NORGE

(12) **PATENT**

(19) NO (11) **305530** (13) B1

(51) Int Cl^6 H 04 L 9/08, 9/32

Patentstyret

(21) Søknadsnr	19924077	(86) Int. inng. dag og søknadsnummer	
(22) Inng. dag	21.10.1992		
(24) Løpedag	21.10.1992	(85) Videreføringsdag	
(41) Alm. tilgj.	26.04.1993	(30) Prioritet	25.10.1991, NL, 9101796
(45) Meddelt dato	14.06.1999		

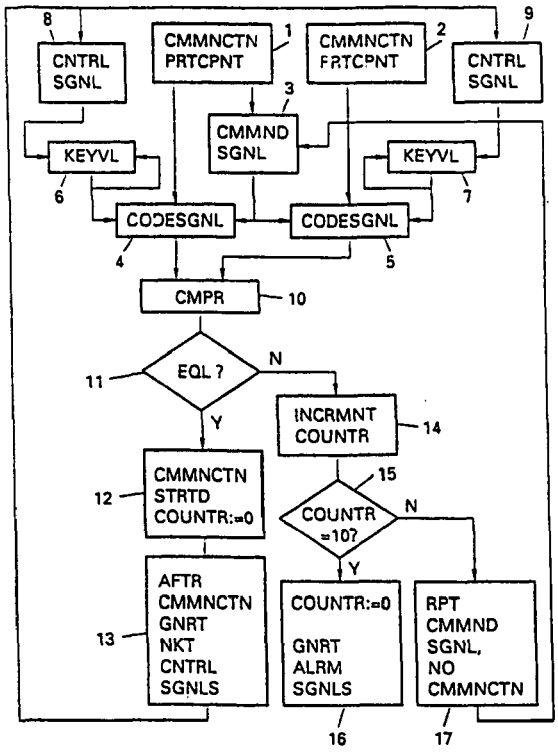
(73) Patenthaver Koninklijke KPN NV, Postbus 95321, NL-2509 CH Haag, NL
(72) Oppfinner Klaas Pieter Vlieg, Groningen, NL
Jurgen Jacob Spaanderman, Sliedrecht, NL
Maria Leo Wenas, Delft, NL
(74) Fullmektig Oslo Patentkontor AS, 0306 Oslo

(54) Benevnelse **Fremgangsmåte ved autentifisering av kommunikasjonsdeltakere, samt system og deltakere som utnytter fremgangsmåten**

(56) Anførte publikasjoner Ingen

(57) Sammendrag

Kjente fremgangsmåter for autentisering av kommunikasjonsdeltakere, legger et kodeord til et kommandosignal, hvilket kodeord er et kryptografisk funksjon av kommandosignalet og en nøkkelverdi som i sin tur er en funksjon av en hovednøkkel og et forandringskodeord. Hovednøkkelverdien har en permanent fast verdi, i motsetning til forandrings-kodeordet som tjener til å forandre nøkkelverdien. Fremgangsmåten ifølge oppfinnelsen gjør bruk av en nøkkelverdi som er en funksjon av minst én tidligere nøkkelverdi, hvorved hovednøkkelverdien med permanent fast verdi, som straks den blir oppdaget eller har lekket ut svekker i vesentlig grad kryptograferingen, ikke lenger er nødvendig.


8
9
CNTRL SGNL
CMMNCTN PRTCPNT
1
CMMNCTN PRTCPNT
2
CNTRL SGNL
3
CMMND SGNL
KEYVL
KEYVL
6
7
CODESGNL
CODESGNL
4
5
CMPR
10
EQL ?
11
N
Y
INCRMNT COUNTR
14
CMMNCTN STRTD COUNTR:=0
12
15
COUNTR =10?
N
Y
AFTR CMMNCTN GNRT NKT CNTRL SGNLS
13
COUNTR:=0
GNRT ALRM SGNLS
16
RPT CMMND SGNL, NO CMMNCTN
17

A. Oppfinnelsens bakgrunn

Oppfinnelsen vedrører en fremgangsmåte av den art som er angitt i den innledende del av det vedføyde patentkrav 1.

En fremgangsmåte av denne type er omtalt i US 4.688.250. Den beskriver hvordan en bakkestasjon (den første kommunikasjonsdeltaker) og en satellitt (den andre kommunikasjonsdeltaker, også kalt sekundær kommunikasjonsdeltaker) kommuniserer med hverandre, idet satellitten kun tillates å utføre kommandoer som kommer fra denne ene bakkestasjon og ikke tillates å reagere på kommandoer som kommer fra andre (fiendlige) bakkestasjoner. For dette formål sender bakkestasjonen, sammen med en del kommandodata (kommandosignalet), et kodeord (det første kodesignal) som er en kryptografisk funksjon av kommandodataene, og en hemmelig nøkkel (den første nøkkelverdi) som er lagret i bakkestasjonen. På basis av de samme kommunikasjonsdata og en hemmelig nøkkel (den andre nøkkelverdi) som er lagret i satellitten, genererer satellitten deretter et kodeord (det andre kodesignal), og sammenligner dette med kodeordet som ble sendt fra bakkestasjonen. De to kodeordene vil være like dersom og bare dersom de to hemmelige nøklene er identiske. I tilfelle av identiske kodeord, er bakkestasjonen blitt tilstrekkelig autentisert, og kommandoen blir utført av satellitten. I alle andre tilfeller blir kommandoen ignorert.

Dette krever at de hemmelige nøkler blir forandret fra tid til annen. I den ovenfor nevnte US patentbeskrivelse er dette implementert ved at bakkestasjonen sender en nøkkelforandringskode (det første og andre styresignal), og som svar på dette genererer både bakkestasjonen og satellitten nye hemmelige koder (den påfølgende første nøkkelverdi og den påfølgende andre nøkkelverdi) som er en funksjon av et forandringskodeord og en hovednøkkel som begge er lagret i bakkestasjonen så vel som i satellitten. Dessuten blir dette forandringskodeordet regelmessig forandret.

