(19) DANMARK

DIREKTORATET FOR
PATENT- OG VAREMÆRKEVÆSENET

(12) **FREMLÆGGELSESSKRIFT** (11) **148049 B**

(21) Patentansøgning nr.: **5852/77**

(22) Indleveringsdag: **29 dec 1977**

(41) Alm. tilgængelig: **01 jul 1978**

(44) Fremlagt: **11 feb 1985**

(86) International ansøgning nr.: –

(30) Prioritet: **30 dec 1976 DE 2659622**

(51) Int.Cl.[4]: **H 04 Q 7/04**
H 04 K 1/00
H 04 B 7/26

(71) Ansøger: ***SIEMENS AKTIENGESELLSCHAFT; Berlin und Muenchen, 8 Muenchen 2, DE.**

(72) Opfinder: **Josef *Brusch; DE.**

(74) Fuldmægtig: **Internationalt Patent-Bureau**

(54) **Radiotelefonisystem**

DK 148049 B

Opfindelsen angår et radiotelefonisystem for et større antal abonnenter, ved hvilket information overføres ved hjælp af et chiffrerings- eller sløringsapparat navnlig ved hjælp af digitale signaler eksempelvis med en bestemt for hver abonnent individuel rækkefølge, dvs. med en bestemt for hver abonnent individuel chiffrering.

I forbindelse med sådanne radiotelefonisystemer, hvor der i hovedsagen benyttes mobile stationer, f.eks. offentlige eller ikke-offentlige radioforbindelser mellem bevægelige landstationer (ÖbL eller NÖbL), skal man på en eller anden måde sikre informationen mod uvedkommende medhør, hvilket vil sige, at de signaler, som transmitteres igennem den pågældende radiokanal, skal chiffreres eller sløres på hensigtsmæssig måde. Hertil har de indbyrdes korresponderende stationer for det meste én eller flere identiske koder, der som indstillingsvarianter er tilvejebragt i det pågældende udstyr, og i hvilke koder informationsoverføringen kan gennemføres efter aftale. Til militære og andre særlige net er det kendt, hvordan sådanne koder fordeles og oplagres, f.eks. ved hjælp af elektroniske komponenter eller f.eks. også ved hjælp af hulkort. I forbindelse med abonnenter, der er tilsluttet et offentligt radionet, f.eks. én af de ovennævnte radioforbindelser mellem landstationer, svigter sådanne fremgangsmåder som følge af, at på grund af det store antal abonnenter, der findes selv i en transferstations forholdsvis begrænsede radiodækningsområde, er enten en mod aflytning sikret transmission ikke mulig, eller også skulle transferstationen ved individuel indstilling af koderne være bekendt med og lagre samtlige abonnenternes chiffreringsindstillinger (personlig kode); også alle de, som gælder for alle andre transferstationer i det samlede net. Da der i et net med flere transferstationer, som er fordelt geografisk, normalt skal betjenes flere tusind abonnenter, ville et kendskab til chiffreringsindstillingen ikke blot gøre en

aflytning mulig, men også muliggøre et opkald under et falsk nummer, hvilket medfører fejlagtige gebyrberegninger.

Det tilsigtes med opfindelsen at tilføre den påviste problemstilling en løsning, der er så enkel som mulig, og hvorved ulemperne af ovenfor beskrevne art er undgået.

Dette opnås med et radiotelefonisystem for et større antal abonnenter, ved hvilket information overføres ved hjælp af et chiffrerings- eller sløringsapparat navnlig ved hjælp af digitale signaler eksempelvis med en bestemt for hver abonnent individuel rækkefølge, dvs. med en bestemt for hver abonnent individuel chiffrering, hvilket system ifølge opfindelsen er ejendommeligt ved, at der foruden den bestemte individuelle chiffreringsindstilling hos hver abonnent er oplagret selve abonnentnummeret eller tillige en særlig kode, og at der mellem abonnentnummeret eller koden og den individuelle chiffreringsindstilling består en funktionel sammenhæng, som kun kendes af den overordnede central (radiotransmissionsstation), at endvidere ved opbygning af en forbindelse mellem to abonnenter den kaldende abonnent først overfører sit nummer hhv. den specielle kode samt den opkaldte abonnents nummer til centralen, at denne konstaterer den opkaldte abonnent og foranlediger, at denne overfører sit nummer hhv. den specielle kode, at endvidere centralen ud fra disse modtagne informationer beregner abonnenternes individulle chiffreringsindstillinger og programmerer chiffrerings- hhv. sløringsapparatet, og at den chiffrerede overføring mellem de to abonnenter derefter gennemføres over centralen med samtidig omsætning af den sendende abonnents kode til den modtagende abonnents kode på centralen.

Det er i denne forbindelse en fordel, at den ved hjælp af en passende datamat på centralen før begyndelsen af hver informationsoverføring separat bestemte chiffreringsindstilling slettes efter samtalens afslutning.

