(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 042 587**
A1

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **81104666.3**

(51) Int. Cl.³: **H 04 K 1/06**

(22) Anmeldetag: **17.06.81**

(30) Priorität: **20.06.80 CH 4763/80**

(43) Veröffentlichungstag der Anmeldung:
30.12.81 Patentblatt 81/52

(84) Benannte Vertragsstaaten:
AT BE CH DE FR GB IT LI NL SE

(71) Anmelder: **Crypto Aktiengesellschaft**
Zugerstrasse 42
CH-6312 Steinhausen(CH)

(72) Erfinder: **Mengia, Caflisch, Dr.**
Zugerstrasse 18
CH-8915 Hausen a.A.(CH)

(72) Erfinder: **Weber, Richard, Dr.**
Eichholzstrasse 9
CH-6312 Steinhausen(CH)

(74) Vertreter: **Blum, Rudolf E. et al,**
c/o E. Blum & Co Patentanwälte Vorderberg 11
CH-8044 Zürich(CH)

(54) Verfahren zur Umformung von für die verschlüsselte Übertragung in Signalabschnitte unterteilten Sprachsignalen sowie Vorrichtung zur Ausführung des Verfahrens.

(57) Bei analoger Sprachverschlüsselung ergibt sich infolge der Umschaltung zwischen zwei aufeinanderfolgenden Signalabschnitten eine Zunahme der Bandbreite. Die Bandbegrenzung durch den Uebertragungskanal verursacht im entschlüsselten Signal nicht-lineare Verzerrungen. Durch eine zeitliche Stauchung um einen Faktor s kann im Gebiet der Stossstelle zweier benachbarter Signalabschnitte (T) ein Zeitabschnitt (Tu) verfügbar gemacht werden, in welchem Teile des Signals zweimal übertragen werden. Der redundante Anteil in diesem Zeitabschnitt (Tu) wird mit einer Gewichtungsfunktion versehen, so dass eine weiche Umschaltung ohne Unstetigkeiten im Signalverlauf entsteht. Im Empfänger wird der redundante Anteil ausgetastet, und die übrigen Abschnitte werden auf die ursprüngliche zeitliche Länge (T) gedehnt.

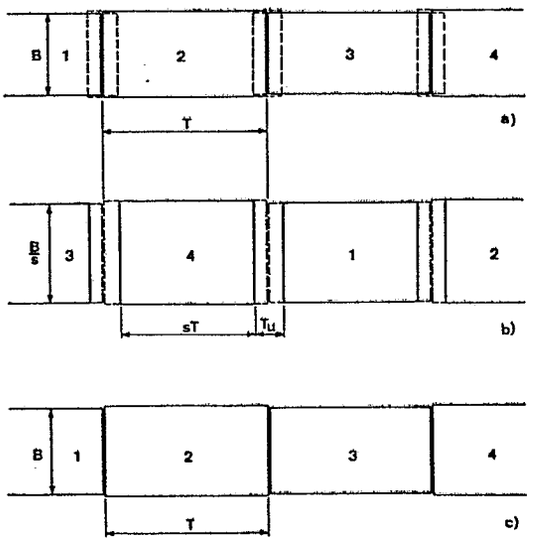

Fig.1

EP 0 042 587 A1

Verfahren zur Umformung von für die verschlüsselte Uebertragung in Signalabschnitte unterteilten Sprachsignalen sowie Vorrichtung zur Ausführung des Verfahrens

Die Erfindung betrifft ein Verfahren zur Umformung von für die verschlüsselte Uebertragung in Signalabschnitte unterteilten Sprachsignalen, wobei die einzelnen Signalabschnitte durch Ein- und Auslesen in bzw. aus Speichern mit unterschiedlichen Ein- und Auslesegeschwindigkeiten zeitlich gestaucht werden, sowie eine Vorrichtung zur Durchführung des Verfahrens.

Bei der Mehrzahl von analogen Sprachschlüsselverfahren wird das zu verschlüsselnde Eingangssignal in Abschnitte unterteilt. Die Aufteilung kann frequenzmässig oder zeitlich oder in beiden Achsen zugleich erfolgen. Die erhaltenen Signalabschnitte werden schlüsselabhängig permutiert. Das Chiffrat besteht dann aus einer veränderten Folge von Signalabschnitten, wobei an den Nahtstellen Diskontinuitäten auftreten. Infolge der endlichen Bandgrenze des Uebertragungskanals findet eine Dispersion statt. Die Stossstelle wird also verwischt, was ein Uebersprechen zwischen zwei zeitlich benachbarten Signalanschnitten zur Folge hat. Weist der Uebertragungskanal neben der Bandbegrenzung noch Gruppenlaufzeitunterschiede auf, was in

praktisch allen Anwendungen der Fall ist, so kann dieser Effekt noch drastisch verstärkt werden, da der Einschwingvorgang eines solchen Kanals länger dauert.

