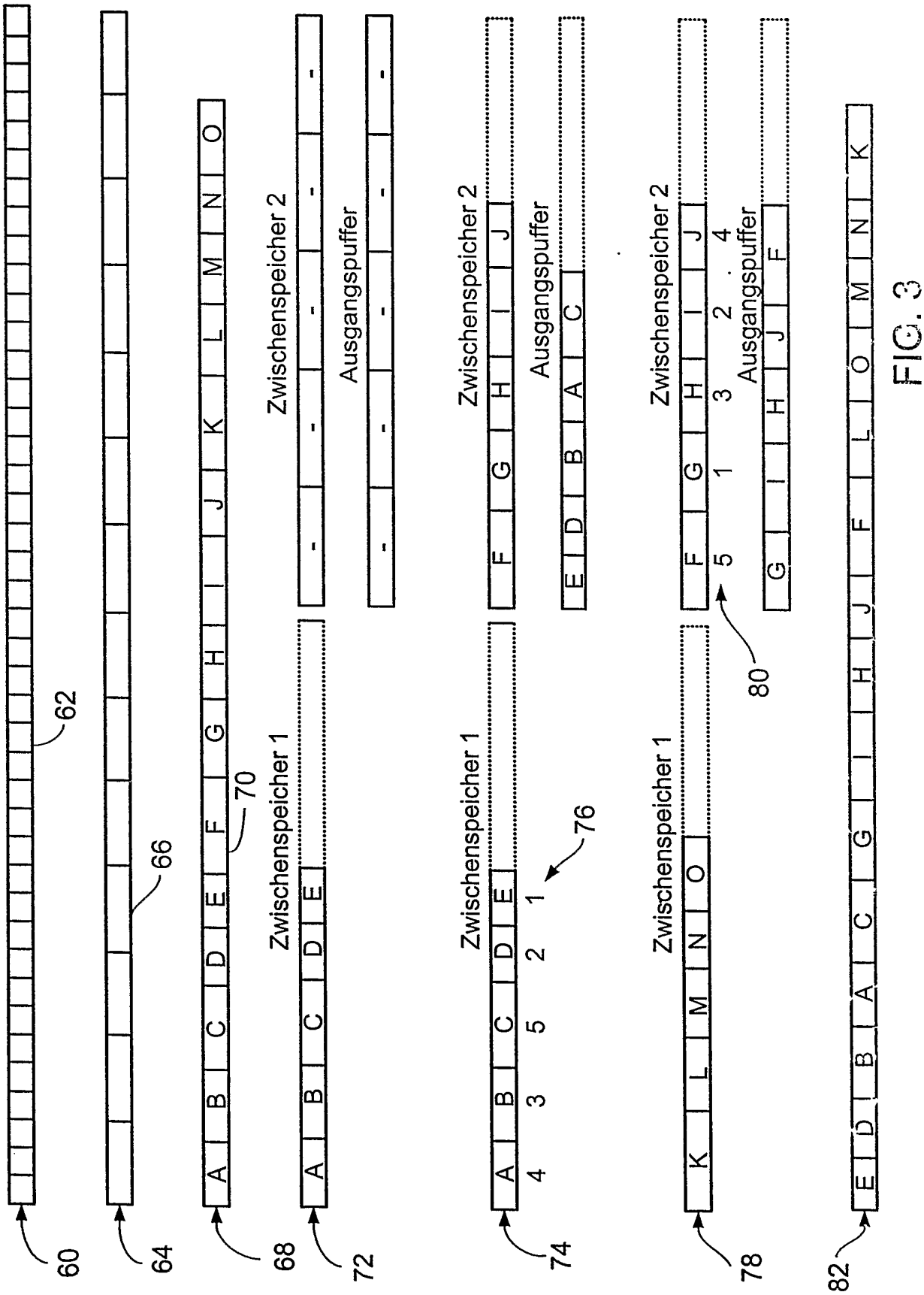

60
62
64
66
68
70
72
74
76
78
80
82
Zwischenspeicher 1
Zwischenspeicher 2
Ausgangspuffer
A B C D E F G H I J K L M N O
A B C D E
- - - - -
F G H I J
E D B A C
K L M N O
G I H J F
E D B A C G I H J F L O M N K
4 3 5 2 1
5 1 3 2 4

