

①



Europäisches Patentamt
European Patent Office
Office européen des brevets

⑪

Veröffentlichungsnummer: **0 136 681**
B1

⑫

EUROPÄISCHE PATENTSCHRIFT

④

Veröffentlichungstag der Patentschrift:
13.07.88

⑤

Int. Cl. 4: **H 04 K 1/00**

⑥

Anmeldenummer: **84111665.0**

⑦

Anmeldetag: **28.09.84**

⑤

Verfahren zur verschlüsselten Nachrichtenübertragung.

⑩

Priorität: **30.09.83 DE 3335672**

④

Veröffentlichungstag der Anmeldung:
10.04.85 Patentblatt 85/15

⑤

Bekanntmachung des Hinweises auf die Patenterteilung:
13.07.88 Patentblatt 88/28

⑧

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

⑥

Entgegenhaltungen:
EP - A - 0 032 107
DE - A - 2 722 700
DE - B - 2 659 622

⑦

Patentinhaber: **Siemens Aktiengesellschaft Berlin und München, Wittelsbacherplatz 2, D-8000 München 2 (DE)**

⑦

Erfinder: **Hofmann, Ludwig, Dipl.-Ing., Raiffeisenstrasse 64, D-8044 Lohhof (DE)**
Erfinder: **Stadler, Klaus, Reismühlerstrasse 33, D-8035 Gauting (DE)**

EP 0 136 681 B1

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99(1) Europäisches Patentübereinkommen).

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren zur verschlüsselten Nachrichtenübertragung in Übertragungssystemen mit fest stationierten und/oder mobilen Teilnehmergeräten (Endgeräten), beispielsweise in Telefon-, Autotelefon- oder Funknetzen, bei dem im Endgerät der einen Übertragungsseite ein Geber für einen individuellen Teilnehmerschlüssel und in der als Zentralstation ausgebildeten anderen lediglich amtsseitig zugänglichen Übertragungsseite ein Auswerter angeordnet ist und bei dem in einem ersten Verfahrensschritt von der den Geber enthaltenden Übertragungsseite die Teilnehmernummer an die andere Übertragungsseite übertragen, in dieser der Teilnehmerschlüssel ermittelt und der Empfänger entsprechend dem Schlüssel eingestellt wird und bei dem danach in einem zweiten Verfahrensschritt im den Geber enthaltenden Endgerät der Übertragungsweg zur Übertragung des verschlüsselten Nutzsignals auf den Sendeteil durchgeschaltet wird.

Mit der zunehmenden Ausbreitung von Mobilfunkanlagen stellt die Verschlüsselung der Nachrichtenübertragung auf dem Funkwege mit zunehmendem Masse ein besonderes Problem dar. Die verschiedenen, sich hierfür anbietenden Möglichkeiten, beispielsweise kryptologische Verfahren oder Verschleierung der Funkwege, sind von der technischen Realisierung meist recht aufwendig.

Eine Realisierung mit Hilfe der n-Band-Vertauschung auf statischem Wege durch einen einheitlichen Schlüssel für das gesamte Funksystem oder mit verschiedenen Verschleierungsschlüsseln, deren Anzahl aufgrund von Pre-Emphase und De-Emphase sowie der erforderlichen Verschleierungsmöglichkeit auf wenige Konstellationen begrenzt ist, bietet neben den Vorteilen geringer Komplexität und Optimierung der Übertragungsqualität bzw. Verschleierung der einzelnen Verbindungen mit unterschiedlichen Verschleierungsmodi den Nachteil, dass sich mit Hilfe eines normalen Funk-Sende/Empfängergerätes die Funkwege durch Einstellung auf die verschiedenen Verschleierungsmodi abhören lassen.

Bei Anwendung einer dynamischen Methode durch zeitlichen Wechsel der einzelnen Verschleierungsmodi und damit Erhöhung des Verschleierungsgrades wird zwar die Verschleierungssicherheit beträchtlich erhöht, es besteht jedoch die Möglichkeit, mit einem normalen Funk-Sende-Empfänger durch entsprechende zeitliche Erfassung des Verschleierungsgrades die Funkwege zu entschleiern.