Die Dispersion kann eine erhebliche Beeinträchtigung der Sprachqualität nach der Entschlüsselung bewirken. In der Regel tritt dadurch ein stark störendes impulsartiges Geräusch auf.

Im Zusammehang mit der Uebertragung von Audiosignalen in zeitkomprimierter Form über Videokanäle ist aus der US-PS 2 819 852 bekannt geworden, an den Rändern der entstehenden Signallücken eine Mehrfachübertragung vorzunehmen. Ferner ist es bei Multiplexverfahren mit Zeitkompression gemäss Proceedings of the I.E.F., Band III, Nr. 4, Seite 647 ff bekannt, Lücken zwischen Signalgruppen derart durch Füllsignale auszufüllen, dass bei der Uebertragung eine ausgeglichene Energieverteilung erreicht wird. Schliesslich wird gemäss GB-PS 1 407 196 bei einem Verfahren zum Aendern der Tonlage von Audiosignalen vorgeschlagen, die entstehenden Signallücken mittels Interpolation auszufüllen.

Keines der genannten Verfahren ist geeignet, die insbesonders durch Amplitudensprünge an den Stossstellen von Signalabschnitten bei der analogen Uebertragung von Sprachsignalen in verschlüsselter Form verursachten Effekte zu beseitigen.

Die vorliegende Erfindung hat die Aufgabe, diese beim eingangs erwähnten Verfahren entstehenden Nachteile zu beheben und die Signalunstetigkeiten im Chiffrat zu vermeiden, so dass mittels geeigneter Auswertung auf der Empfangsseite die störenden Auswirkungen ausgeschaltet werden können.

Diese Aufgabe wird durch die Merkmale gemäss den Ansprüchen 1 und 5 gelöst.

Dadurch gelingt es bei der analogen Verschlüs-

selung von Sprachsignalen, die Sprachqualität nach der Entschlüsselung zu erhöhen. Insbesondere werden die störenden Einflüsse der Bandbegrenzung des Uebertragungskanals bekämpft.

Nachfolgend werden anhand der Zeichnungen die der Erfindung zugrundliegenden Prinzipien sowie ein Ausführungsbeispiel näher erläutert. Es zeigen:

Fig. 1a bis 1 c drei schematische Bandbreite-Zeit-Diagramme zur Erläuterung des erfindungsgemässen Verfahrens;

Fig. 2a bis 2c drei schematische Amplituden-Zeit-Diagramme im Umschaltbereich zwischen zwei Signalabschnitten;

Fig. 3 ein Blockschema eines möglichen Ausführungsbeispiels der Erfindung; und

Fig. 4 ein Ablaufdiagramm mit der Ein- und Auslesefolge in die sende- bzw. empfangsseitigen Speicher.

Die Grundidee des Verfahrens besteht darin, dass das Signal zeitlich gestaucht wird und der so gewonnene Zeitraum zur doppelten Uebertragung der kritischen Signalanteile im Bereich der Stossstellen benutzt wird (vgl. Fig. 1). Die zeitliche Stauchung und die damit verbundene Erhöhung der Bandbreite erhält man, indem das zu verarbeitende Signal mit einer bestimmten Geschwindigkeit in einen Speicher eingelesen und mit erhöhter Geschwindigkeit daraus ausgelesen wird. Die im gewonnen Zeitraum wiederholten Signalanteile können mit einer Gewichtsfunktion versehen werden (vgl. Fig. 4). Mit Ihrer Hilfe kann ein weiches Ein- und Ausblenden realisiert werden. Auf der Empfangsseite werden nur jene Signalanteile ausgewertet, die keine Gewichtung erfahren haben. Richtig zusammengesetzt und auf die ursprüngliche zeitliche Länge gedehnt, ergeben sie wieder das ursprüngliche Signal.

Bei spezieller Wahl der Gewichtsfunktion wer-

den keine Signalanteile wiederholt. In diesem technisch besonders einfachen Fall verhindert man zwar keine Bandbreitenerhöhung. Dagegen wird auch hier das Uebersprechen zwischen benachbarten Signalabschnitten vermindert.