Desuden er det til sikring af opkoblingsdataene en fordel, såfremt overføringen af abonnentnummeret eller koden sker redundant før hver samtales begyndelse.

Opfindelsen forklares nærmere nedenfor under henvisning til tegningen, hvor

fig. 1 viser sender- og modtagersiden af en radioforbindelse, og

fig. 2 skematisk princippet for informationsoverføringen mellem to abonnenter.

Fig. 1 viser en abonnent Tn1, hvis talesignal NF omsættes (A/D) til en digital klartekst KT, hvorefter det i en blander M underkastes en chiffrering med chiffreringsteksten ST - styret fra en chiffreringsgenerator SG - til dannelse af den hemmelige tekst GT. Denne hemmelige tekst transmitteres herefter fra en sende/modtageindretning S/E. På modtagesiden foregår den omvendte proces. Til optagelse af forbindelsen skal chiffreringsindretningen SG+M først være koblet fra. På et tidspunkt vil abonnenten Tn1 optage forbindelse med den ham lokalt tildelte radiotransferstation, dvs. radiocentralen V. Radiotransferstationen spørger ham om hans abonnentnummer og eventuelt om, hvem han ønsker forbindelse med. Allerede på dette tidspunkt kunne chiffreringsindretningen træde i funktion for ved tilbagekald at sikre, at abonnenten har meldt sig under sit rigtige kaldenummer.

Selve chiffreringen beror på følgende grundtanke. Normalt skal samtlige koder for alle abonnenter være kendt af centralen. Da imidlertid i et større net med flere centraler og eventuelt med adskillige abonnenter under hver central alle sådanne koder skal være lagret, hvilket ville være forbundet med et stort teknisk og organisatorisk opbud, går man imidlertid ifølge opfindelsen frem på følgende måde. Mellem abonnentnummeret eller en hver abonnnent særskilt tildelt kode og den individuelle chiffreringsindstilling består der en funktionel sammenhæng svarende til en eller anden matema-

tisk funktion, der dog kun kendes af en kodeberegner SC på centralen. Denne kodeberegner meddeles abonnentnummeret, på grundlag af hvilket den ved hjælp af en regneenhed på meget kort tid bestemmer den individuelle abonnentkode for den kaldende abonnent og oplagrer denne i en indretning S-Sp/V så længe forbindelsen er etableret. Centralen kalder nu, allerede chiffreret, tilbage til abonnenten, og hvis nu denne abonnent Tnl har meldt sig korrekt, så må forståeligheden af samtlige herpå følgende informationsoverførsler mellem abonnenten og radiotransferstationen V være sikret også efter indkobling af abonnentens chiffreringsgenerator SG, der fra abonnentens kodelager S-Sp/F modtager koden. I andre tilfælde vil abonnenten ikke modtage noget tilbagekald, da han på grund af en anden kode ikke forstår opkaldet fra centralen V, og herigennem bliver informationsoverførslen over et forkert opkaldsnummer, som indebærer en forkert gebyrberegning, gjort umulig. Abonnenten kan heller ikke fremkalde denne tilstand kunstigt ved manipulationer i sin egen kodegenerator eller sit eget kodelager, fordi den funktionelle sammenhæng mellem hans abonnentnummer, hans specielle vælge- og opkaldskode og koden til chiffreringsindretningen nemlig er ukendt for ham. Denne allokering kendes kun af radiotransferstationen V, hvor den er lagret i en særlig regneenhed.

Når abonnenten Tnl ønsker at etablere forbindelse, f.eks. med abonnent Tn3, vil centralen nu søge abonnenten Tn3, jf. fig. 2, såfremt denne befinder sig i eller kan nås i sit lokale net, og nu iværksættes på den opkaldte abonnents side den samme procedure med den kode, som den pågældende abonnent Tn3 har fået tildelt. I centralens chiffreringsindretning SC foretages der senest til det tidspunkt, hvor der foregår en ægte informationsoverførsel imellem abonnent Tnl og abonnent Tn3, en omkodning af koderne, hvilket vil sige, at de fra begge abonnenter modtagne informationer bliver de-

chiffreret og koblet igennem på dette plan (klartext). På denne måde er det muligt at opnå en sikret informationsoverførsel, da den individuelle kode i hvert enkelt tilfælde kun kendes af den pågældende abonnent.

