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

(11) Veröffentlichungsnummer: **0 004 340**
A2

(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**

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

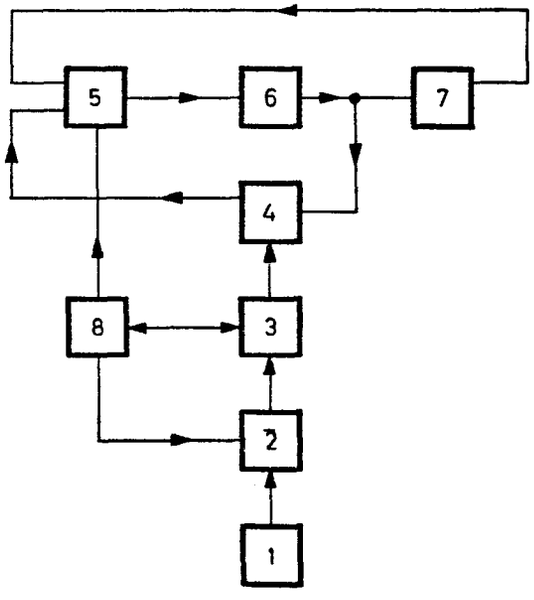
(71) Anmelder: **TE KA DE Felten & Guilleaume Fernmeldeanlagen GmbH, Thurn-und-Taxis-Strasse 10 Postfach 4943, D-8500 Nürnberg 1 (DE)**

(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 anderseits 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.



EP 0 004 340 A2

TE KA DE Felten & Guilleaume
Fernmeldeanlagen GmbH

Den 09.03.1979
P 78 348

Pseudozufällige Erzeugung von orthogonalen Matrizen für Verschlüsselungszwecke.

Die Erfindung betrifft ein Verfahren zur pseudozufälligen Erzeugung von orthogonalen Zahlenmatrizen. Orthogonale Zahlenmatrizen werden u.a. in Verfahren zur Verschlüsselung von Sprache verwendet. Ein solches Verschlüsselungsverfahren ist z.B. in der deutschen Auslegeschrift 2523828 beschrieben. Entsprechend diesem Verfahren werden in einem Zwischenschritt Gruppen von z.B. acht Abtastproben des unverschlüsselten Sprachsignales mit Hilfe einer orthogonalen 8 x 8-Zahlenmatrix nach bekannten Regeln der Matrixtransformation (vgl. hierzu z.B. Zurmühl, Matrizen, Springer Verlag 1958) transformiert und die transformierten Abtastproben weiteren Transformationsprozessen unterworfen. Um auf der Empfängerseite die ursprünglichen Abtastproben zurückzugewinnen, wird in einem entsprechenden Zwischenschritt eine Matrixtransformation mit der inversen Matrix durchgeführt.

Um eine unbefugte Entschlüsselung zu erschweren, ist z.B. in dem Verfahren nach der genannten Auslegeschrift vorgesehen, in einem Festwertspeicher genügender Größe

mehrere Matrizen zu speichern und von Zeit zu Zeit durch einen Pseudozufallsgenerator eine andere Matrix aussuchen zu lassen, die zur Transformation bzw. Rücktransformation der Proben verwendet wird. Die unbefugte Entschlüsselung wird umso schwieriger, je mehr verschiedene Matrizen zur Verfügung stehen und benutzt werden. Die Größe eines aus unterschiedlichen Matrizen bestehenden Vorrates ist allerdings durch die Kapazität der Festwertspeicher sowie der nötigen Adreßspeicher begrenzt.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren anzugeben, durch das bei möglichst geringem Aufwand an Speicherplätzen eine möglichst große Anzahl von unterschiedlichen orthogonalen Matrizen auf pseudozufällige Weise erzeugt und für die Transformation bzw. Rücktransformation der Abtastproben bereitgestellt werden kann.

Diese Aufgabe wird dadurch gelöst, daß aus einer schon für die Verschlüsselung verwendeten orthogonalen Matrix durch pseudozufällige Permutation ihrer Zeilen oder Spalten eine andere Matrix erzeugt wird.

Anhand eines Ausführungsbeispieles soll das erfindungsgemäße Verfahren, die Mittel zu seiner Durchführung sowie seine Weiterbildungen erläutert werden.

