



⑫ A Terinzagelegging ⑪ 8005672

Nederland

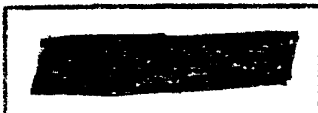
⑲ NL

- ⑤4 Inrichting voor vriend-vijand identificatie.
- ⑤1 Int.Cl³: G01S 13/78.
- ⑦1 Aanvrager: Siemens Aktiengesellschaft te Berlijn en München, Bondsrepubliek Duitsland.
- ⑦4 Gem.: Ir. G.F. van der Beek c.s.
NEDERLANDSCH OCTROOIBUREAU
Joh. de Wittlaan 15
2517 JR 's-Gravenhage.

- ②1 Aanvraag Nr. 8005672.
- ②2 Ingediend 15 oktober 1980.
- ③2 Voorrang vanaf 16 oktober 1979.
- ③3 Land van voorrang: Bondsrepubliek Duitsland (DE).
- ③1 Nummer van de voorrangsaanvraag: P 2941820 .
- ⑥2 --

- ④3 Ter inzage gelegd 3 december 1984.

De aan dit blad gehechte stukken zijn een afdruk van de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekening(en).



Inrichting voor vriend-vijand identifikatie

De uitvinding heeft betrekking op een inrichting voor vriend-vijand identifikatie onder toepassing van gecodeerde ondervragingen en antwoorden in samenhang met een ondervraaginrichting van de ondervragende en een transponder van de ondervraagde posten, en met een radiotelefonie-inrichting voor de overdracht van versleutelde berichten tussen de ondervragende en de ondervraagde post.

Teneinde in IFF-stelsels verwerkbare informaties van ondervraagde posten te verkrijgen kunnen er onder bepaalde omstandigheden een groot aantal maatregelen nodig zijn om de ondervraging en de antwoordafgifte door een transponder vooral tegen doelbewuste stoorhandelingen van een tegenpartij te beschermen en voor niet-bevoegde personen onleesbaar te maken. Eén van deze maatregelen kan bijvoorbeeld hierin bestaan, de ondervraging te versluieren teneinde op deze manier te bereiken, dat ondervragingen van de tegenpartij geen IFF-antwoord kunnen initiëren. Anderzijds is de versleuteling van het IFF-antwoord van groot belang, opdat een vijandelijk wapenstelsel geen positief vriend-kenteken kan afgeven. Eveneens is het van belang, dat het vriend-kenteken ongestoord ontvangen kan worden. Daar het IFF-antwoord tot nu toe betrekkelijk breedbandig op een gereserveerde frequentie uitgezonden wordt, is een storing van de overdracht van het antwoord en daarmee een vermindering van de werking van snel reagerende omvattingssystemen door middel van geringe vijandelijke bemoeiingen mogelijk.

Aan de uitvinding ligt de opgave ten grondslag, om bij een inrichting voor vriend-vijand identifikatie van de in de aanhef genoemde soort, de storingszekerheid met relatief geringe kosten te verbeteren.

Volgens de uitvinding wordt dit aldus bereikt, dat voor de storingsbestendige IFF-overdracht onder mede-toepassing van inrichtingen of delen van inrichtingen van een storingsbestendig uitgevoerde radiotelefonie-inrichting, de overdracht van het antwoord (kentekening) van de ondervraagde post volgens de frequentiesprongwerkwijze via de radiotelefonie-inrichting zodanig gebeurt, dat de ondervragende post als ondervraging een

8005672

[REDACTED]

vast op de ondervraagde post bekend versleuteld codewoord teza-
men met een versleuteld, een frequentie-adres bevattend, varia-
bel gegevensdeel uitzendt, dat gelijktijdig de antwoordontvanger
van de radio-inrichting van de ondervragende post op de zendfre-
5 quentie van het te verwachten antwoord, van de ondervraagde
post instelt, en dat het gereedstellen van de zendfrequenties
van de ondervraagde post met behulp van een door het frequentie-
adres gestuurde frequentiesyntetiseerschakeling gebeurt, en dat
op een eerste antwoord van geringe redundantie wanneer nodig,
10 een genummerd tweede antwoord met grote redundantie na elkaar
op meerdere verschillende frequenties uitgezonden wordt.