Denne kjente fremgangsmåte har den ulempe at de nye hemmelige nøkler som skal genereres, er en funksjon av hovednøkkelen som er lagret i bakkestasjonen så vel som i satellitten, og som har en fast verdi gjennom hele satellitt-toktet. Så snart hovednøkkelens verdi er blitt kjent for utenforstående, blir det mye enklere for dem å finne de nye hemmelige kodene som skal genereres i løpet av resten av satellitt-toktet. Videre har denne fremgangsmåte, når den benyttes i større systemer med betydelig flere sekundære kommunikasjonsdeltakere (slik som ISDN nettverk med mange NTer, og smartkortsystemer), den ulempe at hver sekundær kommunikasjonsdeltaker må ha sin egen unike hovednøkkel, og fremgangsmåten, når den benyttes i mange tett nærliggende systemer (idet hvert system omfatter en første og an andre kommunikasjonsdeltaker, f.eks. trådløse telefonsystemer), har den ulempe at hvert system skulle ha sin egen unike hovednøkkel, hvlket stiller ytterligere krav til produksjonsprosessen.

B. Sammefatning av oppfinnelsen

Hensikten med oppfinnelsen er blant annet å fremskaffe en fremgangsmåte hvor den ovenfor nevnte ulempe med hovednøkkelen med en fast verdi, ikke lenger forekommer, hvor, i tilfelle av benyttelse i et stort system med flere [sic] sekundære kommunikasjonsdeltakere, alle sekundære kommunikasjonsdeltakere i prinsippet er identiske, og hvor, i tilfelle av benyttelse i tett nærliggende systemer, alle systemer i prinsippet er identiske, slik at man ikke behøver å stille ytterligere krav til produksjonsprosessen.

I denne sammenheng er en fremgangsmåte av den innledningsvis angitt art, ifølge oppfinnelsen karakterisert ved de trekk som fremgår av den karakteriserende del av det vedføyde patentkrav 1.

Oppfinnelsen er basert på den innsikt at ved at man lar vedkommende (første eller andre) kommunikasjonsdeltaker

genererer den påfølgende (første eller andre) nøkkelverdi som svar på (første eller andre) styresignal, oppnås det resultat at den påfølgende nøkkelverdi ikke lenger blir bestemt på basis av en hovednøkkel med en fast verdi, at alle i prinsippet identiske sekundære kommunikasjonsdeltakere hver kan gjøres unike ved å variere antall styresignaler pr. sekundær kommunikasjonsdeltaker umiddelbart etter installasjon av nevnte deltaker, idet hver sekundær kommunikasjonsdeltaker blir forsynt med et forskjellig antall tider med en påfølgende nøkkelverdi og således blir gjort unik med hensyn til de andre sekundære kommunikasjonsdeltakerne, og at alle de tett nærliggende systemer, som i prinsippet er identiske, hver kan gjøres unike ved å variere antall styresignaler pr. system umiddelbart etter installasjon av nevnte system, idet hvert system blir forsynt med et forskjellig antall tider med en påfølgende nøkkelverdi og således blir gjort unik med hensyn til de andre tett nærliggende systemer.

En utførelsesform for fremgangsmåten ifølge oppfinnelsen er karakterisert ved at den påfølgende første nøkkelverdi også er en funksjon av minst det første styresignal og den påfølgende andre nøkkelverdi er også en funksjon av minst det andre styresignal.

Ved generering av den påfølgende (første eller andre) nøkkelverdi også som en funksjon av (første eller andre) styresignal, oppnår man det resultat at antall mulige påfølgende nøkkelverdier blir betydelig øket, og at antall styresignaler som kreves for å gjøre kommunikasjonsdeltakerne unike etter at de er blitt installert, blir betydelig redusert. F.eks., dersom styresignalet er et vilkårlig generert nummer (som sammen med den momentane nøkkelverdi derfor bestemmer den påfølgende nøkkelverdi), kan svært mange kommunikasjonsdeltakere som i prinsippet er identiske med hverandre, gjøres nesten fullstendig unike med hensyn til hverandre, ved å generere bare ett eller noen få styresignaler.

Ytterligere vedrører oppfinnelsen et kommunikasjonsdeltakersystem, av den art som er angitt i den innledende del av det vedføyde patentkrav 3, for utnyttelse av den omtalte fremgangsmåte, og et slikt system er i henhold til oppfinnelsen karakterisert ved de trekk som er angitt i den karakteriserende del av nevnte patentkrav.

Med andre ord fremskaffes det ifølge oppfinnelsen et system for bruk av fremgangsmåten av den type som er beskrevet i innledningen, ved hvilken fremgangsmåte den ovenfor nevnte ulempe med hovednøkkelen med den faste verdi ikke lenger forekommer, og ved hvilken fremgangsmåte, i tilfelle det benyttes et stort system med flere [sic] sekundære kommunikasjonsdeltakere, alle de sekundære kommunikasjonsdeltakere i prinsippet er identiske og, i tilfelle det benyttes mange tett nærliggende systemer, alle systemene i prinsippet er identiske, slik at det ikke stilles ytterligere krav til produksjonsprosessen.

I denne sammenheng er systemet i henhold til oppfinnelsen karakterisert ved at de første nøkkelverdi-genereringsorganer er tilpasset for å generere, som en funksjon av minst en første nøkkelverdi, den påfølgende første nøkkelverdi, og de andre nøkkelverdi-genereringsorganer er tilpasset for å generere, som en funksjon av minst en andre nøkkelverdi, den påfølgende andre nøkkelverdi.

En utførelsesform for systemet ifølge oppfinnelsen er karakterisert ved at de første nøkkelverdi-genereringsorganer er tilpasset for å generere den påfølgende første nøkkelverdi også som en funksjon av det første styresignal, og de andre nøkkelverdi-genereringsorganer er tilpasset for å generere den påfølgende andr nøkkelverdi også som en funksjon av det andre styresignal.

Oppfinnelsen vedrører ytterligere en første kommunikasjonsdeltaker som angitt i den innledende del av det vedføyde patentkrav 5, samt en andre kommunikasjonsdeltaker som angitt i den innledende del av det vedføyde patentkrav

7.

Den første kommunikasjonsdeltaker er karakterisert ved at de første nøkkelverdi-genereringsorganer er tilpasset for å generere, som en funksjon av minst den første nøkkelverdi, den påfølgende første nøkkelverdi.

I en utførelsesform er den første kommunikasjonsdeltaker karakterisert ved at de første nøkkelverdi-genereringsorganer er tilpasset for å generere den påfølgende første nøkkelverdi også som en funksjon av det første styresignal.