Fig. 1 zeigt ein einfaches Beispiel einer orthogonalen Zahlenmatrix. Die Matrix besteht aus vier durchnummerierten Zeilenvektoren (Zahlenreihe von rechts nach links) und vier Spaltenvektoren (Zahlenreihe von oben nach unten). Die Matrix nach Fig. 1 kann gleichzeitig als Bild des Inhaltes einer entsprechend großen Speichermatrix eines Schreib-Lese-Speichers verstanden werden. Permutationen der Zeilen der Zahlenmatrix, wie z.B. Vertauschen von zwei Zeilen, korrespondieren dann

zur Vertauschung des Inhaltes der entsprechenden Zeilen der Speichermatrix. So zeigt z.B. Fig. 2 die Matrix, die aus der Zahlenmatrix nach Fig. 1 durch Vertauschen des zweiten mit dem vierten Zeilenvektor hervorgegangen ist. Übertragen auf die Speichermatrix bedeutet, daß der Inhalt der zweiten Speicherzeile mit dem Inhalt der vierten Speicherzeile des Schreib-Lese-Speichers vertauscht worden ist. Wichtig im vorliegenden Zusammenhang ist, daß auch nach der Permutation die Zahlenmatrix eine orthogonale Matrix ist und damit für die Transformation auf der Sendeseite und die Rücktransformation auf der Empfangsseite in der gleichen Weise verwendet werden kann wie die Ausgangsmatrix.

Fig. 3 dient zur Erläuterung einer Anordnung, mit der das erfindungsgemäße Verfahren durchgeführt werden kann. Die verwendeten Bauteile sind ein Zufallsgenerator 1, ein Adreßspeicher 3, ein Schreib-Lese-Speicher 4, ferner ein Umschalter 5, ein erstes Schieberegister 6, ein zweites Schieberegister 7, sowie eine Steuereinheit 8. Sämtliche Bauteile zusammen bilden ein getaktetes System, wobei der Taktgenerator sowie die Zuführungsleitungen zu den Takteingängen der einzelnen Bausteine nicht eingezeichnet sind. Im Adreßspeicher 2 werden die vom Pseudozufallsgenerator 1 abgegebenen Zufallszahlen gespeichert. Der Schreib-Lese-Speicher 4 hat die Form eines Matrizenspeichers und besitzt ebenso viele Speicherstellen wie die zu behandelnde Zahlenmatrix Komponenten. Die Steuereinheit 8 schaltet über die eingezeichneten Verbindungen die beiden Speicher 2 und 4 vom Lese- in den Schreibbetrieb um. Außerdem bedient sie den Umschalter 5 sowie den Adreßzähler 3 und verarbeitet Informationen über dessen Zählerstand. Die bisher für die Verschlüsselung verwendete Zahlenmatrix ist im Speicher 4 gespeichert. Der Permutationsprozess zur Erzeugung einer anderen Zahlenmatrix wird damit eingelei-

tet, daß der Zufallsgenerator 1 eine Zufallszahl an den Adreßspeicher 2 abgibt und der Adreßzähler 3 von der Steuereinheit 8 auf die Adresse 0 gesetzt wird. Bei entsprechender Stellung des Umschalters 5 und einem Steuersignal von der Steuereinheit 8 an den Speicher 4 hat das zur Folge, daß der Inhalt der Speicherzelle mit der Adresse 0 in das Schieberegister 6 eingelesen wird. Sodann gibt die Steuereinheit 8 an den Speicher 2 und den Adreßzähler 3 die nötigen Befehle dafür, daß dieser auf die Adresse eingestellt wird, die im Adreßspeicher 2 gespeichert ist. Nach der Einstellung des Adreßzählers wird die der eingespeicherten Adresse entsprechende Speicherzeile des Speichers 4 in das Schieberegister 6 übernommen, während der bisherige Inhalt des Schieberegisters 6 an das Schieberegister 7 weitergegeben wird. Sodann wird der Umschalter 5 durch die Steuereinheit 8 in eine Stellung gebracht, die ein ringförmiges Zusammenschließen des Schieberegisters 6 und 7 bewirkt. Dadurch wird erreicht, daß durch die nächsten Takte die Inhalte der Schieberegister 6 und 7 vertauscht werden. Ist dieser Vertauschungsvorgang abgeschlossen, so stellt die Steuereinheit den Adreßzähler 3 sofort auf 0. Der Inhalt des Schieberegisters 6 wird nun in die Speicherzeile mit der Adresse 0 eingelesen, während gleichzeitig der Gesamtinhalt der Register 6 und 7 zyklisch verschoben wird. Ist die Speicherzeile mit der Adresse 0 beschrieben, so wird der Adresszähler 3 erneut mit dem unverändert gebliebenen Inhalt des Adreßspeichers 2 eingestellt. Jetzt erfolgt das Beschreiben der dieser Adresse entsprechenden Speicherzeile mit dem zu diesem Zeitpunkt im Schieberegister 6 enthaltenen Inhalt. Ist auch diese Speicherzeile beschrieben, so ist folgender Endzustand des Speichers erreicht: Der Inhalt der Speicherzeile mit der Adresse 0 ist in die Speicherzeile mit der zu Anfang vom Pseudo-Zufallsgenerator erzeugten Adresse gelangt, während