Het voordeel van de inrichting volgens de uitvinding is
hierin gelegen, dat de ondervraging buitengewoon storingszeker
is en dat geringe extra kosten voor het opwekken van de fre-
15 quentie-adressen en van de sleuteltekst voor de versleuteling
van het kenteken nodig zijn, daar het antwoordadres impliciet
medegedeeld wordt.

Daar vrijwel alle wapenstelsels in de toekomst storings-
bestendige radiotelefonie-inrichtingen mee zullen voeren, is
20 het van voordeel om deze inrichtingen of delen daarvan voor
een storingsbestendige kentekenoverdracht mede te benutten.
Hierbij heeft de IFF-antwoordafgifte een absolute voorrang. De
storingswerking op een juist bestaande radiotelefonieverbin-
ding kan door de redundante spraakoverdracht opgevangen worden
25 op voorwaarde, dat het IFF-antwoord kort (ca 10 ms.) is en be-
trekkelijk zelden afgegeven behoeft te worden (twee onder-
vragingen per sek.).

Om de storingsbestendigheid van de radiotelefoniever-
binding te verhogen resp. eerst te bereiken, wordt de voor grond-
30 grond communicatie zeer geschikte frequentie-sprongwerkwijze toe-
gepast. Dat wil zeggen, dat er in elk radiotelefonie-apparaat
een reeks van frequenties (beter binaire instelwaarden voor de
syntetiseerschakeling) opgeslagen zijn. Daarenboven worden er
voor de opbouw van de radiotelefonieverbinding signaliseringsme-
35 thoden van de correlatie-ontvangst toegepast. De oproepsignalen
bestaan hierbij uit een duidelijk, volgens goede correlatie-eigen-
schappen uitgezocht tijdsken en een versleuteld, de ontvanger
markerend oproepwoord.

Voor het IFF-antwoord kunnen deze radiotelefonie-type-
40 rende oproepsignalen, i.h.b. de overeenkomstige signaalgever en

8005672

signaalontvanger mede gebruikt worden. Een geschikte IFF-specifieke camouflage of versluiering van het oproepwoord zorgt voor de afscheidbaarheid van IFF- en radiotelefoniesignalen.

- Voor de afgifte van een IFF-antwoord moeten er aan het
- 5 radio-telefonie-apparaat de volgende signalen afgegeven worden:
- frequentieadres of instelinformatie voor de frequentiesyntetiseerschakeling;
 - een versluier/^{tekst}voor de IFF-individuele versluiering van het radiotelefonie-oproepwoord;
- 10 - zendinstructie.

Het gereedmaken van deze signalen geschiedt of in een aanpassingsapparaat tussen IFF-transponder en radiotelefonie-apparaat, of het gebeurt als een vast onderdeel van de transponder.

- 15 Verder wordt de IFF-antwoordafgifte op adaptieve wijze uitgevoerd, d.w.z. een eerste ondervraging behoort slechts een kort antwoord te initiëren. De storingswerking van dit antwoord op de radiotelefonie is dan slechts gering. Slechts in 10% van alle ondervragingen zal een z.g. tweede ondervraging nodig zijn
- 20 en een herhaald, op vele frequenties over te dragen IFF-antwoord initiëren, zodat de totale zekerheid van onderscheiding van een IFF-antwoord zeer groot wordt.

De versleuteling en ontsleuteling van een IFF-ondervragingssignaal gaat uit van synchronisatie van de korresponderende versleutelingsapparaten. Deze synchronisatie kan door middel

25 van meer of minder nauwkeurige standaard-tijdinrichtingen (klokken) gedwongen verkregen worden. Een eenvoudige werkwijze om ondanks synchronisatiefouten op korrekte wijze te ontsleutelen, bestaat hierin, dat door middel van een start-stop-bedrijf van

30 de sleutelinrichting elk tijdincrement (millisekonden tot sekonden) een nieuwe sleuteltekst gegenereerd en opgeslagen wordt. Voor de ontsleuteling worden er nu drie sleutelteksten simultaan toegepast.