Ein Verfahren zur verschlüsselten Nachrichtenübertragung der im Oberbegriff des Anspruchs 1 beschriebenen Art ist durch die DE-B-2 659 622 bekannt. Diese beschreibt ein Funktelefoniesystem für eine grössere Zahl von Teilnehmern, bei dem die Nachrichten durch ein Verschlüsselungs- oder Verschleierungsgerät insbesondere mittels digitaler Signale, z.B. mit bestimmter teilnehmerindividueller Folge, d.h. mit bestimmtem teil-

nehmerindividuellen Schlüssel, übertragen werden. Dabei ist neben der bestimmten individuellen Schlüsseleinstellung bei jedem Teilnehmer die Teilnehmernummer selbst oder zusätzlich ein spezieller Code gespeichert. Zwischen der Teilnehmernummer bzw. dem Code und der individuellen Schlüsseleinstellung besteht ein funktioneller, nur der übergeordneten Vermittlungsstelle (Funküberleitstelle) bekannter Zusammenhang. Dieser individuelle Schlüssel wird in der Vermittlungsstelle errechnet und das Verschlüsselungs- bzw. Verschleierungsgerät programmiert. Dann wird die verschlüsselte Übertragung zur Vermittlungsstelle und von dort aus gegebenenfalls nach Umsetzung in den Schlüssel des Gesprächspartners die Übermittlung der Nachrichten durchgeführt.

Ferner ist aus der EP-A-0 032 107 ein Chiffrier-/Dechiffriersystem bekannt mit einem Chiffrierteil mit Mitteln zum Umwandeln von Klartexten in ein Chifftrat und einem Dechiffrierteil mit Mitteln zum Rückumwandeln des Chifftrats in Klardaten. Der Chiffrierteil enthält einen Chiffriergenerator, dessen Anfangszustand und/oder Struktur wenigstens durch einen ersten geheimen Schlüssel bestimmt wird, sowie einen ersten Speicher mit einer Anzahl verschiedener erster Schlüssel. Der Dechiffrierteil enthält einen gleich wie der Chiffriergenerator aufgebauten Dechiffriergenerator sowie einen zweiten Speicher mit denselben ersten Schlüsseln wie im ersten Speicher. Chiffrier- und Dechiffrierteil enthalten ferner Schlüssellademittel, um bei einer Neuinitialisierung des Systems einen ersten Schlüssel aus dem ersten Speicher auszuwählen, in den Chiffriergenerator zu laden, die Speicheradresse des ausgewählten ersten Schlüssels zum Dechiffrierteil zu übertragen und dort aufgrund der übertragenen Speicheradresse denselben ersten Schlüssel aus dem zweiten Speicher auszulesen und in den Dechiffriergenerator zu laden. Die Schlüssellademittel sind dabei durch eine im Chiffrierteil befindliche Zufallstufe gesteuert, welche bei jeder Neuinitialisierung des Systems eine zufällige Auswahladresse für die im ersten und zweiten Speicher enthaltenen und bei der Neuinitialisierung neu zu ladenden ersten Schlüssel bildet.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zur verschlüsselten Nachrichtenübertragung zu schaffen, das vielseitig in Netzen der Nachrichtenübertragung einsetzbar und relativ schwer automatisch abhörbar ist.

Diese Aufgabe wird gemäss der Erfindung gelöst durch eine hierarchische Struktur derart, dass in den Netzen jeweils mehrere Endgeräte mit einer Zentrale verbunden sind und die Codesignalisierung vom Endgerät zum Zentralgerät in einem nicht systemkompatiblen Ablauf erfolgt, und ferner dadurch, dass im ersten Verfahrensschritt von der den Geber enthaltenden Übertragungsseite der eingestellte Code an die als Zentralstation ausgebildete andere Übertragungsseite übertragen wird.

In vorteilhafter Weiterbildung des erfindungsgemässen Verfahrens ist vorgesehen, dass der

übertragene Code einen Zeiger in einer Codetabelle bildet.

Nachstehend wird die Erfindung anhand eines in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert.

