CH 625 650 A5

(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
BUNDESAMT FÜR GEISTIGES EIGENTUM

(51) Int. Cl.³: H 04 B 7/26
H 04 L 9/02
H 04 K 1/00

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT A5

(11) 625 650

(21) Gesuchsnummer: 14811/77

(22) Anmeldungsdatum: 05.12.1977

(30) Priorität(en): 30.12.1976 DE 2659622

(24) Patent erteilt: 30.09.1981

(45) Patentschrift veröffentlicht: 30.09.1981

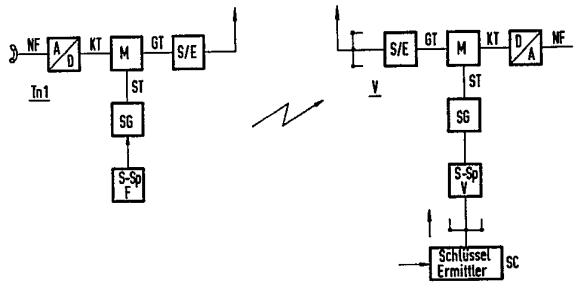
(73) Inhaber:
Siemens Aktiengesellschaft, Berlin und München, München 2 (DE)

(72) Erfinder:
Josef Brusch, Unterhaching (DE)

(74) Vertreter:
Siemens-Albis Aktiengesellschaft, Zürich

(54) Funktelefonieverfahren.

(57) Bei diesem Funktelefonieverfahren für eine Vielzahl von Teilnehmern (Tn 1) werden die Nachrichten durch ein Verschlüsselungs- oder Verschleierungsgerät (SG,M) insbesondere mittels digitaler Signale, mit bestimmtem teilnehmerindividuellen Schlüssel übertragen. Hierzu ist neben der bestimmten individuellen Schlüsseleinstellung bei jedem Teilnehmer die Teilnehmernummer selbst oder zusätzlich ein spezielles Codezeichen gespeichert. Zwischen der Teilnehmernummer bzw. dem Codezeichen und der individuellen Schlüsseleinstellung besteht ein funktioneller, nur der übergeordneten Vermittlungsstelle bekannter Zusammenhang, wobei dieser individuelle Schlüssel in der Vermittlungsstelle errechnet, damit das Verschlüsselungs- bzw. Verschleierungsgerät (SG,M) programmiert und dann die verschlüsselte Übertragung zur Vermittlungsstelle (V) und von dort aus, gegebenenfalls nach Umsetzung in den Schlüssel des Gesprächspartners, die Übermittlung der Nachrichten durchgeführt wird.



PATENTANSPRÜCHE

1. Funktelefonieverfahren für eine Vielzahl von Teilnehmern, bei dem die Nachrichten durch ein Verschlüsselungs- oder Verschleierungsgerät mit bestimmtem teilnehmerindividuellen Schlüssel, übertragen werden, dadurch gekennzeichnet, dass neben der bestimmten individuellen Schlüsseleinstellung bei jedem Teilnehmer die Teilnehmernummer selbst oder zusätzlich ein spezielles Codezeichen gespeichert ist und dass zwischen der Teilnehmernummer bzw. dem Codezeichen und der individuellen Schlüsseleinstellung ein funktioneller, nur der übergeordneten Vermittlungsstelle bekannter Zusammenhang besteht, dass ferner dieser individuelle Schlüssel in der Vermittlungsstelle errechnet wird und das Verschlüsselungs- bzw. Verschleierungsgerät programmiert wird und dann die verschlüsselte Übertragung zur Vermittlungsstelle und von dort aus die Übermittlung der Nachrichten durchgeführt wird.

2. Funktelefonieverfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Schlüsseleinstellung in der Vermittlungsstelle von einem Rechner vor Beginn jeder Nachrichtenübertragung gesondert ermittelt wird und nach Gesprächsende wieder gelöscht wird.

3. Funktelefonieverfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Übertragung der Teilnehmernummer bzw. des Codezeichens vor jedem Gesprächsbeginn redundant erfolgt.

Die Erfindung bezieht sich auf ein Funktelefonieverfahren für eine grössere Zahl von Teilnehmern, bei dem die Nachrichten durch ein Verschlüsselungs- oder Verschleierungsgerät mit bestimmtem teilnehmerindividuellen Schlüssel, übertragen werden.