Im folgenden wird das Verfahren anhand des Beispiels einer einfachen Zeitpaketvertauschung erläutert. Fig. 1a zeigt ein mögliches Format des zu verschlüsselnden Sprachsignals. Die Signalabschnitte weisen hier eine Bandbreite B und eine zeitliche Länge T auf. Dieses Signal wird mit einer bestimmten Geschwindigkeit in einen Speicher eingelesen und in permutierter Reihenfolge mit $1/_s$-facher Geschwindigkeit ausgelesen. Dadurch erfährt jeder Signalabschnitt T eine zeitliche Stauchung auf die Länge sT, wobei die Bandbreite B auf $B/_s$ anwächst. In den dadurch gewonnenen Zeitabschnitten, den Umschaltintervallen T_U, wird ein Teil der Information ein zweites Mal ausgelesen (siehe Fig. 1a und b). Auf diese Weise kann verhindert werden, dass an den Rändern der Signalabschnitte mit der Länge T bzw. sT Unstetigkeiten auftreten, da an diesen Stellen der ursprüngliche Signalverlauf noch während $T_U/2$ fortgesetzt wird. Die eigentliche Stossstelle tritt dann innerhalb des Umschaltintervalls T_U auf.

Der im Intervall T_U übertragene Signalteil wird im Empfänger ausgetastet, da ja die gesamte Information in den übrigen Abschnitten enthalten ist. diese Abschnitte werden mit einer bestimmten Geschwindigkeit in den empfangsseitigen Speicher eingelesen und in rückvertauschter Reihenfolge mit s-facher Geschwindigkeit ausgelesen (siehe Fig. 1c). Das Signal erhält dadurch wieder die ursprüngliche Bandbreite B. Der im Empfänger nicht benötigte redundante Signalanteil, der im Umschaltintervall T_U übertragen wird, kann

zur Uebertragung mit einer Gewichtungsfunktion versehen werden, welche eine möglichst weiche Umschaltung erlaubt und damit die Einschwingvorgänge auf dem Uebertragungskanal verkürzt.

Fig. 2 zeigt schematische Ausschnitte eines Chiffrats s(t) an einer Stossstelle. In Fig. 2a fehlt die Austastfunktion, in Fig. 2b ist das Chiffrat in einer "weichen" Umschaltfunktion gewichtet. In Fig. 2c ist ein Spezialfall dargestellt. Hier ist die technische Realisierung besonders einfach, die erwünschten Eigenschaften werden aber nur teilweise erreicht.

Fig. 3 zeigt das Blockschema einer möglichen Realisierung des beschriebenen Ausführungsbeispiels.

In einem Eingangsfilter 1 wird das zu verschlüsselnde Sprachsignal auf die Bandbreite B begrenzt. Ueber einen Analog-Digital-Wandler 2 und eine Schalteranordnung 3 wird das Signal in eine Speichergruppe 4 eingelesen. Dieser Einlesevorgang findet nach dem in Fig. 4 gezeigten Schema statt. Mit erhöhter Auslesegeschwindigkeit und in innerhalb eines Signalrahmens T_R permutierter Reihenfolge gelangen die Signalabschnitte mit der Länge T ($T_R = n \cdot T$; n ganzzahlig) über einen Umschalter 5 und einen Digital-Analog-Wandler 6 auf eine steuerbare Verstärkerstufe 7. Durch diesen Auslesevorgang erfährt das Signal die in Fig. 1a und b dargestellte Umformung. Dank dem überlappenden Einlesen zu Beginn und am Ende jedes Signalrahmens (vgl. Fig. 4) kann man das doppelte Auslesen derselben Signalausschnitte im Gebiete der Stossstellen nicht nur innerhalb eines Rahmens, sondern auch am Anfang und Ende jedes Rahmens verwirklichen. Die in Fig. 2b gezeigte weiche Umschaltung wird mit Hilfe des Verstärkers 7 realisiert. Ueber einen Sendefilter 8 wird das Chiffrat hernach in den Uebertragungskanal eingespeist. Die Steuerung der Schalter 3,5 und des variablen Verstär-

kers 7 sowie die Adressierung der Speicher 4 übernimmt eine Steuereinheit 9. Die Steuereinheit 9 des Senders ist dabei in der Lage, die drei Speicherteile und die Schalter der Schalteranordnung 3 einzeln zu adressieren bzw. zu steuern. Durch die Wiederholung einer Adressequenz beim Auslesen kann der betreffende Signalausschnitt ein zweites Mal ausgelesen und übertragen werden, so dass die in Fig. 1 gezeigte Situation entsteht.

Im Empfänger gelangt das Signal über einen Empfangsfilter 10, einen Analog-Digital-Wandler 11 und einen Umschalter 12 in Speicher 13.

Im Gegensatz zum Sender, wo drei Speicher eingesetzt werden, um auf einfache Weise das überlappende Auslesen des Chiffrats an den Rändern des Rahmens T zu ermöglichen, genügen im Empfänger zwei Speicher. Mit verkleinerter Auslesegeschwindigkeit und in rückvertauschter Reihenfolge werden die Signalabschnitte über einen Umschalter 14 und einen Digital-Analog-Wandler 15 einem Ausgangsfilter 16 zugeführt. Auch im Empfänger werden die Umschalter 12,14 und die Adressierung der Speicher 13 von einer Steuereinheit 17 kontrolliert. Fig. 4 gibt einen Ueberblick über den Ein- und Ausleserhythmus im Sender und Empfänger.