1. Sleuteltekst uit een voorafgegaan tijdincrement.
- 35 2. Sleuteltekst uit het juist geldige tijdincrement.
3. Sleuteltekst uit het eerstvolgende tijdincrement.

Het blijkt nu vanzelf, dat de toegestane synchronisatiefout ± 1 tijdincrement mag zijn. Eén van de drie sleutelteksten kan dan het bericht ontsleutelen. Wel moet in het ontvangen

40 bericht het begin resp. einde onderscheiden kunnen worden.

8005672

Daarenboven moet een op de zend- en ontvangplaats bekend, en in het bericht opgenomen versleuteld codewoord de bijbehorende sleuteltekst bepalen.

Al naar gelang de kwaliteit van de toegepaste uurwerken zijn er verschillende methoden voor de IFF-ondervraging- en antwoordafgifte. De kloknaauwkeurigheid speelt in zoverre een rol, dat er met precieze, maar dure klokken (fout 10^{-8}) zeer korte tijdincrementen gemaakt kunnen worden, d.w.z. dat er zeer dikwijls nieuwe sleutelteksten in werking komen. Onnauwkeurige klokken leiden tot lange tijdincrementen, dus ook tot lange geldingstijdduren van een sleuteltekst. Deze samenhang zal hierna-
volgend aan de hand van twee voorbeelden toegelicht worden.

1. Kloknaauwkeurigheid $\pm 10^{-6}$.

De "klok" wordt alle 8 dagen gekorrigeerd.

15 Acht dagen identiek = 691.200 sek.

$$691.200 \cdot 2 \cdot 10^{-6} = 1,38 \text{ sek.}$$

De klokfout kan na 8 dagen $\pm 1,38$ sek. bedragen. Hieruit volgt een tijdincrement van ongeveer 1,5 sek., d.w.z.

20 dat er elke 1,5 sek. een nieuwe sleuteltekst toegepast wordt en alle ondervragingen binnen 1,5 sek. dezelfde versleuteling hebben.

2. Kloknaauwkeurigheid $\pm 10^{-8}$.

De "klok" wordt alle 8 dagen gekorrigeerd.

$$691.200 \cdot 2 \cdot 10^{-8} = 13,8 \text{ msek.}$$

25 Er is dus elke 15 msek. een nieuwe sleuteltekst mogelijk. Praktisch elke ondervraging heeft een andere sleuteltekst als basispositie.

Zoals reeds vermeld, kunnen er bij onnauwkeurige klokken meerdere ondervragingen in de geldingsduur van een sleuteltekst vallen en kunnen dus identieke ondervragingssignalen resp. antwoordsignalen teweegbrengen. Dit kan door de tegenpartij voor storingsdoeleinden benut resp. voor een vriendsimulatie aange-
getrokken worden. Om deze reden wordt bij voorkeur in elke ondervraging een telkens per ondervraging gegenereerd variabel ge-
35 vensdeel ingebouwd. Dit variabele gegevensdeel kan tezamen met de voor langere tijd geldige sleuteltekst als basisinformatie dienen voor het opwekken van frequentie-adressen en voor het versluieren van antwoordkentekens.

De ondervraging bevat in dit geval niet alleen een vast
40 of versleuteld codewoord, maar aanvullend een per ondervraging

8005672



veranderend gegevensdeel. Terwijl er in het vaste codewoord fouten zijn toegelaten, moeten er in het variabele gegevensdeel van de ondervraging door gegevenswaarborgmaatregelen overdracht-fouten ten minste onderscheiden worden. Methoden van de redundante codering kunnen hier toegepast worden.