Bei solchen Funktelefoniesystemen, bei denen hauptsächlich mobile Stationen im Einsatz sind, zum Beispiel beim öffentlichen beweglichen Landfunk (ÖbL) oder nicht öffentlichen beweglichen Landfunk (NÖbL) soll auf irgendeine Weise eine Nachrichtensicherung gegen Mithören erreicht werden, das heisst die Signale, die auf dem Funkweg übertragen werden, sollen in geeigneter Weise verschlüsselt oder verschleiert werden. Die miteinander korrespondierenden Stellen haben dazu meist einen oder mehrere identische Schlüssel, die als Einstellungsvariante am Gerät angebracht sind und auf denen nach Absprache die Nachrichtenübertragung durchgeführt werden kann. Für militärische und sonstige Sondernetze ist es bekannt, wie solche Schlüssel verteilt und gespeichert werden, zum Beispiel mittels elektronischer Bauelemente oder beispielsweise auch Lochkarten. Bei Teilnehmern an einem öffentlichen Funknetz, zum Beispiel beim erwähnten Landfunk, scheitern solche Verfahren daran, dass wegen der grossen Anzahl von Teilnehmern auch in einem relativ begrenzten Funkbereich einer Überleitstelle entweder eine gegen Abhören gesicherte Übertragung nicht möglich ist oder bei individueller Einstellung der Schlüssel der Überleitstelle sämtliche Schlüsseleinstellungen der Teilnehmer (persönliche Schlüssel), und zwar auch denjenigen, die an allen übrigen Überleitstellen im gesamten Netz tätig sind, bekannt sein müssten und damit auch gespeichert werden müssten. Da normalerweise in einem Netz mit mehreren Funküberleitstellen, die örtlich verteilt sind, viele tausend Teilnehmer vermittelt werden müssen, würde bei Bekanntsein der Schlüsseleinstellung nicht nur ein Abhören möglich, sondern auch der Ruf unter einer falschen Nummer, was zu Gebührenfehlverrechnungen führt.

Der Erfindung liegt die Aufgabe zugrunde, die aufgezeigte Problematik einer möglichst einfachen Lösung zuzuführen, die die Nachteile der oben geschilderten Art vermeidet.

Diese Aufgabe wird bei einem Funktelefonieverfahren für eine Vielzahl von Teilnehmern, bei dem die Nachrichten durch ein Verschlüsselungs- oder Verschleierungsgerät mit bestimmtem teilnehmerindividuellen Schlüssel, übertragen werden, gemäss der Erfindung dadurch gelöst, dass neben der bestimmten individuellen Schlüsseleinstellung bei jedem Teilnehmer die Teilnehmernummer selbst oder zusätzlich ein spezielles Codezeichen gespeichert ist und dass zwischen der Teilnehmernummer bzw. dem Codezeichen und der individuellen Schlüsseleinstellung ein funktioneller, nur der übergeordneten Vermittlungsstelle bekannter Zusammenhang besteht, dass ferner dieser individuelle Schlüssel in der Vermittlungsstelle errechnet wird und das Verschlüsselungs- bzw. Verschleierungsrät programmiert wird und dann die verschlüsselte Übertragung zur Vermittlungsstelle und von dort aus die Übermittlung der Nachrichten durchgeführt wird.

Es ist dabei vorteilhaft, wenn die Schlüsseleinstellung in der Vermittlungsstelle von einem Rechner vor Beginn jeder Nachrichtenübertragung gesondert ermittelt wird und nach Gesprächsende gelöscht wird.

Ferner ist es zur Sicherung der Vermittlungsdaten vorteilhaft, wenn die Übertragung der Teilnehmernummer bzw. des Codezeichens vor jedem Gesprächsbeginn redundant erfolgt.

Nachfolgend wird die Erfindung anhand zweier Figuren beispielsweise näher erläutert.

