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

(11) Veröffentlichungsnummer: **0 136 681**
A2

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **84111665.0**

(22) Anmeldetag: **28.09.84**

(51) Int. Cl.⁴: **H 04 K 1/00**

(30) Priorität: **30.09.83 DE 3335672**

(43) Veröffentlichungstag der Anmeldung:
10.04.85 Patentblatt 85/15

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

(71) Anmelder: **Siemens Aktiengesellschaft**
Berlin und München Wittelsbacherplatz 2
D-8000 München 2(DE)

(72) Erfinder: **Hofmann, Ludwig, Dipl.-Ing.**
Raiffeisenstrasse 64
D-8044 Lohhof(DE)

(72) Erfinder: **Stadler, Klaus**
Reismühlerstrasse 33
D-8035 Gauting(DE)

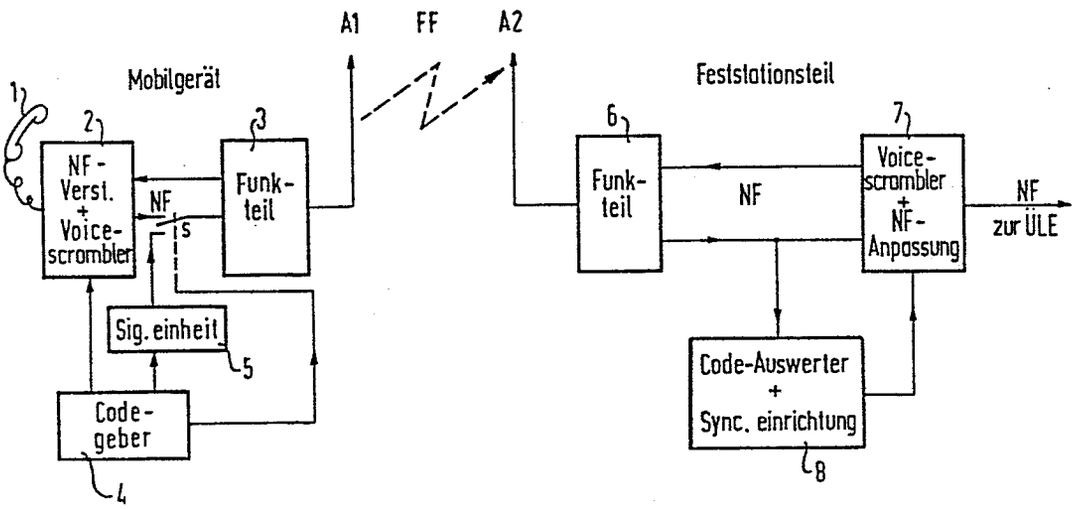
(54) Verfahren zur verschlüsselten Nachrichtenübertragung.

(57) Die Erfindung bezieht sich auf ein Verfahren zur verschlüsselten Nachrichtenübertragung in Übertragungssystemen mit fest stationierten und/oder mobilen Teilnehmergeräten (z.B. in Telefon-, Autotelefon- oder Funknetzen). Damit soll eine möglichst abhörsichere Nachrichtenübertragung erreicht werden. Die Erfindung sieht hierzu vor, daß im Endgerät der einen Übertragungsseite (Mobilgerät) ein Code-Geber (4), im Endgerät der anderen Übertragungsseite (Feststationsteil), die als Zentralstation ausgebildet und lediglich für autorisiertes Personal zugänglich ist, ein Code-Auswerter (8) angeordnet ist. Dabei wird in einem ersten Verfahrensschritt vom Code-Geber (4) der mittels eines Zufallsgenerators ausgewählte Code zum Endgerät der anderen Übertragungsseite übertragen und nach Auswertung und Einstellung von dessen Empfänger von dem den Code-Geber enthaltenden Endgerät das verschlüsselte Nutzsignal übertragen.

EP 0 136 681 A2

./...

Croydon Printing Company Ltd


A1
FF
A2
Mobilgerät
Feststationsteil
1
2
NF-
Versi.
+
Voice-
scrombler
NF
S
3
Funk-
teil
Sig. einheit
5
Code-
geber
4
6
Funk-
teil
NF
7
Voice-
scrombler
+
NF-
Anpassung
NF
zur ÜLE
Code-Auswerter
+
Sync. einrichtung
8

SIEMENS AKTIENGESELLSCHAFT
Berlin und München

Unser Zeichen
VPA 83 P 1811 E

Verfahren zur verschlüsselten Nachrichtenübertragung

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.