Het variabele gegevensdeel van de ondervraging kan tezamen met de juist geldige sleuteltekst (delen daarvan) op eenvoudige manier als startinformatie van een lineair teruggekoppeld schuifregister (scrambler) fungeren. Na de onderscheiding van een ondervraging, de ontsleuteling van het ondervraag-sig-naal en het stellen van dit register, kunnen^{er} door gedefinieerde klokpulsen van het register frequentie-adressen en de versluieringstekst voor de versluiering van het antwoordkenteken verkregen en aan de radio-inrichting voor het afgeven van het antwoord verder gegeven worden. Op deze manier kan ook het z.g. tweede antwoord, n.l. vele kentekens op verschillende frequenties, opgewekt worden. In dit geval wordt het register in een opgelegde reeks meervoudig met klokpulsen gestuurd en worden dus per werkstap verschillende frequentie-adressen en verschillende versluieringsteksten opgewekt. Vanzelfsprekend moet een dergelijke procedure aan de ondervraagkant uitgevoerd worden voor het decoderen van het antwoord. Met vertragingstijden welke door de verwerkingstijd van het ondervraagssig-naal bij de transponder veroorzaakt worden, moet aan de antwoordontvangkant rekening gehouden worden. Eveneens kan met de maximaal optredende trajectlooptijd door een "ontvangvenster" voor het betreffende kenteken rekening gehouden worden. De graad van beveiliging van deze werkwijze ten opzichte van vijandelijke stoorcapaciteit resp. simulatievermogen, is weliswaar beperkt maar nog voldoende groot. Deze methode kan vanzelfsprekend ook bij toepassing van meer nauwkeurige klokken toegepast worden. De graad van beveiliging wordt hierbij bij korter wordende geldingsduur van de sleuteltekst hoger.

Bij toepassing van nauwkeurige klokken resp. bij korte geldingsduur van de sleuteltekst (enige millisek.) kan men de overdracht van een variabel gegevensdeel in de ondervraging weglaten, daar elke ondervraging met hoge waarschijnlijkheid met een andere sleuteltekst versleuteld wordt. De waardering van de ondervraging beperkt zich dan slechts nog tot de decodering van het vaste versleutelde codewoord voor de synchro-



nisatie van de transpondersleutelinrichting op de ondervraag-
sleutelinrichting en decodering : 1./2. ondervraging, frequen-
tie-adres en versluis tekst voor de versluiting van het ken-
teken kunnen aan de sleutelinrichting in de transponder ont-
5 leend worden, d.w.z. behalve het opwekken van de sleuteltekst
voor de ontsleuteling van de ondervraging (telkens 3 teksten)
worden verdere sleutelbits voor frequentieadres en kentekenver-
sleuteling opgewekt en verder met het onderscheiden van een
ondervraging^{aan} de radio-inrichting afgegeven. Bij een tweede onder-
10 vraging wordt de sleutelinrichting in een opgelegde tijdreeks
met klokpulsen gestuurd en wordt de ontstane sleuteltekst
aan de radio-inrichting verder afgegeven. Dit gebeurt zowel bij
de ondervrager als bij de transponder (rekening houdend met de
signaalverwerkingstijd).

15 De uitvinding zal aan de hand van verdere uitvoerings-
voorbeelden toegelicht worden met verwijzing naar de tekeningen,
waarin :

fig. 1 het blokschema geeft van een antwoordgever (trans-
ponder) en van de bijbehorende inrichtingen met aansluitingen
20 voor een bijbehorend radiotelefonie-apparaat, en de

fig. 2 en 3 blokschema's geven van een ondervragende
post en een bijbehorend radiotelefonie-apparaat.

Het via een optisch resp. elektronisch ontvangstelsel
1 (fig. 1) gedemoduleerde ondervraagssignaal wordt aan een ont-
25 sleutelingsschakeling 2 ingevoerd. In de ontsleutelingsschake-
ling wordt met behulp van drie verknopingselementen M1, M2 en
M3 gelijktijdig met drie, in de registers SR1, SR2 en SR3 op-
geslagen sleutelteksten het ondervraagssignaal ontsleuteld. De
drie ontsleutelde ondervraagssignalen passeren telkens een ver-
30 gelijkingsregister VR1, VR2 en VR3. De inhouden van deze regis-
ters worden met behulp van een vast ingesteld codewoord in de
vergelijkingsschakelingen V1, V2 en V3 op identiteit onderzocht.
De resultaten van het identiteitsonderzoek worden aan drempel-
waardeschakelingen SW1, SW2 en SW3 toegevoerd. In de drempel-
35 waardeschakelingen wordt het aantal van overeenstemmingen van
ontvangen met het vast ingestelde codewoord bepaald en wordt
bij overschrijding van een voorafbepaalde drempel (aantal over-
eenstemmingen) een signaal aan een logische beslissings-schake-
ling EL afgegeven. De logische beslissingsschakeling bekrach-
40 tigt dan schakelaars S1 en S1' zodanig, dat slechts die sleutel-