Die Figur 1 zeigt einen Teilnehmer Tn1, dessen NF in einen digitalen Klartext KT umgewandelt wird (A/D) und dann in einem Mischer M mit dem Schlüsseltext ST – von einem Schlüsselgenerator SG gesteuert – einer Verschlüsselung zu dem Geheimtext GT unterworfen wird. Dieser Geheimtext wird dann von einer Sende-Empfangseinrichtung S/E übertragen. Auf der Empfangsseite findet der umgekehrte Vorgang statt. Zur Verbindungsaufnahme soll die Verschlüsselungseinrichtung SG + M zunächst abgeschaltet sein. Irgendwann wird der Teilnehmer Tn1 mit seiner ihm örtlich zugeteilten Funküberleitstelle, das heisst Funkvermittlungsstelle V, Verbindung aufnehmen. Die Funküberleitstelle befragt ihn nach seiner Teilnehmernummer und gegebenenfalls nach seinem Verbindungswunsch. Schon zu diesem Zeitpunkt könnte jetzt beim Rückruf zur Sicherstellung, ob sich der Teilnehmer unter seiner richtigen Rufnummer gemeldet hat, die Verschlüsselungseinrichtung in Tätigkeit treten.

Die Verschlüsselung selbst beruht auf folgendem Grundgedanken. Normalerweise müssten bei der Vermittlungsstelle sämtliche Schlüssel aller Teilnehmer bekannt sein. Da jedoch in einem grösseren Netz mit mehreren Vermittlungsstationen und unter Umständen sehr vielen Teilnehmern bei jeder Vermittlungsstation alle solche Schlüssel gespeichert sein müssten und damit ein hoher technischer und organisatorischer Aufwand verbunden wäre, wird bei der Erfindung folgender Weg beschritten. Zwischen der Teilnehmernummer oder einem jedem Teilnehmer separat zugeordneten Code besteht ein funktioneller Zusammenhang nach irgendeiner mathematischen Funktion, die jedoch nur in einem Schlüsselermittler SC bei der Vermittlungsstation bekannt ist. Diesem Schlüsselermittler wird die Teilnehmernummer mitgeteilt und aufgrund dessen kann der Schlüsselermittler mittels einer Recheneinrichtung in sehr kurzer Zeit den individuellen Teilnehmerschlüssel des rufenden Teilnehmers ermitteln und in einer Einrichtung S-Sp/V für die Verbindungsdauer speichern. Die Vermittlungsstation ruft nun bereits verschlüsselt an die Teilnehmer zurück und wenn sich nun der Teilnehmer Tn1 richtig gemeldet hat, dann muss auch nach Einschalten seines Schlüsselgenerators SG, der von seinem Schlüsselspeicher S-Sp/F den Schlüssel erhält, die Verständlichkeit sämtlicher weiterer Nachrichtenübertragungen zwischen dem Teilnehmer und der Funküberleitstelle V gesichert sein. Im anderen Falle wird der Teilnehmer keinen Rückruf erhalten, da er den Ruf der Vermittlungsstation V wegen eines anderen Schlüssels nicht versteht und dadurch wird die Nachrichtenübertragung über eine falsche Rufnummer, also mit falscher Gebührenzählung unmöglich gemacht. Der Teilnehmer kann diesen Zustand auch

nicht durch Manipulationen an seinem Schlüsselgenerator bzw. Speicher künstlich herbeiführen, da nämlich der funktionelle Zusammenhang zwischen seiner Teilnehmernummer, seinem speziellen Wahl- und Rufcode und dem Schlüssel für die Verschlüsselungseinrichtung unbekannt ist. Diese Zuordnung ist nur den Funküberleitstellen V bekannt und dort in einem speziellen Rechner gespeichert.

Bei einem Verbindungswunsch des Teilnehmers Tn1, zum Beispiel nach Teilnehmer Tn3, wird nun die Vermittlungsstelle den Teilnehmer Tn3 (siehe Figur 2) zu ermitteln suchen, falls er sich in seinem örtlichen Netz überhaupt aufhält oder erreichbar ist, und nun beginnt auch auf der Seite des angerufenen Teilnehmers dasselbe Spiel mit dem für den Teilnehmer Tn3 zugeordneten Schlüssel. In der Schlüsselcodiereinrichtung SC der Vermittlungsstation wird spätestens zum Zeitpunkt der echten Nachrichtenübertragung zwischen Teilnehmer Tn1 und Tn3 eine Umcodierung der Schlüssel vorgenommen, das heisst die empfangenen Nachrichten der beiden Teilnehmer werden entschlüsselt und auf dieser Ebene (Klartext) durchverbunden. Es ist auf diese Weise möglich, eine gesicherte Nachrichtenübertragung zu gewährleisten, da ja die individuellen Schlüssel jeweils nur dem zugehörigen Teilnehmer bekannt sind.