In der Figur ist ein Verschlüsselungssystem für eine Mobil-Telefonanlage im Blockschaltbild dargestellt. Hierbei sind ein Mobilgerät und ein Feststationsteil (Funkkonzentrator) vorgesehen, die über ein Funkfeld FF miteinander in Funkverbindung stehen. Das Mobilgerät enthält einen Handset 1, einen mit diesem verbundenen NF-Verstärker und Voice-Scrambler, die im Kästchen 2 angeordnet sind, sowie einen diesem nachgeschalteten Funkteil 3, der ausgangsseitig mit einer Antenne A1 verbunden ist. NF-Verstärker und Voice-Scrambler 2 sind über eine Empfangsleitung und eine Sendeleitung für die Niederfrequenz miteinander verbunden. In der Sendeleitung ist ein Umschalter S eingefügt, der von einem Code-Geber 4 angesteuert wird. Der Code-Geber 4 ist ferner mit dem NF-Verstärker und Voice-Scrambler 2 verbunden und bewirkt in dieser die Code-Einstellung sowie mit einer Signalisierungseinheit 5, die ausgangsseitig an den einen Umschaltkontakt des Umschalters S angeschlossen und über diesen Umschalter S an den Sendeweg des Mobilgeräts anschaltbar ist. Der Feststationsteil enthält einen mit einer Antenne A2 verbundenen Funkteil 6, der mit einem Voice-Scrambler und einer NF-Anpassung, welche in dem Kästchen 7 angeordnet sind, verbunden ist. Voice-Scrambler und NF-Anpassung sind ausgangsseitig zur Übertragung der Niederfrequenz NF zu einer in der Figur nicht dargestellten Überleiteinrichtung ÜLE geführt, die eine Verbindungseinrichtung zwischen dem Feststationsteil (Funkkonzentrator) und dem Fernsprechnet mit den Vermittlungsämtern bildet. Funkteil 6 und Voice-Scrambler und NF-Anpassung 7 sind über eine Empfangsleitung und eine Sendeleitung für die Niederfrequenz miteinander verbunden, wobei von der Empfangsleitung eine Verbindung zu einem Code-Auswerter und einer Synchronisiereinrichtung, die in dem Kästchen 8 enthalten sind, geführt ist. Dieses ist ausgangsseitig zur Codeeinstellung mit dem Voice-Scrambler und der NF-Anpassung 7 verbunden. Die Funkteile 3 und 6 in den beiden Endgeräten können aus handelsüblichen Sende/Empfangsgeräten bestehen, die in der dargestellten Weise mit den jeweiligen Verschleierungseinrichtungen zusammengeschaltet werden.

Bei dem vorliegenden Verschlüsselungssystem unterscheidet man in der Verschleierungsschaltung zwischen einer solchen für die beweglichen Stationen und einer solchen, die ausschliesslich für die Funkkonzentratoren, also den Feststationsteil, vorgesehen ist. Es wird hierbei ein dynamischer Verschleierungsmodus unter Benutzung der 4-Band-Vertauschung angewendet, der z.B. mit Hilfe eines Zufall-Generators von dem beweglichen Teilnehmer mit dem Geber zu der Verschleierungseinrichtung des Funkkonzentrators mit dem Empfänger übertragen wird. Es besteht natürlich auch die Möglichkeit, diesen Empfänger

in der Überleiteinrichtung und/oder in den Vermittlungsstellen oder auch beim B-Teilnehmer zu installieren.

Die Verschlüsselung des Funkweges erfolgt in der Weise, dass zunächst von der Signalisierungseinheit 5 aus über den vom Code-Geber 4 angesteuerten Umschalter S der Feststationsteil auf das Mobilgerät synchronisiert wird. Vom Code-Geber wird dann der dynamische Verschleierungsmodus vom Mobilgerät zum Feststationsteil übertragen, und über dessen Code-Auswerter und Synchronisiereinrichtung 8 erfolgt die Codeeinstellung im Voice-Scrambler und der NF-Anpassung 7, so dass das übertragene, verschleierte Signal im Empfänger des Feststationsteils richtig erkannt wird.

Das erfindungsgemässe Verfahren beruht auf dem Prinzip, dass Endgeräte nur einen Übertragungscode erzeugen, jedoch nicht auswerten können. Die Auswerter wiederum sind nicht in der Lage, den Code zu erzeugen und sie sind ausserdem nur in begrenzten Stückzahlen vorhanden. Es ist nämlich hierbei eine streng hierarchische Struktur vorgesehen. Das heisst in den betreffenden Netzen sind auf der Feststationsseite immer mehrere Endgeräte mit einer Zentrale verbunden, die nur von autorisiertem Personal betreten und gewartet wird. Der vom Endgerät, hier also dem Mobilgerät, zu einem Zentralschlüsselgerät übertragene Schlüssel bildet lediglich einen Zeiger in einer Codetabelle. Hierdurch kann in gleich aufgebauten Systemen durch Veränderung der Codetabelle eine Abhörsicherheit erreicht werden.

Der Vorteil des erfindungsgemässen Verfahrens besteht darin, dass neben einer hohen Zahl an Verschleierungsmodi durch den Einsatz eines normalen, zu diesem entsprechenden Mobilfunksystem gehörenden Funk-Sende-Empfängers die Funkwege nicht abgehört werden können, da dieser Funk-Sende-Empfänger nur mit einem Geber und nicht mit einem Empfänger ausgestattet ist, der Verschleierungs-Empfänger durch entsprechende Lieferbeschränkung für den öffentlichen Verkehr nicht freigegeben werden kann und dieses System, obwohl die Funkteilnehmergeräte auf dem freien Markt unbeschränkt verkauft werden können, ein hohes Mass an Verschleierungssicherheit enthält.