Für eine schlüsselabhängige Permutation der Signalblöcke benötigen die Steuereinheiten 9 und 17 die entsprechende Information. Diese liefert ein hier nicht näher erläuterter Schlüsselstromgenerator.

Mit dem erfindungsgemässen Verfahren gelingt es, die Sprachqualität nach der Entschlüsselung zu erhöhen und störende Einflüsse der Bandbegrenzung des Uebertragungskanals zu mildern.

PATENTANSPRUECHE

1. Verfahren zur Umformung von für die verschlüsselte Uebertragung in Signalabschnitte unterteilten Sprachsignalen, wobei die einzelnen Signalabschnitte (T) durch Ein- und Auslesen in bzw. aus Speichern mit unterschiedlichen Ein- und Auslesegeschwindigkeiten zeitlich gestaucht werden, dadurch gekennzeichnet, dass die durch diese Stauchung verfügbar gewordenen Zeitabschnitte (T_u) zur doppelten Uebertragung der Signalanteile im Bereich der Stossstellen jedes Signalabschnittes benutzt werden, dergestalt, dass der ursprüngliche Verlauf des Signals an den Grenzen jedes Signalabschnittes im verschlüsselten Signal erhalten bleibt, und dass das verschlüsselte Signal innerhalb der durch die Stauchung gewonnenen Zeitabschnitte (T_u) mit einer Gewichtungsfunktion versehen wird, dergestalt, dass innerhalb dieser Zeitabschnitte eine beliebige Umschaltfunktion erzielbar ist.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Gewichtungsfunktion stetig ist und zu Beginn jedes Zeitabschnittes (T_u) den Wert 1 annimmt, anschliessend bis zum eigentlichen Umschaltzeitpunkt auf Null sinkt und dann bis zum Ende des Zeitabschnittes (T_u) wieder auf den Wert 1 steigt.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass empfangsseitig die Zeitabschnitte (T_u) ausgetastet und die Signalabschnitte auf ihre ursprüngliche zeitliche Länge gedehnt werden.

4. Verfahren nach Anspruch 1 und 3, wobei sendeseitig mehrere Signalabschnitte (T) zu einem Signalrahmen (T_R) zusammengefasst werden und die Verschlüsselung durch schlüsselabhängiges Vertauschen der Signalabschnitte (T) innerhalb des Signalrahmens vorgenommen wird, dadurch gekennzeichnet, dass die doppelte

Uebertragung an den Stossstellen der Signalrahmen durch überlappendes Einlesen in verschiedene Speicher gefolgt von aufeinanderfolgendem Auslesen dieser Speicher mit erhöhter Geschwindigkeit erzielt wird und dass die doppelte Uebertragung an den Stossstellen der Signalabschnitte (T) innerhalb eines Signalrahmens (T_R) durch doppeltes Auslesen von Grenzbereichen der Signalabschnitte (T) und entsprechend erhöhte Auslesegeschwindigkeit erreicht wird.

5. Vorrichtung zur Durchführung des Verfahrens nach Anspruch 4 mit einer sendeseitigen Einrichtung, die einen Analog-Digital-Wandler (2) und einen Digital-Analog-Wandler (6) aufweist, dadurch gekennzeichnet, dass der Ausgang des Analog-Digital-Wandlers mit einer Schalteranordnung (3) verbunden ist, welche von einer mit ihr verbundenen Steuereinheit (9) derart betätigbar ist, dass das aus dem Analog-Digital-Wandler (2) stammende Signal in Form sich zeitlich überlappender Signalrahmen abwechselnd in je einen von mindestens drei mit der Schalteranordnung (3) verbundenen Speichern (4) einlesbar ist, wobei die Speicher (4) zur Vertauschung und zum teilweisen doppelten Auslesen der Signalabschnitte an den Stossstellen sowie zur Steuerung der Auslesegeschwindigkeit an die Steuereinheit (9) angeschlossen sind, dass die Speicher (4) ausgangsseitig über einen Umschalter (5), der zum Zusammensetzen der ausgelesenen Signalrahmen mit der Steuereinheit (9) verbunden ist, an den Digital-Analog-Wandler (6) angeschlossen sind und dass dem Digital-Analog-Wandler (6) ein ebenfalls mit der Steuereinheit (9) verbundener, variabler Verstärker nachgeschaltet ist.