Den andre kommunikasjonsdeltaker er karakterisert ved at de andre nøkkelverdi-genereringsorganer er tilpasset for å generere, som en funksjon av minst den andre nøkkelverdi, den påfølgende andre nøkkelverdi.

I en utførelsesform er den andre kommunikasjonsdeltaker karakterisert ved at de andre nøkkelverdi-genereringsorganer er tilpasset for å generere den påfølgende andre nøkkelverdi også som en funksjon av det andre styresignal.

I tilfelle av fremgangsmåten ifølge oppfinnelsen er det selvfølgelig også mulig å autentisere fra begge sider. Dersom systemet f.eks. omfatter to første kommunikasjonsdeltakere, kan den ene autentisere den andre og omvendt, fordi begge kommunikasjonsdeltakerne er utstyrt med kommandosignal-genereringsorganene og sammenligningsorganene.

C. Referanse

US 4.688.250

D. Eksempler på utførelsesformer

Oppfinnelsen vil bli beskrevet mer detaljert under henvis-

ning til et utførelseseksempel vist på figurene, på hvilke figurer:

figur 1 viser en skjematisk illustrasjon av fremgangsmåten ifølge oppfinnelsen, og

figur 2 viser et blokkdiagram av systemet ifølge oppfinnelsen, utstyrt med første og andre kommunikasjonsdeltaker i henhold til oppfinnelsen.

På den skjematiske illustrasjon av fremgangsmåten ifølge oppfinnelsen vist på figur 1, har boksene følgende betydning:

1	CMMNCTN PRTCPNT	første kommunikasjonsdeltaker
2	CMMNCTN PRTCPNT	andre kommunikasjonsdeltaker
3	CMMNDSGNL	generering av kommandosignalet
4	CODESGNL	generering av det første kodesignal
5	CODESGNL	generering av det andre kodesignal
6	KEYVL	generering av den første nøkkelverdi
7	KEYVL	generering av den andre nøkkelverdi
8	CNTRLSGNL	generering av det andre styresignal
9	CNTRLSGNL	generering av det andre styresignal
10	CMPR	sammenligning av kodesignaler

11	EQL?	dersom kodesignalene er identiske: utgang ja dersom kodesignalene ikke er identiske: utgang nei
12	CMMNCTN STRTD COUNTR: -0	starten av kommunikasjonen etter at likheten av de to kodesignalene er funnet i boks 11; utgangen av telleren (se boks 14) blir satt til 0
13	AFTR CMMNCTN GNRT NXT CNTRL SGNLS	generering av de neste første og andre styresignaler etter at kommunikasjonen er avsluttet, som svar på hvilket de påfølgende første og andre nøkkelverdier blir generert
14	INCRMNT COUNTR	øke telleren med 1 etter atulikheten av de to kodesignaler er blitt funnet i boks 11
15	COUNTR = 10?	dersom tellerens utgangsverdi er 10: utgang ja dersom tellerens utgangsverdi ikke er 10: utgang nei
16	COUNTR: = 0 GNRT ALRM SGNL	tellerens utgang settes til 0 generering av alarmsignalet
17	RPT CMMNDSGNL NO CMMNCTN	repetering av kommandosignalet kommunikasjon har ennå ikke funnet sted

Fremgangsmåten ifølge oppfinnelsen som er illustrert skjematisk på figur 1, finner sted som følger. Dersom den før-

ste kommunikasjonsdeltaker (boks 1) ønsker å kommunisere med den andre kommunikasjonsdeltaker (boks 2), sender den første kommunikasjonsdeltaker et kommandosignal (boks 3). Som svar på dette genererer den første kommunikasjonsdeltaker et første kodesignal (boks 4) som er en funksjon av både kommandosignalet og en første nøkkelverdi (boks 6), og den andre kommunikasjonsdeltaker genererer et andre kodesignal (boks 5) som er en funksjon av både kommandosignalet og en andre nøkkelverdi (boks 7). Deretter blir de to kodesignaler gjensidig sammenlignet (boks 10, lik ja eller nei, boks 11). Dersom de er like (hvilket bare er mulig dersom også de to nøkkelverdier er lik hverandre), kan de to kommunikasjonsdeltakere kommunisere med hverandre, idet en tellerutgang som skal benyttes deretter, blir satt til 0 (kommunikasjon startet, teller = 0, boks 12). Etter kommunikasjonen blir påfølgende første og andre styresignal generert (etter kommunikasjon, generer påfølgende styresignaler, boks 13), idet påfølgende første nøkkelverdi (boks 6) blir generert som en funksjon av det påfølgende første styresignal (boks 8) og av en momentan første nøkkelverdi (boks 6), og en påfølgende andre nøkkelverdi (boks 7) som blir generert som en funksjon av det påfølgende andre styresignal (boks 9) og av en momentan andre nøkkelverdi (boks 7).

Dersom de to kodesignaler ikke er lik hverandre (hvilket bare er mulig dersom heller ikke de to nøkkelverdier er lik hverandre), blir tellerutgangen øket med 1 (økningsteller, boks 14). Det blir så testet om denne tellerutgang har verdien 10 (teller = 10?, boks 15). Så lenge dette ikke er tilfelle, blir kommandosignalet repetert og ingen kommunikasjon finner sted (repeter kommandosignal, ingen kommunikasjon, boks 17). Så snart tellerutgangen har verdien 10, blir denne utgang satt til verdien 0 og alarmsignalet blir generert (teller = 0, generer alarmsignal, boks 16).

For at fremgangsmåten ifølge oppfinnelsen skal fungere ordentlig, er det nødvendig at første og andre kodesignal

hver er den samme funksjon av kommandosignalet og av henholdsvis første og andre nøkkelverdi (med andre ord at boksene 4 og 5 er identiske), at påfølgende første og andre nøkkelverdi hver er den samme funksjon av henholdsvis den momentane første og andre nøkkelverdi og av henholdvis første og andre styresignal (med andre ord at boksene 6 og 7 er identiske), og at første og andre styresignal er identiske med hverandre (med andre ord at boksene 8 og 9 er identiske), hvilket f.eks. kan realiseres ved å ta begge disse fra utgangen av en tilfeldig generator. Tellerens utgangsverdi 10, ved hvilken alarmen blir generert, er selvfølgelig valgt helt vilkårlig fra settet med naturlige numre.