Patentansprüche

1. Verfahren zur verschlüsselten Nachrichtenübertragung in Übertragungssystemen mit fest stationierten und/oder mobilen Teilnehmergeräten (Endgeräten), beispielsweise in Telefon-, Autotelefon- oder Funknetzen, bei dem im Endgerät der einen Übertragungsseite ein Geber (4) für einen individuellen Teilnehmerschlüssel und in der als Zentralstation ausgebildeten anderen lediglich amtsseitig zugänglichen Übertragungsseite ein Auswerter (8) angeordnet ist und bei dem in einem ersten Verfahrensschritt von der Geber (4) enthaltenden Übertragungsseite die Teilnehmernummer an die andere Übertragungsseite übertragen, in dieser der Teilnehmerschlüssel er-

mittelt und der Empfänger entsprechend dem Schlüssel eingestellt wird und bei dem danach in einem zweiten Verfahrensschritt im den Geber (4) enthaltenden Endgerät der Übertragungsweg zur Übertragung des verschlüsselten Nutzsignals auf den Sendeteil durchgeschaltet wird, gekennzeichnet durch eine hierarchische Struktur derart, dass in den Netzen jeweils mehrere Endgeräte mit einer Zentrale verbunden sind und die Codesignalisierung vom Endgerät zum Zentralgerät in einem nicht systemkompatiblen Ablauf erfolgt, und ferner dadurch, dass im ersten Verfahrensschritt von der den Geber (4) enthaltenden Übertragungsseite der eingestellte Code an die als Zentralstation ausgebildete andere Übertragungsseite übertragen wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der übertragene Code einen Zeiger in einer Codetabelle bildet.

Claims

1. Method for the coded transmission of messages in transmission systems having permanently stationary and/or mobile subscriber units (terminals), for example in telephone, car telephone or radio networks, in which method a transmitter (4) for an individual subscriber code is arranged in the terminal of one transmission side and an analyser (8) is arranged in the other transmission side which is constructed as central station and is only accessible from the exchange side and in which method, in a first method step, the subscriber number is transmitted from the transmission side containing the transmitter (4) to the other transmission side, the subscriber code is determined in the latter and the receiver is set in accordance with the code and in which method, thereafter, in a second method step, the transmission path is switched through to the transmit section in the terminal containing the transmitter (4), for transmitting the coded useful signal, characterized by a hierarchical structure, in such a manner that several terminals are in each case connected to a centre in the networks and the code

signalling from the terminal to the central unit occurs in a non system-compatible sequence, and also in that, in the first method step, the code set is transmitted from the transmission side containing the transmitter (4) to the other transmission side constructed as central station.

2. Method according to Claim 1, characterized in that the transmitted code forms a pointer in a code table.

Revendications

1. Procédé de transmission chiffrée d'informations dans des systèmes de transmission comportant des postes d'abonnés (terminaux) fixes et/ou mobiles, par exemple dans des réseaux téléphoniques, radiotéléphoniques ou radio, dans lequel il est prévu, dans le terminal d'un des côtés de la transmission, un générateur (4) destiné à un code propre au terminal, et dans l'autre côté de la transmission qui est réalisé comme poste central, et qui est uniquement accessible côté central, un analyseur (8), et dans lequel, dans un premier stade du procédé, le numéro de l'abonné est transmis du côté de la transmission comprenant le générateur (4), à l'autre côté de la transmission, dans lequel le code d'abonné est déterminé et le récepteur est réglé en fonction du code, et dans lequel ensuite, et dans un second stade du procédé, dans le terminal comportant le générateur (4), la voie de transmission est établie pour la transmission du signal utile chiffré à la partie émission, caractérisé par une structure hiérarchique d'un type tel que dans les réseaux, plusieurs terminaux sont chaque fois reliés à un central, et la signalisation codée du terminal à l'appareil central a lieu suivant un processus non compatible à un système, et de plus par le fait que dans le premier stade du procédé, le code réglé est transmis du côté de la transmission contenant le générateur (4), à l'autre côté de la transmission réalisé comme poste central.

2. Procédé selon la revendication 1, caractérisé en ce que le code transmis constitue un indicateur dans une table de codes.

50

55

60

65

4

