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

(11) Veröffentlichungsnummer: **0 004 340**
A3

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **79100778.4**

(51) Int. Cl.²: **H 04 K 1/00**

(22) Anmeldetag: **15.03.79**

(30) Priorität: **17.03.78 DE 2811635**

(43) Veröffentlichungstag der Anmeldung:
03.10.79 Patentblatt 79/20

(88) Veröffentlichungstag des später veröffentlichten Recherchenberichts: **17.10.79**

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

(71) Anmelder: **TE KA DE Felten & Guilleaume Fernmeldeanlagen GmbH**
Thurn-und-Taxis-Strasse 10 Postfach 4943
D-8500 Nürnberg 1(DE)

(72) Erfinder: **Robra, Jörg, Dr. Dr.-Ing.**
Hallerstrasse 7
D-8501 Heroldsberg(DE)

(54) Pseudozufällige Erzeugung von orthogonalen Matrizen für Verschlüsselungszwecke.

(57) Orthogonale Zahlenmatrizen werden in der Nachrichtentechnik zum Verschlüsseln von Sprachsignalen verwendet. Liegt eine Nachricht z. B. in digitaler Form vor, so werden unter anderem durch Multiplikation der Zahlen, durch die die Nachricht dargestellt ist, mit den Elementen der Zahlenmatrix neue Zahlen gewonnen, die die verschlüsselte Nachricht darstellen. Wird während der Übermittlung der verschlüsselten Nachricht von Zeit zu Zeit für den Verschlüsselungsprozess eine andere Matrix verwendet, so erschwert das einerseits eine unbefugte Entschlüsselung, erfordert jedoch andererseits zusätzliche Speicherplätze, in denen die Elemente sämtlicher verwendeter Zahlenmatrizen gespeichert werden müssen.

Um Speicherplätze zu sparen, wird ein Verfahren angegeben, nachdem aus einer für die Verschlüsselung verwendeten Zahlenmatrix eine andere dadurch gewonnen wird, daß z. B. die Zeilen der verwendeten Matrix permutiert werden. Diese Zeilenpermutation wird durch einen Pseudo-Zufallsgenerator gesteuert. Der Vorgang der Permutation wird derart in Einzelschritte aufgelöst, daß er ohne weiteres mit digitalen Bausteinen realisiert werden kann.

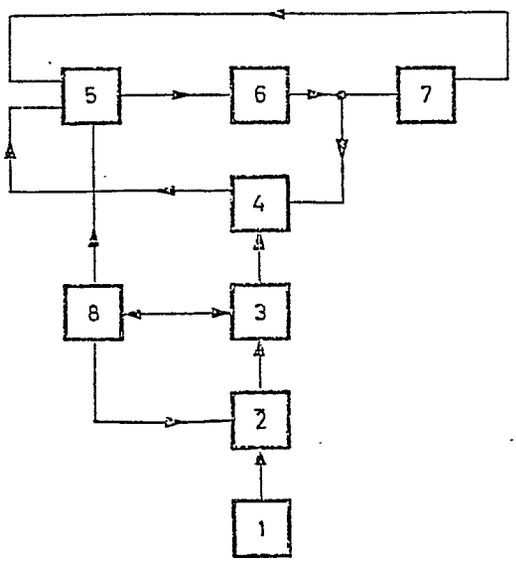

FIG. 3

EP 0 004 340 A3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 79 10 0778

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	betrifft Anspruch
	THE RADIO AND ELECTRONIC ENGINEER Vol. 43, Nr. 8, August 1973, London, GB, V. PHILLIPS et al.: "Speech scrambling by the matrixing of amplitude samples", Seiten 459-470 * Seite 460, linke Spalte, Zeilen 5-16; Seite 469, linke Spalte, Zeilen 36-41 *	1
D	DE - B - 2 523 828 (TEKADE) * Spalte 3, Zeilen 26-31 *	1
P	DE - A - 2 652 607 (LICENTIA) * Seite 10, Zeilen 10-13,19,20 *	1,2
P	DE - A - 2 725 065 (LICENTIA) * Seite 5, letzter Absatz *	1,2

KLASSIFIKATION DER ANMELDUNG (Int.Cl.²)

H 04 K 1/00

RECHERCHIERTE SACHGEBIETE (Int. Cl.²)

H 04 K 1/00
1/06

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

K Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt.

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	26-06-1979	GEISLER