De første og andre kontrollsignaler, som svar på hvilke de påfølgende første og andre nøkkelsignaler kan genereres, kan sendes enten etter kommunikasjonen (figur 1), før kommunikasjonen, eller i løpet av kommunikasjonen, i hvilken sammenheng uttrykket kommunikasjon skal tolkes så vidt som mulig. F.eks. kan det være en telefonsamtale mellom forskjellige (trådløse) abonnenter, eller bare en kommando som kommer fra en bakkestasjon og er ment for en satellitt. Det kan også være en fullstendig datafil, eller et dataord, hvor f.eks. noen numre er ment for autentisering.

Blokkdiagrammet vist på figur 2 av systemet 20 ifølge oppfinnelsen omfatter en første kommunikasjonsdeltaker 21 og en andre kommunikasjonsdeltaker 22. For enkelhets skyld er det bare vist to gjensidig koblede kommunikasjonsdeltakere, mens i praksis (f.eks. i tilfelle av et telefonnettverk) kan mange andre kommunikasjonsdeltakere bli koblet til en første kommunikasjonsdeltaker, og to første kommunikasjonsdeltakere kan også være gjensidig koblet. Kommunikasjonsdeltaker 21 og kommunikasjonsdeltaker 22 er gjensidig koblet via forbindelsen 23, som kan være implementert i enten fysisk form eller delvis i trådløs form.

Kommunikasjonsdeltaker 21 omfatter en overvåkningsenhet 30 med en inngang 30-1 og en utgang 30-2 som begge er koblet

til en forbindelse 23 i den hensikt å kontinuerlig overvåke forbindelsens tilstand. Overvåkningsenhet 30 har også en utgang 30-3 som er koblet til en inngang 31-1 av en styresignalgenerator 31 som via en utgang 31-3 genererer et første styresignal som svar på et overvåkningssignal som er til stede ved inngangen 31-1. Utgang 31-3 er koblet til en inngang 32-1 hos første nøkkelverdi-genereringsorganer 32 som, som svar på det første styresignal, genererer en (påfølgende) første nøkkelverdi som kan være en funksjon av det første styresignal, og som, i alle tilfelle, er en funksjon av en (momentan) første nøkkelverdi. I denne sammenheng er en utgang 32-3 hos nøkkelverdi-genereringsorganene 32 koblet til en inngang 32-2. Utgang 32-3 er også koblet til en inngang 33-1 hos første kodesignal-genereringsorganer 33 som ytterligere har en inngang 33-2 og en utgang 33-3. Inngang 33-2 er koblet til en utgang 34-3 hos kommandosignal-genereringsorganene 34, som ytterligere har en inngang 34-1 som er koblet til forbindelsen 23, og en inngang 34-2 som er koblet til utgang 30-3. Som svar på overvåkningssignalet som er til stede ved inngangen 34-2 og/eller signalet som er til stede ved inngangen 34-1, genererer kommandosignal-genereringsorganene 34 et kommandosignal som via utgang 34-3 og inngang 33-2, blir tilført til kodesignal-genereringsorganene 33. Kodesignal-genereringsorganene 33 genererer et første kodesignal som er en funksjon av kommandosignalet som er til stede ved inngangen 33-2 og av den første nøkkelverdi som er til stede ved inngang 33-1. Via utgang 33-3 blir det første kodesignal tilført til en inngang 35-1 hos sammenligningsorganene 35, som også har en inngang 35-2 som er knyttet til forbindelsen 23 i den hensikt å motta et andre kodesignal, og en utgang 35-3. Utgang 3-53 er knyttet til forbindelsen 23 og til en inngang 36-1 hos tellerorganene 36 som ytterligere har en utgang 36-3 som er knyttet til en inngang 37-1 hos komparatoren 37, og en inngang 36-2 som er koblet til en utgang 37-3 hos komparatoren 37. I tillegg har komparatoren 37 en inngang 37-2 som får tilført et signal med verdien 10, og utgangen 37-3 er koblet til forbindelsen 23. Dersom det

første kodesignal ved inngang 35-1 og et andre signal ved inngang 35-2 ikke stemmer overens, genererer sammenligningsorganer 35 et tellersignal til tellerorganer 36 som, som svar på dette, øker sin utgangsverdi med én. Så snart denne utgangsverdien har verdien 10, genererer komparatoren 37 et alarmsignal for å alarmere enhet 38 og et tilbakestillingssignal som blir tilført til tellerorganene 36 som, som svar på dette, tilbakestiller deres utgangsverdi til null.

Kommunikasjonsdeltaker 22 omfatter en overvåkningsenhet 40 med en inngang 40-1 og en utgang 40-2 som begge er koblet til forbindelsen 23 i den hensikt å kontinuerlig overvåke forbindelsens tilstand. Overvåkningsenhet 40 har også en utgang 40-3 som er koblet til en inngang 41-1 hos en styresignalgenerator 41 som via en utgang 41-3, genererer et andre styresignal som svar på et overvåkningssignal som er til stede ved inngang 41-1. Utgang 41-3 er koblet til en inngang 42-1 hos andre nøkkelverdi-genereringsorganer 42 som, som svar på et andre styresignal, genererer en (påfølgende) andre nøkkelverdi som kan være en funksjon av det andre styresignal og som, i alle tilfelle, er en funksjon av en (momentan) andre nøkkelverdi. I denne sammenheng er en utgang 42-3 hos nøkkelvergi-genereringsorganene 42 koblet til en inngang 42-2. Utgang 42-3 er også koblet til en inngang 43-1 hos andre kodesignal-genereringsorganer 43, som videre har en inngang 43-2 og en utgang 43-3. Inngang 43-2 er koblet til forbindelsen 23. Kodesignal-genereringsorganer 43 genererer et andre kodesignal som er en funksjon av det kommandosignal som er til stede ved inngang 43-2, og som blir tilført via forbindelse 23, og av den andre nøkkelverdi som er til stede ved inngang 43-1. Det andre kodesignal blir via utgang 43-3 og forbindelsen 23 tilført til inngang 35-2 hos sammenligningsorganene 35.