der Inhalt dieser Speicherzeile in die Zeile mit der Adresse 0 eingeschrieben wurde.

Nun stellt die Steuereinheit den Adreßzähler abermals auf 0 und bringt den Umschalter 5 in eine Stellung, in der aus dem Matrizenspeicher 4 Informationen in das Schieberegister 6 übertragen werden können. Ist der Inhalt der Speicherzeile mit der Adresse 0 in das Schieberegister 6 geschrieben, so wird der Adreßzähler auf 1 gestellt. Der Inhalt der Zeile mit der Adresse 1 des Speichers 4 wird nun in das Schieberegister 6 eingelesen, wobei der dort gespeicherte Inhalt in die Zeile mit der Adresse 1 übernommen wird. Nach Abschluß dieses Vorgangs wird der Stand des Zählers abermals um eine Einheit erhöht und der Inhalt der diesem Zählerstand zugeordneten Speicherzeile mit dem Inhalt des Schieberegisters 6 ausgetauscht. Der Vorgang wiederholt sich solange, bis sämtliche Adressen durchgelaufen sind und der Zähler wieder bei der Adresse 0 angelangt ist. Ist die Zeile mit der Adresse 0 durch den Inhalt der Zeile mit der höchsten Adresse überschrieben worden, so ist durch die beschriebenen Verfahrensschritte eine zyklische Verschiebung sämtlicher Zeileninhalte des Speichers 4 erreicht worden. Insgesamt gesehen ist der Inhalt des Speichers 4 aus dem ursprünglichen Inhalt durch eine Permutation der Zeileninhalte hervorgegangen, und zwar besteht diese Permutation aus der Vertauschung zweier Zeilen mit anschließender zyklischer Verschiebung um genau eine Stelle.

Was bisher über die Zeilen des Speichers 4 gesagt worden ist, läßt sich mit nur geringen Abwandlungen auch mit den Spalten durchführen. Möglich ist auch, daß Zeilen- und Spaltenpermutationen gemischt werden.

Die Erzeugung einer Permutation der Zeileninhalte der Speichermatrix 4 nach dem beschriebenen Verfahren hat den Vorteil, daß mit nur einer Zufallszahl eine Zahlenmatrix zur Verfügung steht, die sich von der vorangegangenen Zahlenmatrix in der Regel in jeder Zeile unterscheidet. Aus kryptologischen Gründen ist ein möglichst großer Unterschied zwischen zwei nacheinander verwendeten Zahlenmatrizen wünschenswert. Dieser Unterschied könnte auch durch mehrmaliges pseudozufälliges Vertauschen jeweils zweier Zeilen erreicht werden. Jedoch wäre es dann nötig, daß in dem Zeitraum, in dem die neue Matrix zu Verschlüsselungszwecken zur Verfügung gestellt werden muß, der Zufallsgenerator mehr als eine Adresse abzugeben hat, er also mit einer höheren Taktfrequenz betrieben werden muß. Da in den meisten Anwendungsfällen der Zufallsgenerator ohnehin schon an der Grenze seiner obersten Taktfrequenz betrieben wird, ist eine weitere Erhöhung der Taktfrequenz unmöglich. Die erfindungsgemäße Ausgestaltung des Verfahrens zur Lösung der gestellten Aufgabe zeigt einen leicht gangbaren Ausweg aus den genannten Schwierigkeiten.