6. Vorrichtung nach Anspruch 5 mit einer empfangsseitigen Einrichtung, die einen Analog-Digital-Wandler (11) und einen Digital-Analog-Wandler (15) auf-

weist, dadurch gekennzeichnet, dass der Ausgang des Analog-Digital-Wandlers mit einem Umschalter (12) verbunden ist, welcher von einer mit ihm verbundenen Steuereinheit (17) derart betätigbar ist, dass die eintreffenden Signalrahmen abwechselnd in einen von mindestens zwei Speichern (13) einlesbar sind, wobei die Speicher zum Rückgängigmachen der Vertauschung der Signalabschnitte und zu deren Auslesung mit reduzierter Geschwindigkeit unter Austastung der doppelt übertragenen Signalanteile mit der Steuereinheit (1) verbunden sind, und dass die Speicher ausgangsseitig über einen weiteren Umschalter (14), der zum Zusammensetzen der ausgelesenen Signalrahmen ebenfalls mit der Steuereinheit (17) verbunden ist, an den Digital-Analog-Wandler (15) angeschlossen sind.

0042587

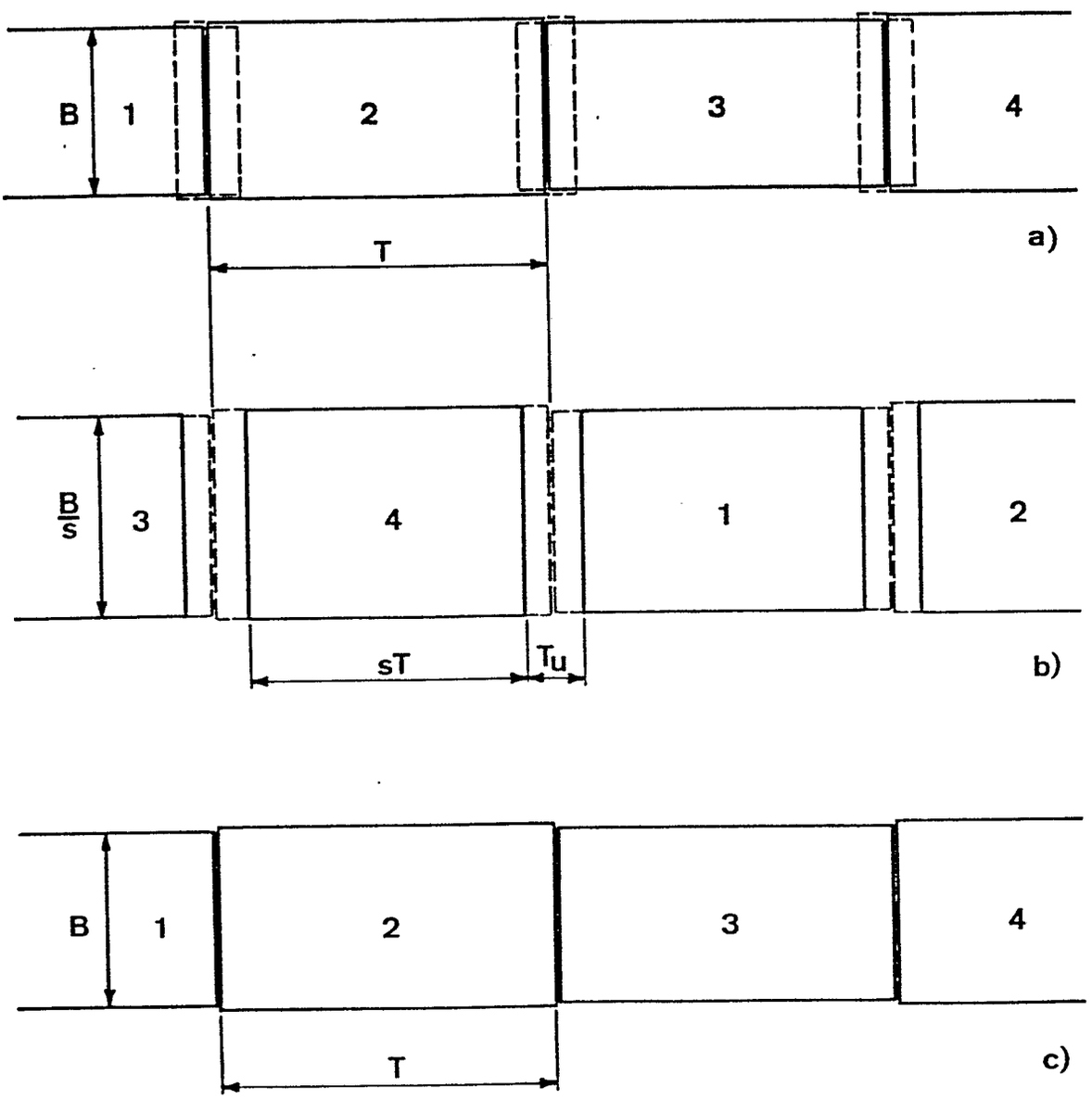

Fig.1

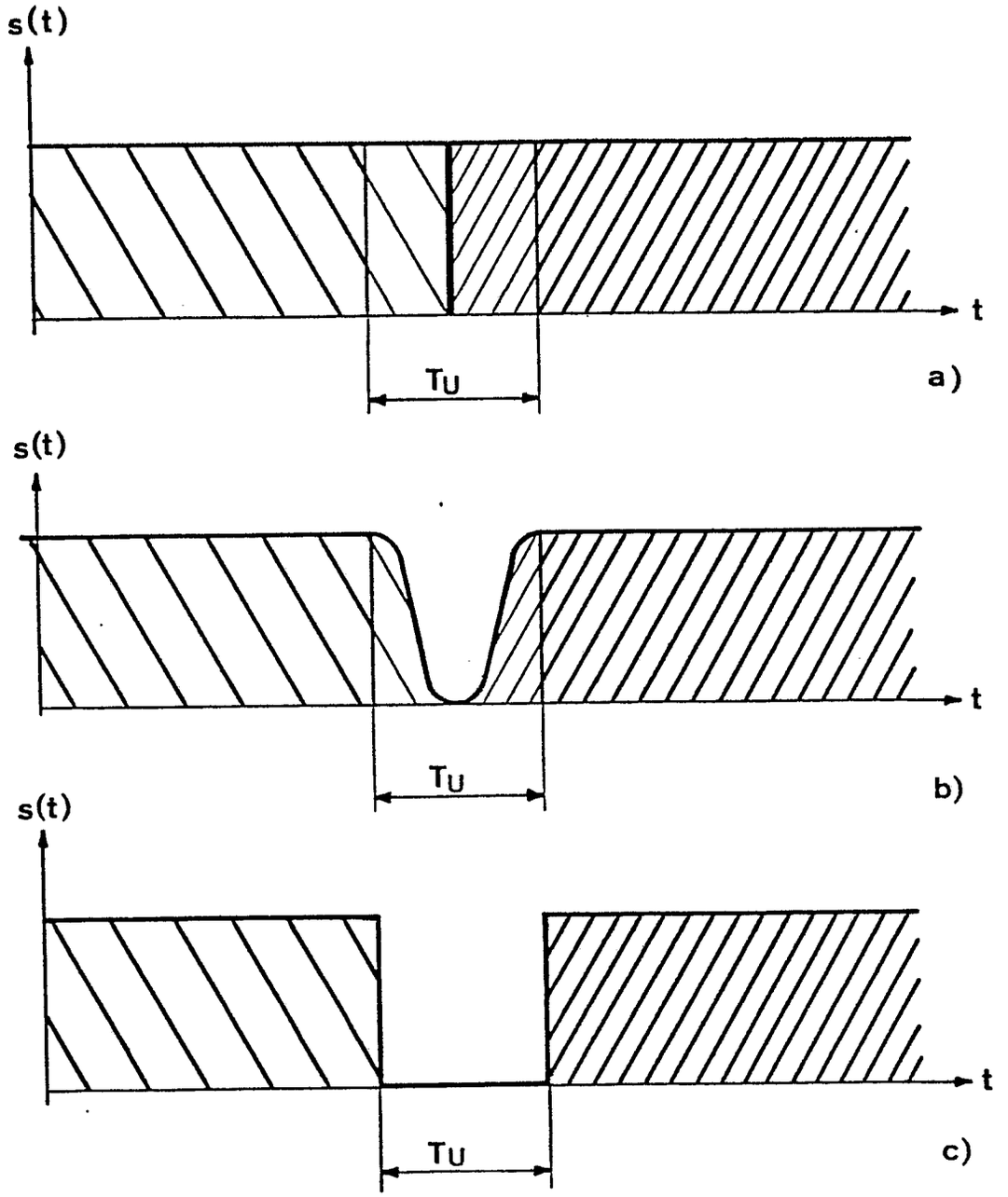

Fig. 2

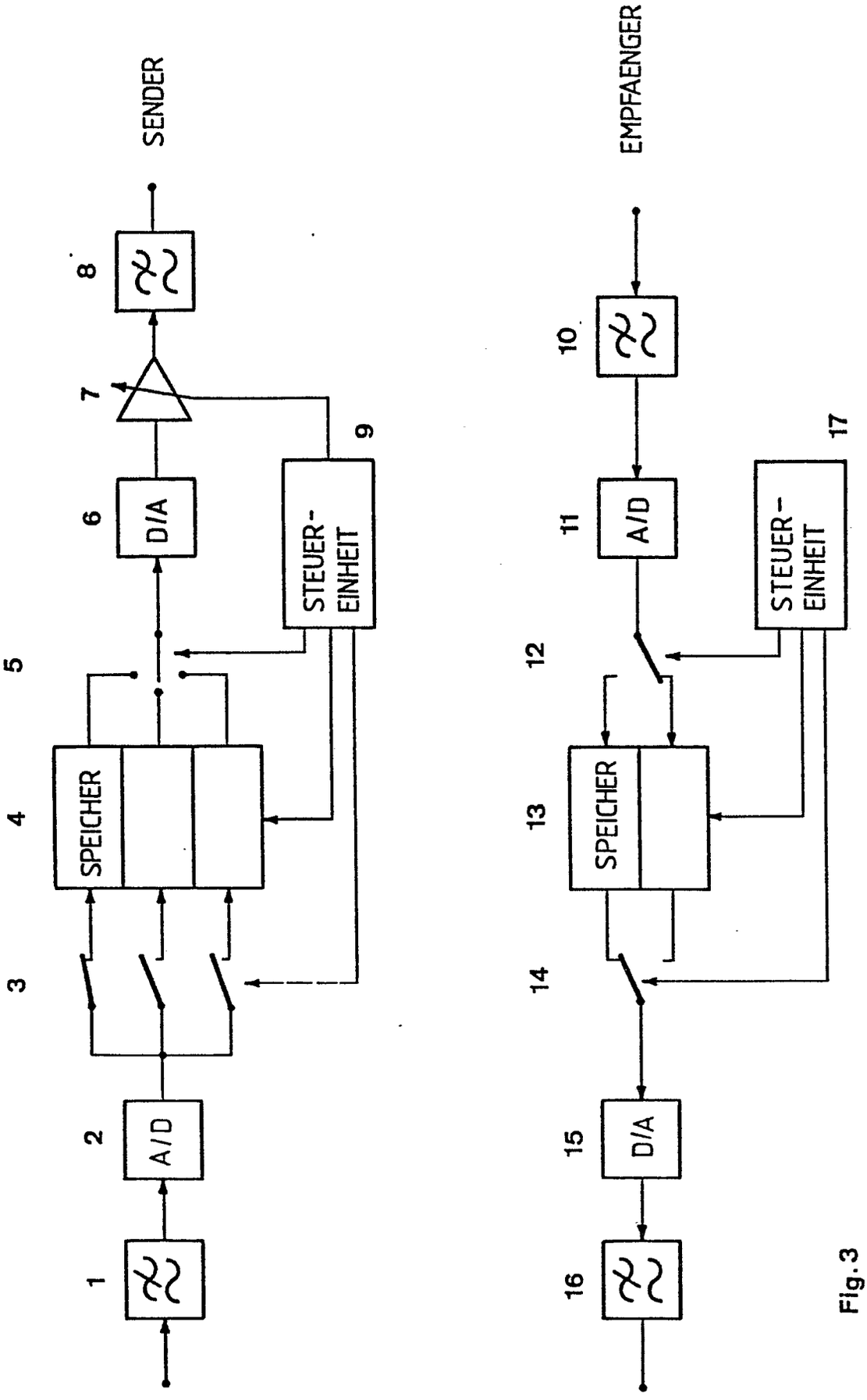
SENDER
EMPFAENGER
1
2
A/D
3
4
SPEICHER
5
6
D/A
7
8
9
STEUER-
EINHEIT
10
11
A/D
12
13
SPEICHER
14
15
D/A
16
17
STEUER-
EINHEIT