8005672



tekst in werking blijft, die het codewoord op de juiste wijze kon ontsleutelen.

Het op het codewoord volgende variabele gegevensdeel en het bijbehorende testdeel van het ondervraagssignaal wordt nu met
5 de juiste sleuteltekst ontsleuteld en kan verder verwerkt worden.

Zoals reeds vermeld, wordt het ontvangen ondervraagssignaal, i.h.b. het codewoordgedeelte, met behulp van drie verschillende sleutelteksten simultaan ontsleuteld. Dit is nodig opdat de nauwkeurigheidsvereiste voor de besturing van een
10 sleutelapparaat S binnen realiseerbare grenzen blijft. Een klokbesturing van het sleutelapparaat 5 zorgt op de plaats van de ondervrager zoals ook bij de transponder voor het opwekken van de sleutelteksten, d.w.z. elk tijdincrement (b.v. sek.) wordt een nieuwe sleuteltekst opgewekt. Tussen twee nieuwe sleutel-
15 teksten kunnen echter meerdere ondervragingen optreden, daarom wordt er bij elke ondervraging een individueel deel (variabel gegevensdeel) in het ondervraagssignaal ingebouwd. Als gevolg van de toegestane klokfout moet ter plaatse van de transponder - zoals boven reeds beschreven - de voor de ondervraging
20 geldige sleuteltekst opgezocht worden. Hierbij staan drie sleutelteksten ter beschikking. Betrokken op een klok U van de transponder en op het binnenkomen van een ondervraging zijn dit de sleutelteksten uit een voorafgaand, een juist geldig en een toekomstig tijdincrement. Via het codewoord, een bij de zend-
25 en ontvangplaats bekende informatie, wordt de passende sleuteltekst uitgezocht en wordt met deze sleuteltekst de verdere verwerking van het ondervraagssignaal uitgevoerd. Het transponder-sleutelapparaat kan op de volgende manier gestuurd worden :

Een klok U, die uit een kwartsgestuurde klokpulsverdeler-
30 keten bestaat, zorgt voor de besturing van de sleutelinrichting 5. Elk tijdincrement kan nu een via een dagsleutel beïnvloedbare sleuteltekst opgewekt worden.

Wordt nu aan de kloktijd de waarde "0" toegevoegd, dan is het juist geldige tijdincrement bij de sleutelinrichting S
35 werkzaam. Het afgelopen resp. toekomstige tijdincrement kan door additie van -1 resp. +1 bij de juist geldige kloktijd werkzaam gemaakt worden.

Bij de onderscheiding van een ondervraging in de transponder wordt de sleutelinrichting S met verhoogde kloksnel-
40 heid driemaal geactiveerd en wordt aan een sommeerschakeling SU

8005672

de waarde -1,0 en +1 toegevoegd. De ontstane sleutelteksten worden in de gescheiden registers SR1, SR2, SR3 en in de registers SIR1, SIR2, SIR3 van een scrambler 4 opgeslagen.

Een andere mogelijkheid van ^{de}besturing bestaat hierin, dat de klok U in de transponder in het algemeen een tijdincrement voorloopt en dat er in het klokritme van de klok per tijdincrement een nieuwe sleuteltekst opgewekt wordt. De opslag van de drie sleutelteksten gebeurt dan seriegewijs door achter elkaar geschakelde registers. Bij de invoer van een nieuwe sleuteltekst worden automatisch de inhouden van de registers verschoven, zodat altijd ook de twee voorafgegane sleutelteksten ter beschikking staan. Gedurende ^{de}ontsleuteling van de ondervraging moeten de drie registers gescheiden worden en moeten zij elk in de keten gesloten worden, opdat de inhouden aan verdere ondervragingen ter beschikking kunnen blijven staan.