FIG. 3

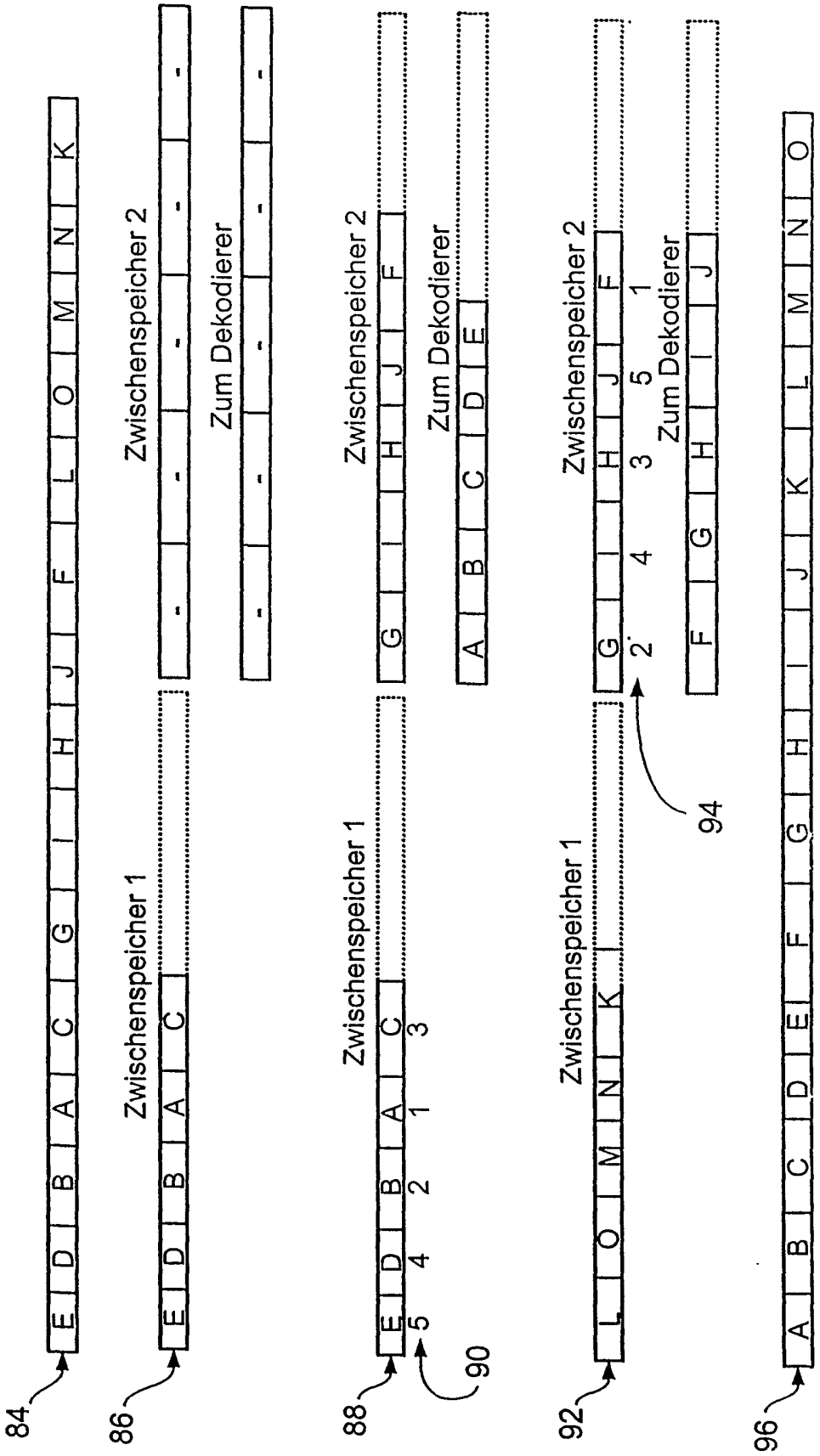

84
E D B A C G I H J F L O M N K
86
Zwischenspeicher 1
E D B A C
Zwischenspeicher 2
- - - - - - - -
Zum Dekodierer
- - - - - - - -
88
Zwischenspeicher 1
E D B A C
4 2 1 3
5
90
Zwischenspeicher 2
G I H J F
Zum Dekodierer
A B C D E
92
Zwischenspeicher 1
L O M N K
Zwischenspeicher 2
G I H J F
2 4 3 5 1
94
Zum Dekodierer
F G H I J
96
A B C D E F G H I J K L M N O

FIG. 4