TE KA DE Felten & Guilleaume
Fernmeldeanlagen GmbH

Den 09.03.1979
P 78 348

Patentansprüche

1. Pseudozufällige Erzeugung von orthogonalen Zahlenmatrizen für Verschlüsselungszwecke, dadurch gekennzeichnet, daß aus einer schon für die Verschlüsselung verwendeten orthogonalen Zahlenmatrix durch pseudozufällige Permutation ihrer Zeilen oder Spalten eine andere orthogonale Zahlenmatrix erzeugt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zu einer pseudozufälligen Permutation der Zeilen einer orthogonalen Zahlenmatrix ihre Komponenten in den Speicherelementen eines Matrizenspeichers (4) gespeichert werden und daß mit einer Steuereinrichtung (8) und einem einstellbaren Adresszähler (3) der Inhalt der ersten Speicherzeile des Matrizenspeichers und der Inhalt einer Speicherzeile, deren Adresse von einem Pseudo-Zufallsgenerator bestimmt wurde, zunächst aus dem Matrizenspeicher ausgelesen und in jeweils einem Schieberegister (6,7) zwischengespeichert und danach in den Matrizenspeicher so eingelesen werden, daß die Inhalte der beiden erwähnten Speicherzeilen des Matrizenspeichers miteinander vertauscht sind und daß anschließend der Inhalt der ersten Speicherzeile in eines der Schieberegister (6) eingelesen wird und daß der Inhalt der nächsten Speicherzeile mit dem Inhalt des Schieberegisters ausgetauscht wird, und daß dieser Austauschvorgang mit den folgenden Speicherzeilen so lange wiederholt wird, bis jede Speicherzeile einmal ihren Inhalt mit dem Schieberegister (6) getauscht hat.

	1	2	3	4
1	0,1	-0,1	0,7	0,7
2	0,1	0,1	0,7	-0,7
3	0,7	-0,7	-0,1	-0,1
4	0,7	0,7	-0,1	0,1

FIG. 1

	1	2	3	4
1	0,1	-0,1	0,7	0,7
2	0,7	0,7	-0,1	0,1
3	0,7	-0,7	-0,1	-0,1
4	0,1	0,1	0,7	-0,7

FIG. 2

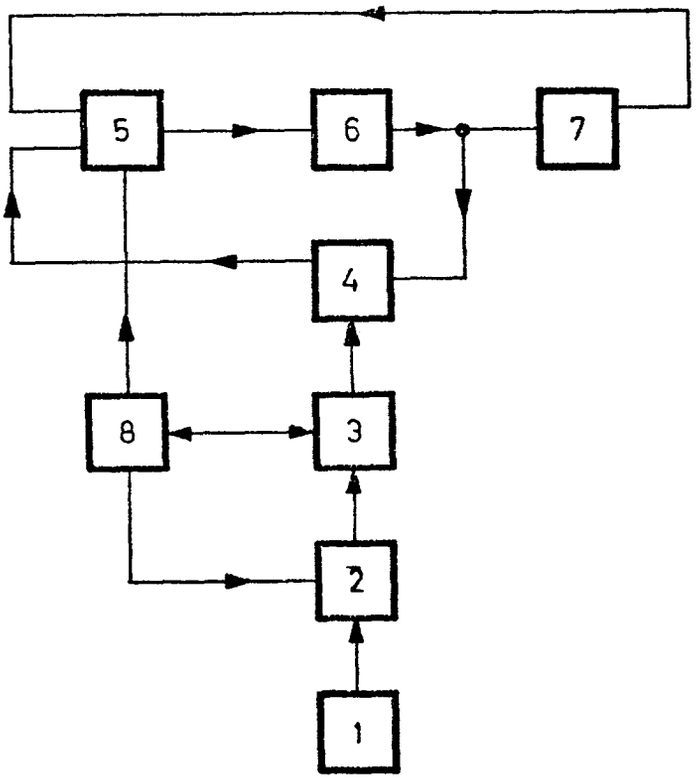


FIG. 3