Systemet 20 som vist på figur 2, virker som følger. Dersom det forlanges kommunikasjon, genererer kommandosignalgenereringsorganene 34 kommandosignalet som blir tilført

til kodesignal-genereringsorganene 33 og, via forbindelse 23, til kodesignal-genereringsorganene 43. Kodesignal-genereringsorganene 33 genererer det første kodesignal som er en funksjon av kommandosignalet og av den første nøkkelverdi som kommer fra nøkkelverdi-genereringsorganene 32. Kodesignal-genereringsorganene 43 genererer det andre kodesignal som er en funksjon av kommandosignalet og av den andre nøkkelverdi som kommer fra nøkkelverdi-genereringsorganene 42. Det første kodesignal blir tilført direkte, og det andre kodesignal blir via forbindelsen 23 tilført til sammenligningsorganene 35.

Vanligvis vil de to kodesignalene være identiske fordi det to kodeverdiene er identiske, og sammenligningsorganene 35 genererer et signal som, via forbindelse 23, blir tilført til overvåkningsenhet 30 og overvåkningsenhet 40, som svar på hvilket kommunikasjonen kan begynne. Organene som implementerer denne kommunikasjonen er ikke vist på figur 2, og de kan i prinsippet utføres på mange måter. Således er det f.eks. mulig å arrangere at påfølgende kommandosignaler, som er utstyrt med data, kan genereres av kommando-signal-genereringsorganene 34, hvilke kommandosignaler, enten kodede eller ikke kodede via kodesignal-genereringsorganene 33 og 43, så blir sendt frem og tilbake via forbindelse 23. Det ville også være mulig å sende lange dataord frem og tilbake via forbindelsen 23, idet et antall byte for hvert dataord tjener som autentisering, og idet det således utføres en kontroll for hvert dataord for å se om de to nøkkelverdier stemmer overens.

Etter at kommunikasjonen er slutt, hvilket blir overvåket av overvåkningsenhetene 30 og 40, genererer overvåkningsenhet 30 et signal til styresignalgeneratoren 31, som svar på hvilket nevnte generator genererer det første styresignal som blir tilført til nøkkelverdi-genereringsorganene 32, og overvåkningsenhet 40 genererer et signal til styresignalgenerator 41, som svar på hvilket nevnte generator genererer det andre styresignal som blir tilført til nøkkelverdi-genereringsorganene 42. Nøkkelverdi-generatorene,

henholdsvis 32 og 42, genererer så den påfølgende respektive første og andre nøkkelverdi, som er en funksjon av den momentane respektive første og andre nøkkelverdi, og som også kan være en funksjon av det respektive første og andre styresignal. Deretter kan den neste kommunikasjon finne sted på basis av de nye nøkkelverdier. Det er i denne sammenheng hensiktsmessig at de sekundære kommunikasjonsdeltakere (på figur 2 er bare én sekundær kommunikasjonsdeltaker 22 vist) kan produseres på samme måte, uten at hver kommunikasjonsdeltaker må få tilført en unik nøkkel. Eller, f.eks. i tilfelle av et trådløst telefonsystem med en primær og en sekundær kommunikasjonsdeltaker, at av alle trådløse telefonsystemer som skal produseres, kan alle de primære kommunikasjonsdeltakere på den ene side og alle de sekundære kommunikasjonsdeltakere på den andre side produseres på identisk måte. Etter at autentisering har funnet sted bare noen få ganger, vil hver sekundær kommunikasjonsdeltaker, eller hvert sett av primære og sekundære kommunikasjonsdeltakere, ha blitt fullstendig unike med hensyn til alle de andre kommunikasjonsdeltakerne, eller med hensyn til alle de andre sett av kommunikasjonsdeltakere.

Dersom de to kodesignaler ikke er identiske (fordi de to nøkkelverdier ikke er like), genererer sammenligningsorganene 35 tellersignalet, som svar på hvilket tellerorganene 36 øker sine utgangsverdier med 1, og som svar på hvilket kommandosignal-genereringsorganene 34 genererer kommandosignalet igjen. Som et resultat blir de to kodesignaler generert igjen av kodesignal-genereringsorganene 33 og 43 på basis av de momentane, uforandrede nøkkelverdier hos nøkkelverdi-genereringsorganene 32 og 42, og de to kodesignaler blir sammenlignet igjen, osv. Dersom de to kodesignaler faktisk er identiske denne gang, f.eks. fordi det forekom en feil ved den tidligere generering, kan kommunikasjonen begynne. I dette tilfelle skulle utgangsverdien hos tellerorganene tilbakestilles til null. Dersom de to kodesignaler blir funnet å være ulike ved ti påfølgende tilfeller, har utgangsverdien hos tellerorganene 36 verdi-

en ti og komparatoren 37 genererer alarmsignalet til alarmenheten 38.

Genereringen av kommandosignalet ved hjelp av kommandosignal-genereringsorganene 34 når kommunikasjon er ønsket, blir generelt utført under kontroll av overvåkningsenheten 30, eller ellers under kontroll av kommunikasjonsdeltaker 21. Dersom kommunikasjonsdeltaker 22 også er påkrevet for å være i stand til å initiere kommunikasjon, kan dette utføres ved å gjøre overvåkningsenhet 40 så vel som overvåkningsenhet 30 egnet for kontroll av kommandosignal-genereringsorganer 34 (via forbindelsen 23). Alternativt kan dette oppnås ved hjelp av likeledes å utstyre kommunikasjonsdeltaker 22 med kommandosignal-genereringsorganer. I begge tilfeller må det så etableres prioritetsregler for å forhindre at de to kommunikasjonsdeltakere 21, 22 kommer ut av synkronisasjon som en konseskvens av samtidig tilkjennegivelse av ønsket om å kommunisere. Videre kunne kommunikasjonsdeltaker 22 være utstyrt med ytterligere sammenligningsorganer, ytterligere tellerorganer og/eller en ytterligere komparator, svarende til kommunikasjonsdeltaker 21, som da gjør det mulig for hver kommunikasjonsdeltaker 21, 22 selv å kontrollere identiteten hos den andre.