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/Empfangsgerätes 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.

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

Diese Aufgabe wird gemäß der Erfindung in der Weise gelöst, daß im Endgerät der einen Übertragungsseite ein Code-Geber und im Endgerät der anderen, als Zentralstation ausgebildeten, lediglich amtsseitig zugänglichen Übertragungsseite ein Code-Auswerter angeordnet ist und daß in einem ersten Verfahrensschritt von der den Code-Geber enthaltenden Übertragungsseite der eingestellte Code an die andere Übertragungsseite übertragen, in dieser ausgewertet und deren Empfänger entsprechend dem Code eingestellt wird und daß danach in einem zweiten Verfahrensschritt im den Code-Geber enthaltenden Endgerät der Übertragungsweg zur Übertragung des verschlüsselten Nutzsignals durchgeschaltet wird.

Vorteilhafte Ausgestaltungen und Weiterbildungen des erfindungsgemäßen Verfahrens, insbesondere für ein mobiles Funksystem, bei dem der Code-Geber in der mobilen Station und der Code-Auswerter in den stationären Einrichtungen angeordnet ist, sind in den Unteransprüchen angegeben.

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 ausgangs-

seitig 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 Fernsprechnetz 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 dynami-

scher 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. D.h. in den betreffenden Netzen sind*) 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

*) auf der Feststationsseite

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.

9 Patentansprüche
1 Figur

Patentansprüche

1. Verfahren zur verschlüsselten Nachrichtenübertragung in Übertragungssystemen mit fest stationierten und/oder mobilen Teilnehmergeräten (Endgeräten), beispielsweise in Telefon-, Autotelefon- oder Funknetzen, dadurch gekennzeichnet, daß im Endgerät der einen Übertragungsseite ein Code-Geber und im Endgerät der anderen, als Zentralstation ausgebildeten, lediglich amtsseitig zugänglichen Übertragungsseite ein Code-Auswerter angeordnet ist und daß in einem ersten Verfahrensschritt von der den Code-Geber enthaltenden Übertragungsseite der eingestellte Code an die andere Übertragungsseite übertragen, in dieser ausgewertet und der Empfänger entsprechend dem Code eingestellt wird und daß danach in einem zweiten Verfahrensschritt im den Code-Geber enthaltenden Endgerät der Übertragungsweg zur Übertragung des verschlüsselten Nutzsignals auf den Sendeteil durchgeschaltet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Code-Auswahl mittels eines Zufalls-Generators erfolgt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß vom Code-Geber Synchronisierimpulse auf die Übertragungsleitung zur empfangenden Endstelle gegeben werden.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß bei einem mobilen Funksystem der Code-Geber für den Verschleierungsmodus in der mobilen Station und der Code-Auswerter in den stationären, als Zentralstation

ausgebildeten, lediglich amtsseitig zugänglichen Einrichtungen angeordnet ist.