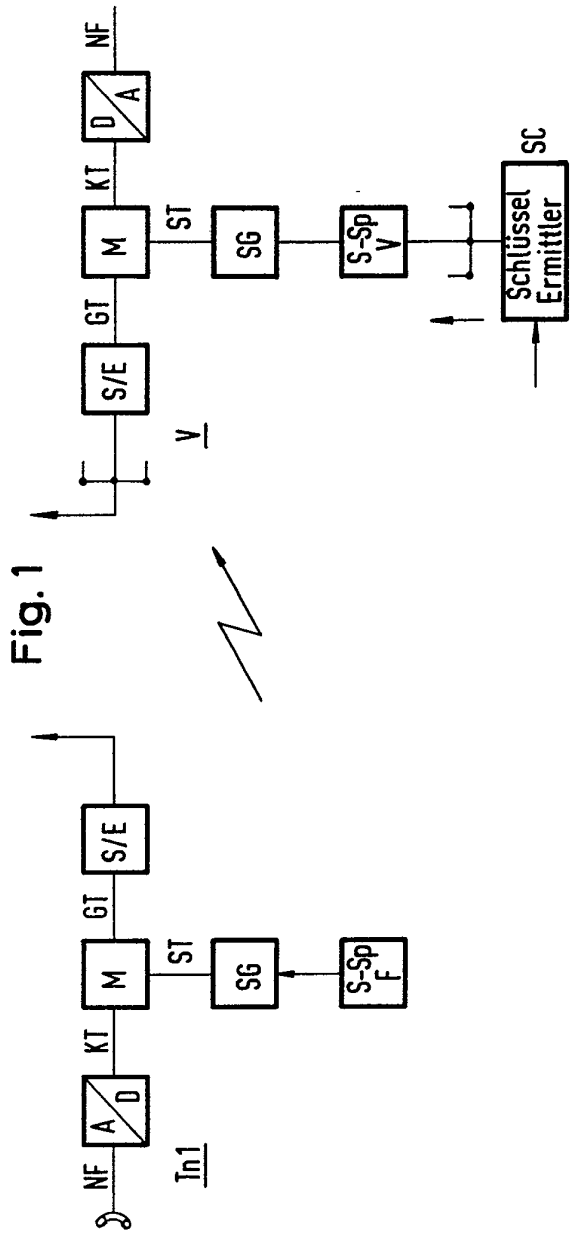

NF
D/A
KT
M
ST
SG
S-Sp V
SC
Schlüssel Ermittler
GT
S/E
V
S/E
GT
M
ST
SG
S-Sp F
KT
A/D
NF
Tn1

Fig. 1

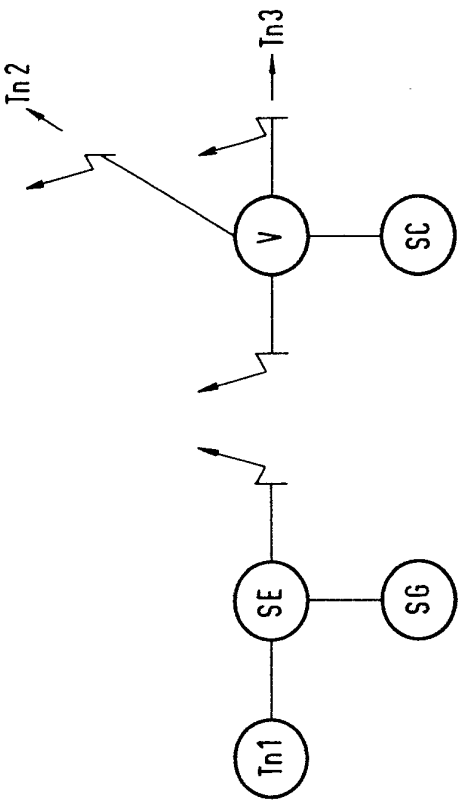

Tn2
Tn3
V
SC
SE
SG
Tn1

Fig. 2