Når hver kommunikasjonsdeltaker 21, 22 selv kan kontrollere identiteten til den andre, frembringer dette, med en liten forlengelse, muligheten for å muliggjøre kommunikasjon selv etter at tellerorganene som er til stede i begge kommunikasjonsdeltakerne, har eller skulle ha generert tilbakestillingssignalet og alarmsignalet. Ved f.eks. å ha en fast tilbakestillingsnøkkelverdi generert i apparatet hos hver kommunikasjonsdeltaker 21, 22 som svar på tilbakestillingssignalet hos tellerorganene, er det oppnådd at de to kommunikasjonsdeltakere følgelig vil generere like kodesignaler, hvilket muliggjør kommunikasjon. Denne "tilbakestilling" burde finne sted internt og på en slik måte at hver kommunikasjonsdeltaker 21, 22 kun er i stand til å gjøre dette med hensyn til seg selv, idet det ikke er mu-

lig for noen utenforstående å være i stand til å gjøre det samme med hensyn til den gjeldende kommunikasjonsdeltaker. Tilbakestillingssignalet i dette tilfelle må under ingen omstendigheter bli overført via forbindelsen 23 eller komme frem til forbindelsen 23, idet dette forhindres ved å utstyre hver kommunikasjonsdeltaker 21, 22 med egne tellerorganer.

Konstruksjonen av kommuniksasjonsdeltakere 21, 22 som vist i blokkdiagrammet på figur 2, kunne ha blitt betydelig forenklet ved å utelate styresignalgeneratorene 31, 41, i hvilket tilfelle de to nøkkelverdi-generatororganene32, 42 f.eks. kan styres ved hjelp av kommandosignal-generatororgan 34. I praksis betyr dette at første og andre styresignal faller samme med kommandosignalet og at den påfølgende nøkkelverdi er en funksjon av den momentane nøkkelverdi og av kommandosignalet.

I tilfelle av forskjellige sekundære kommunikasjonsdeltakere 22, som alle må være i stand til å kommunisere med den primære kommunikasjonsdeltaker 21, vil det være mulig å sende en identifikasjonskode før kommunikasjonen, hvilken identifikasjonskode identifiserer hvilken sekundær kommunikasjonsdeltaker 22 som skal involveres i kommunikasjonen. En slik identifikasjonskode kan f.eks. legges til kommandosignalet. Det er imidlertid også tenkelig at kodesignalet i seg selv i og for seg tjener som identifikasjon, f.eks. ved at hver sekundær kommunikasjonsdeltaker 22 har kodesignal-genereringsorganer 43 som er basert på en unik funksjon, eller ved å ha nøkkelverdi-genereringsorganer som er basert på en unike funksjon. I dette tilfelle er det ufordelaktig at hver sekundær kommunikasjonsdeltaker 22 da må bli utstyrt med en unik funksjon, hvilket setter ytterligere krav til produksjonsprosessen. Ytterligere må alle de unike funksjoner være kjent hos den første kommunikasjonsdeltaker 21, hvilket øker sistnevntes størrelse og kompleksitet.

At kommondosignal-genereringsorganer 34 genererer komman-

dosignalet en gang til dersom de to kodesignaler ikke er identiske, er selvfølgelig bare én utførelsesform. Det er f.eks. også tenkelig at dette kommandosignal forblir ved utgang 34-3 så lenge det ikke er funnet noen likhet mellom kodesignalene, dvs. inntil tilbakestillingssignalet genereres eller har blitt generert av komparatoren 37.

P a t e n t k r a v

1. Fremgangsmåte ved autentisering av kommunikasjonsdeltakere, idet en første kommunikasjonsdeltaker (1) genererer et kommandosignal (3) og genererer et første kodesignal (4) som er en funksjon av minst kommandosignalet (3) og en første nøkkelverdi (6) som er knyttet til den første kommunikasjonsdeltaker (1), og idet en andre kommunikasjonsdeltaker (2) genererer et andre kodesignal (5) som er en funksjon av minst kommandosignalet (3) og en andre nøkkelverdi (7) som er knyttet til den andre kommunikasjonsdeltaker (2), hvilke første (4) og andre (5) kodesignal blir sammenlignet (10) med hverandre for å autentisere kommunikasjonsdeltagere (1, 2) dersom begge signaler er like, i hvilket tilfelle kommunikasjon blir etablert, idet den første kommunikasjonsdeltaker (1), som svar på et første styresignal (8), genererer en påfølgende første nøkkelverdi (13) og den andre kommunikasjonsdeltaker (2), som svar på et andre styresignal (9), genererer en påfølgende andre nøkkelverdi (13),
k a r a k t e r i s e r t v e d at den påfølgende første nøkkelverdi (13) er en funksjon av minst den første nøkkelverdi (6), og den påfølgende andre nøkkelverdi (13) er en funksjon av minst den andre nøkkelverdi (7).

2. Fremgangsmåte som angitt i krav 1,
k a r a k t e r i s e r t v e d at den påfølgende første nøkkelverdi (13) også er en funksjon av minst det første styresignal (8), og den påfølgende andre nøkkelverdi (13) er også en funksjon av minst det andre styresignal (9).

3. System (20) for kommunikasjonsdeltagere (21, 22), idet en første kommunikasjonsdeltaker er utstyrt med

- kommandosignal-genereringsorganer (34) for å generere et kommandosignal,
- første kodesignal-genereringsorganer (33) for å generere et første kodesignal som en funksjon av minst kommandosignalet og den første nøkkelverdi knyttet til den

første kommunikasjonsdeltaker (21),
og idet en andre kommunikasjonsdeltaker (22) er utstyrt med

- andre kodesignal-genereringsorganer (43) for å generere et andre kodesignal som en funksjon av minst kommandosignalet og den andre nøkkelverdi knyttet til den andre kommunikasjonsdeltaker (22),
- sammenligningsorganer (35) for å sammenligne det første og andre kodesignal med hverandre, og dersom de er like å generere et autentiseringssignal for å muliggjøre kommunikasjon mellom den første kommunikasjonsdeltager (21) og den andre kommunikasjonsdeltager (22), og
- første nøkkelverdi-genereringsorganer (32) for å generere den påfølgende første nøkkelverdi som svar på et første styresignal, og
- andre nøkkelverdi-genereringsorganer (42) for å generere en påfølgende andre nøkkelverdi som svar på et andre styresignal,

k a r a k t e r i s e r t v e d at de første nøkkelverdi-genereringsorganer (32) er tilpasset for å generere, som en funksjon av minst en første nøkkelverdi, den påfølgende første nøkkelverdi og de andre nøkkelverdi-genereringsorganer (42) er tilpasset for å generere, som en funksjon av minst en andre nøkkelverdi, den påfølgende andre nøkkelverdi.