Fig.3

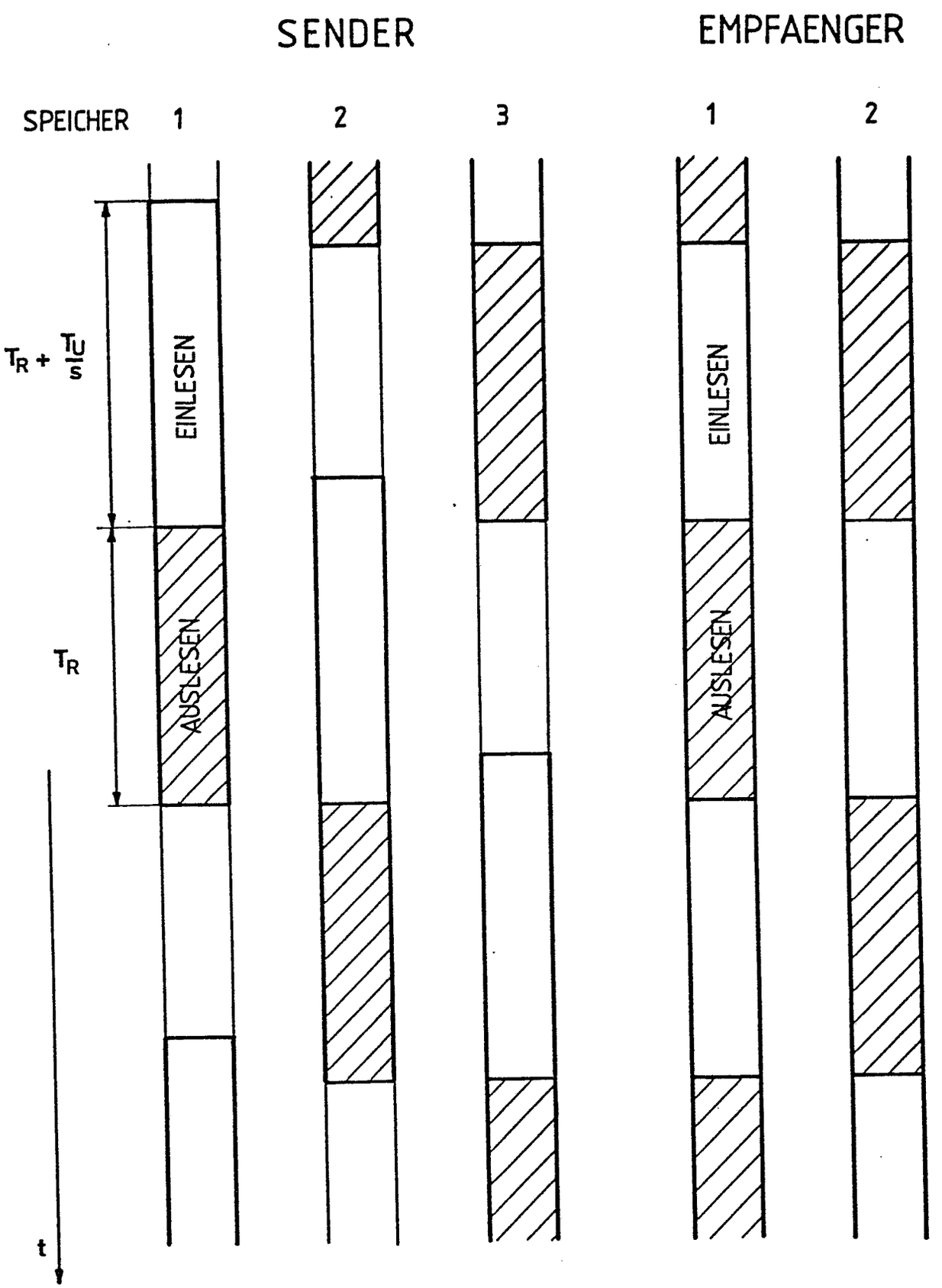
SENDER
EMPFAENGER
SPEICHER
1
2
3
1
2
$T_R + \frac{T_U}{S}$
T_R
EINLESEN
AUSLESEN
EINLESEN
AUSLESEN
t

Fig. 4

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 81 10 4666

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	betrifft Anspruch
D	US - A - 3 819 852 (WOLF) * Spalte 2, Zeilen 7-30; Spalte 3, Zeilen 11-37; Spalte 3, Zeilen 62-64; Spalte 4, Zeilen 21-40 * --	1,4,5
D	PROCEEDINGS OF THE IEE, Band III, Nr. 4, April 1964 J.E. FLOOD et al. "Time-compression-multiplex transmission" Seiten 647-668 * Seite 655, rechte Spalte, Zeilen 13-27; Seite 656, linke Spalte, Zeilen 13-18 * --	1
D	GB - A - 1 407 196 (B.B.C.) * Seite 1, Zeilen 66-75; Seite 2, Zeilen 76-85 * --	1
A	DE - A - 2 834 280 (SIEMENS) * Seite 5, Zeilen 10-29; Seite 9, erste Zeile bis Seite 10, Zeile 2 * ----------	1,4-6

KLASSIFIKATION DER ANMELDUNG (Int. Cl.³)

H 04 K 1/06

RECHERCHIERTE SACHGEBIETE (Int. Cl.³)

H 04 K 1/06
1/00
H 04 B 1/66
H 04 J 3/18

KATEGORIE DER GENANNTEN DOKUMENTE

- X: von besonderer Bedeutung
- A: technologischer Hintergrund
- O: nichtschriftliche Offenbarung
- P: Zwischenliteratur
- T: der Erfindung zugrunde liegende Theorien oder Grundsätze
- E: kollidierende Anmeldung
- D: in der Anmeldung angeführtes Dokument
- L: aus andern Gründen angeführtes Dokument
- &: Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

X Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt.

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	25-09-1981	HOLPER