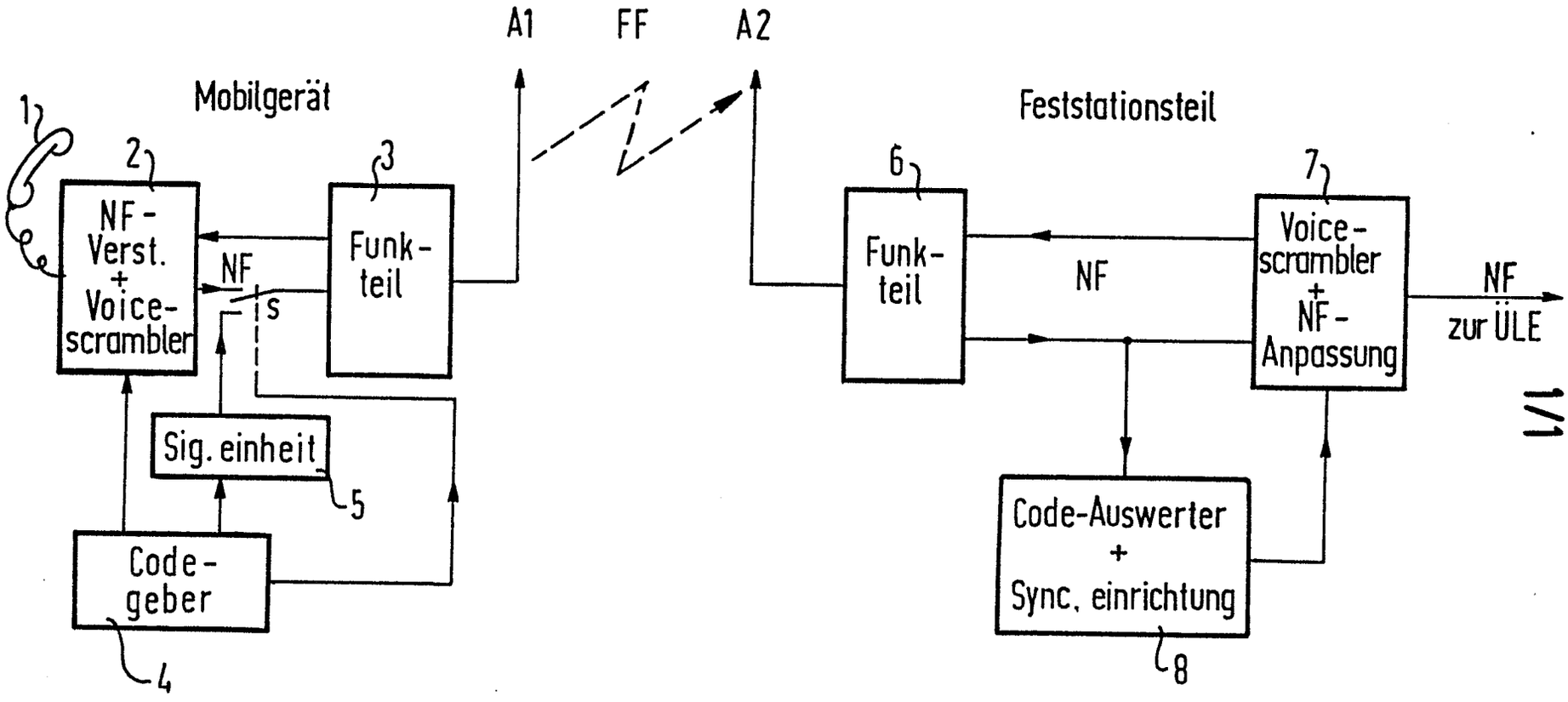
5. Verfahren nach Anspruch 4,
d a d u r c h g e k e n n z e i c h n e t ,
daß der Code-Auswerter in einem die Gegenstation für den Funkverkehr mit der mobilen Station bildenden Funkkonzentrator, in einer dieser nachgeschalteten Überleiteinrichtung als Verbindungsteil mit dem Fernsprechnetz oder in einem Vermittlungsamt angeordnet ist.

6. Verfahren nach einem der vorhergehenden Ansprüche,
g e k e n n z e i c h n e t d u r c h
eine hierarchische Struktur derart, daß in den Netzen jeweils mehrere Endgeräte mit einer Zentrale verbunden sind.

7. Verfahren nach Anspruch 6,
d a d u r c h g e k e n n z e i c h n e t ,
daß die Codesignalisierung vom Endgerät zum Zentralgerät in einem nicht systemkompatiblen Ablauf erfolgt.

8. Verfahren nach Anspruch 4,
d a d u r c h g e k e n n z e i c h n e t ,
daß der Code-Auswerter beim B-Teilnehmer angeordnet ist.

9. Verfahren nach einem der vorhergehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t ,
daß der übertragene Code einen Zeiger in einer Codetabelle bildet.


A1
FF
A2
Mobilgerät
Feststationsteil
1
2
NF-
Verst.
+
Voice-
scrambler
NF
S
3
Funk-
teil
Sig. einheit
5
Code-
geber
4
6
Funk-
teil
NF
7
Voice-
scrambler
+
NF-
Anpassung
NF
zur ÜLE
Code-Auswerter
+
Sync. einrichtung
8

1/1

0136681