4. System (20) som angitt i krav 3,
k a r a k t e r i s e r t v e d at de første nøkkelverdi-genereringsorganer (32) er tilpasset for å generere den påfølgende første nøkkelverdi også som en funksjon av det første styresignal og de andre nøkkelverdi-genereringsorganer er tilpasset for å generere den påfølgende andre nøkkelverdi også som en funksjon av det andre styresignal.

5. Første kommunikasjonsdeltaker (21) for kommunikasjon med en andre kommunikasjonsdeltaker (22), idet begge kommunikasjonsdeltakere er elementer i systemet som angitt i krav 3, hvilken første kommunikasjonsdeltaker er utstyrt

med

- kommandosignal-genereringsorganer (34) for å generere et kommandosignal,
- første kodesignal-genereringsorganer (33) for å generere et første kodesignal som en funksjon av minst kommandosignalet og en første nøkkelverdi knyttet til den første kommunikasjonsdeltaker (21),
- sammenligningsorganer (35) for å sammenligne det første kodesignal med et andre kodesignal, idet det andre kodesignal er generert av andre kodesignal-genereringsorgan (43) innlemmet i den andre kommunikasjonsdeltager (22), og dersom de er like å generere et autentiseringssignal for å muliggjøre kommunikasjon mellom den første kommunikasjonsdeltager (21) og den andre kommunikasjonsdeltager (22), og
- første nøkkelverdi-genereringsorganer (32) for å generere en påfølgende første nøkkelverdi som svar på det første styresignal,

k a r a k t e r i s e r t v e d at de første nøkkelverdi-genereringsorganer (32) er tilpasset for å generere, som en funksjon av minst den første nøkkelverdi, den påfølgende første nøkkelverdi.

6. Første kommunikasjonsdeltaker (21) som angitt i krav 5,

k a r a k t e r i s e r t v e d at de første nøkkelverdi-genereringsorganer (32) er tilpasset for å generere den påfølgende første nøkkelverdi også som en funksjon av det første styresignal.

7. Andre kommunikasjonsdeltaker (22) for kommunikasjon med en første kommunikasjonsdeltaker (21), idet begge kommunikasjonsdeltakere er elementer i systemet (20) i henhold til krav 3, og idet den andre kommunikasjonsdeltaker (22) er utstyrt med

- andre kodesignal-genereringsorganer (43) for å generere et andre kodesignal som en funksjon av i det minste en andre nøkkelverdi som er knyttet til den andre kommunikasjonsdeltaker (22) og et kommandosignal generert av

kommandosignal-genereringsorganer (34) som er innlemmet i den første kommunikasjonsdeltaker (21), idet den første kommunikasjonsdeltaker (21) omfatter sammenligningsorganer (35) for å sammenligne det andre kodesignal og et første kodesignal generert ved de første kodesignal-genereringsorganer (33) innlemmet i den første kommunikasjonsdeltaker (21), og dersom de er like å generere et autentiseringssignal for å muliggjøre kommunikasjon mellom den første kommunikasjonsdeltaker (21) og den andre kommunikasjonsdeltaker (22), og

- andre nøkkelverdi-genereringsorganer (42) for å generere en etterfølgende andre nøkkelverdi som reaksjon på et andre styresignal,

k a r a k t e r i s e r t v e d at de andre nøkkelverdi-genereringsorganer er tilpasset for å generere, som en funksjon av minst den andre nøkkelverdi, den påfølgende andre nøkkelverdi.

8. Andre kommunikasjonsdeltaker (22) som angitt i krav 7,

k a r a k t e r i s e r t v e d at de andre nøkkelverdi-genereringsorganer (42) er tilpasset for å generere den påfølgende andre nøkkelverdi også som en funksjon av det andre styresignal.