P A T E N T K R A V

1. Radiotelefonisystem for et større antal abonnenter, ved hvilket information overføres ved hjælp af et chiffrerings- eller sløringsapparat navnlig ved hjælp af digitale signaler eksempelvis med en bestemt for hver abonnent individuel rækkefølge, dvs. med en bestemt for hver abonnent individuel chiffrering, k e n d e t e g n e t ved, at der foruden den bestemte individuelle chiffreringsindstilling hos hver abonnent er oplagret selve abonnentnummeret eller tillige en særlig kode, og at der mellem abonnentnummeret eller koden og den individuelle chiffreringsindstilling består en funktionel sammenhæng, som kun kendes af den overordnede central (radiotransmissionsstation), at endvidere ved opbygning af en forbindelse mellem to abonnenter den kaldende abonnent først overfører sit nummer henholdsvis den specielle kode samt den opkaldte abonnents nummer til centralen, at denne konstaterer den opkaldte abonnent og foranlediger, af denne overfører sit nummer henholdsvis den specielle kode, at endvidere centralen ud fra disse modtagne informationer beregner abonnenternes individuelle chiffreringsindstillinger og programmerer chiffrerings- henholdsvis sløringsapparatet, og at den chiffrerede overføring mellem de to abonnenter derefter gennemføres over centralen med samtidig omsætning af den sendende abonnents kode til den modtagende abonnents kode på centralen.

2. Radiotelefonisystem ifølge krav 1, k e n d e t e g n e t ved, at den ved hjælp af en passende datamat på centralen før begyndelsen af hver informationsoverføring separat bestemte chiffreringsindstilling slettes efter samtalens afslutning.

3. Radiotelefonisystem ifølge krav 1 eller 2, k e n d e t e g n e t ved, at overføringen af abonnentnummeret eller koden sker redundant før hver samtales begyndelse.

Fremdragne publikationer:

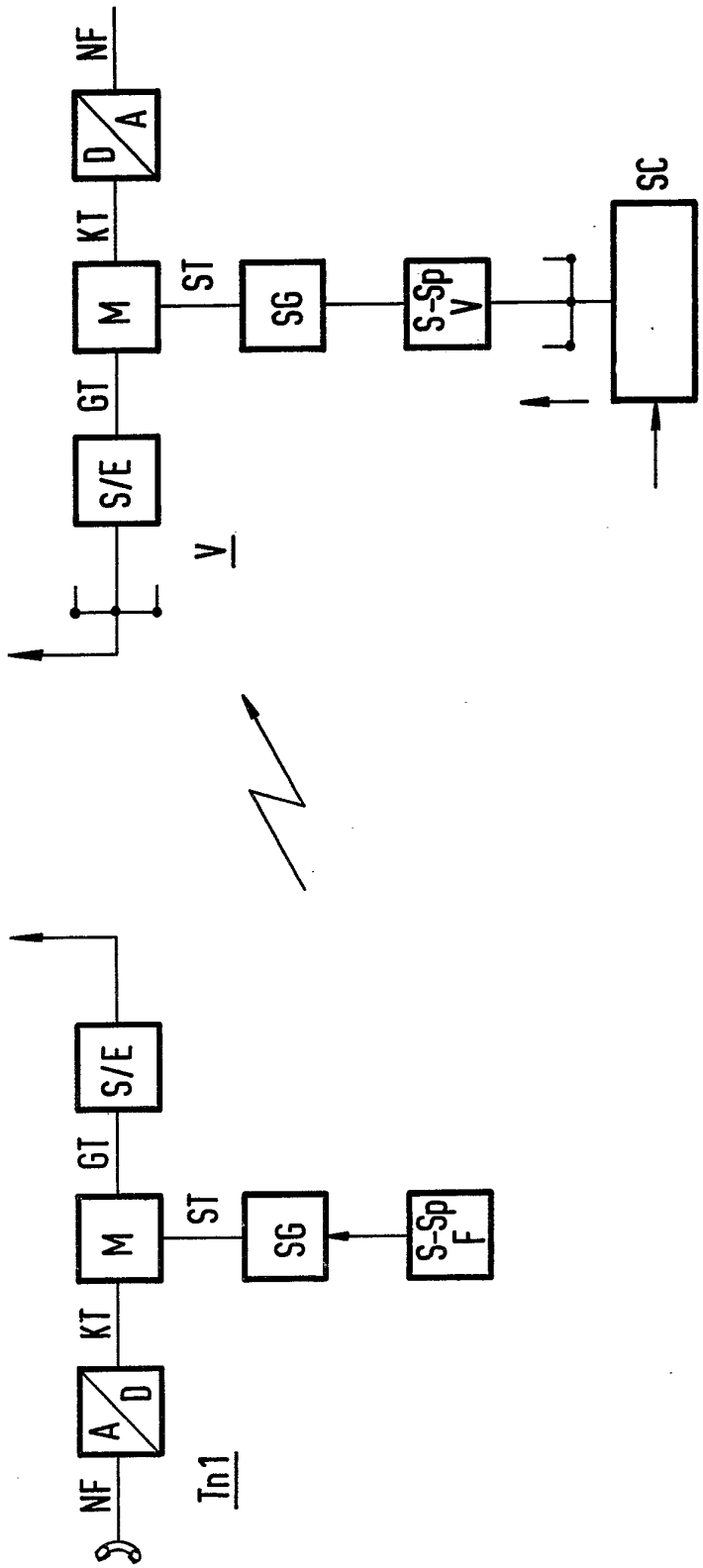

Fig. 1

Fig. 2