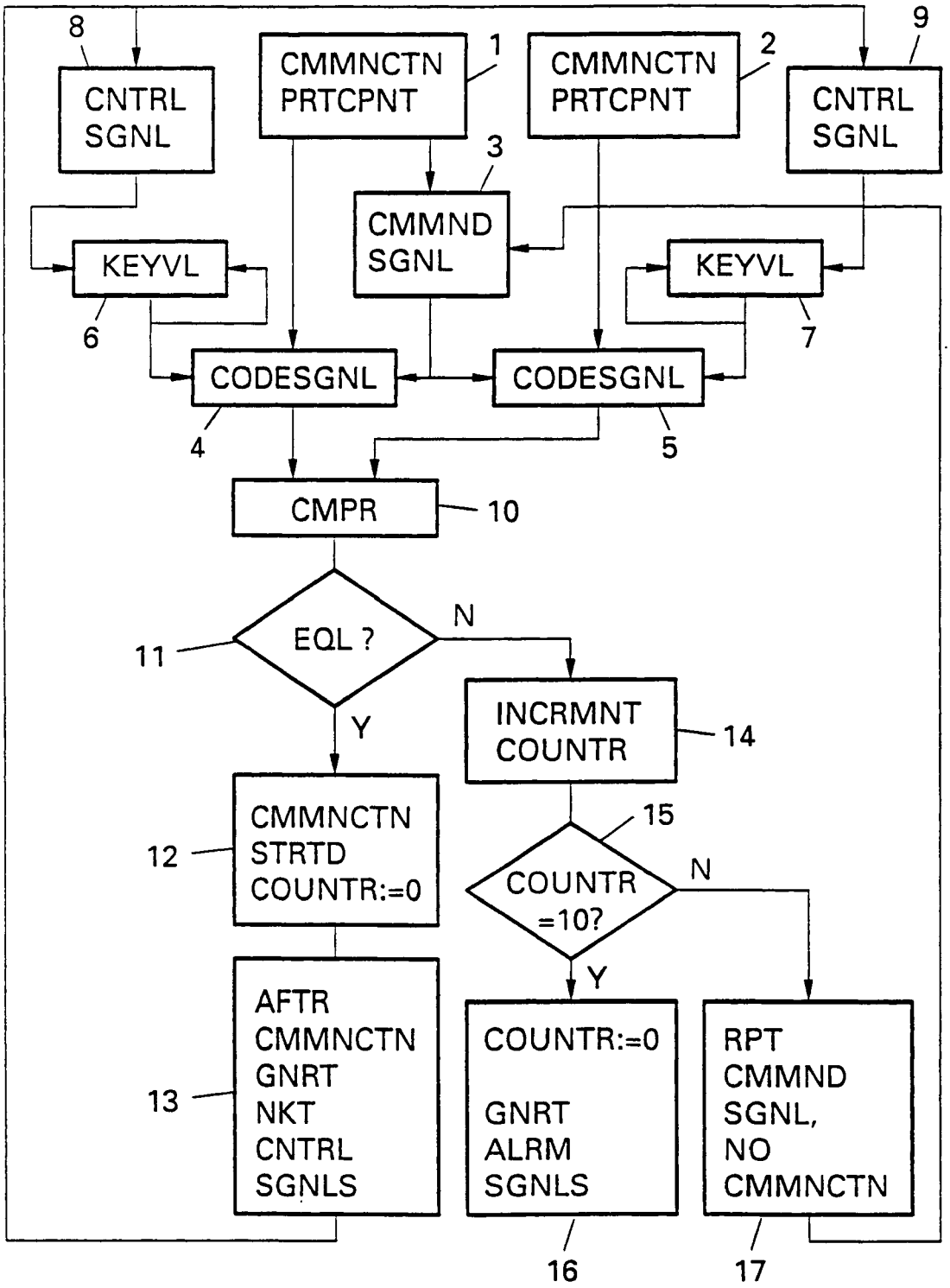

8
CNTRL SGNL
CMMNCTN PRTCPNT
1
CMMNCTN PRTCPNT
2
9
CNTRL SGNL
3
CMMND SGNL
KEYVL
6
KEYVL
7
CODESGNL
4
CODESGNL
5
CMPR
10
EQL ?
11
N
Y
INCRMNT COUNTR
14
CMMNCTN STRTD COUNTR:=0
12
15
COUNTR =10?
N
Y
AFTR CMMNCTN GNRT NKT CNTRL SGNLS
13
COUNTR:=0
GNRT ALRM SGNLS
16
RPT CMMND SGNL, NO CMMNCTN
17

Fig. 1

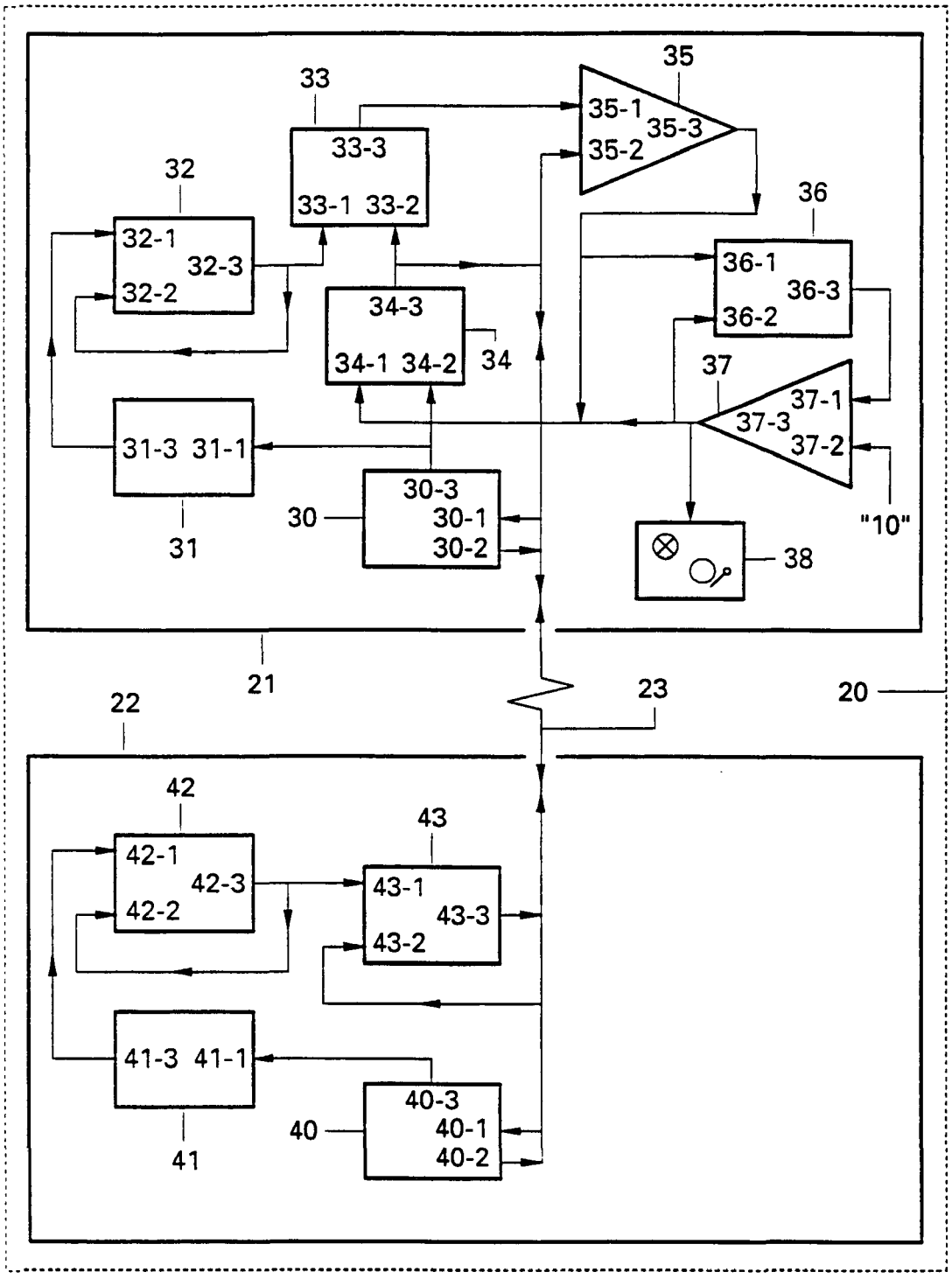

35
33
35-1
35-3
35-2
33-3
33-1 33-2
32
36
32-1
32-3
32-2
36-1
36-3
36-2
34-3
34-1 34-2
34
37
37-1
37-3
37-2
31-3 31-1
30-3
30
30-1
30-2
"10"
38
31
21
23
20
22
42
43
42-1
42-3
42-2
43-1
43-3
43-2
41-3 41-1
40-3
40
40-1
40-2
41

Fig. 2