De verdere verwerking van het reeds ontsleutelde variabele gegevensdeel geschiedt op de volgende manier. Het variabele gegevensdeel wordt gelijktijdig in twee inrichtingen ingelezen, in een foutonderscheidingsinrichting 3 en in een scrambler 4. In de foutonderscheidingsinrichting 3 wordt door een deelregister DR het variabele gegevensdeel en het bijbehorende testdeel door de generator-veelterm gedeeld. Blijft er aan het einde van het deelproces een rest in het register DR over, d.w.z. zijn niet alle plaatsen van het deelregister "0", dan zijn er overdrachtsfouten te onderscheiden. Een nultestinrichting NT spreekt aan zodra het deelregister met nullen gevuld is, d.w.z. dat er met hoge waarschijnlijkheid geen fouten in de overdracht zijn opgetreden. Bij een met succes bekroonde nultest wordt de verdere verwerking van het variabele gegevensdeel voortgezet.

Zoals reeds vermeld, wordt het variabele gegevensdeel aan de scramblerinrichting 4 verdergegeven en wordt het daar in het scrambler-register SA ingevoerd. Gelijktijdig wordt er uit een via de schakelaar S1 gekozen sleutelregister SIR1, SIR2, SIR3 een sleutelinformatie in een scrambler-register SB overgenomen. Beide informatiedelen, het variabele gegevensdeel en het sleuteldeel, dienen als uitgangswaarde voor het opwekken van een bitreeks volgens de wetmatigheden van lineair teruggekoppelde schuifregisters.

In principe zou hierbij het sleuteltekstgedeelte voor de vorming van het startadres weggelaten kunnen worden. Het sleutel-

8005672

tekstgedeelte verhoogt echter de zekerheid van navorming
van het kenteken en maakt lange registerperioden mogelijk.

De laatste bit van het variabele gegevensdeel stelt een
z.g. ondervraag-"nummer" voor, opdat tussen een eerste onder-
5 vraging en een tweede ondervraging onderscheiden kan worden.
Deze laatste bit wordt in een extra geheugen AN bewaard.

Wanneer de nultest in de foutonderscheidingsinrichting 3
met sukses bekroond wordt, dan worden de schakelaars S2 en S2'
van de scrambler 4 in de stand b gebracht. Het met een start-
10 informatie geladen register SA, SB werkt nu als lineair terug-
gekoppeld schuifregister (scrambler) en wekt een bitreeks op
zodra een schuiftakt toegevoerd wordt. De periode van deze
bitreeks bedraagt 2^{n-1} bit; hierbij is n het aantal trappen
van het register.

15 Bij een eerste ondervraging wordt dit register nu met een
paar klokpulsen gestuurd. De aldus opgewekte bitreeks stelt
een frequentie-adres (a-bits) en een versluierinformatie voor
de versluiering van het kenteken voor. Deze informatie wordt
tezamen met een zendinstructie aan een radiotelefonie-apparaat
20 SF1 verder doorgegeven. Daar wordt de bijbehorende frequentie
ingesteld en wordt een versluierd kentekensignaal opgewekt,
en wordt de zender voor de duur van de afgifte van het kente-
ken via een procesbesturing 6 ingeschakeld.

Een tweede ondervraging initiëert meerdere van deze ken-
25 tekenuitzendingen. Hiertoe wordt het register SA, SB meervou-
dig met klokpulsen gestuurd en wordt de zendinstructie via de
procesbesturing meervoudig afgegeven. Elk van deze kentekens
treedt op een andere frequentie op en bevat een andere ver-
sluierinformatie. Het kenteken zelf is het radiospecifieke
30 oproepsignaal, het wordt ter plaatse van de ondervraging door
correlatiemethoden uit de ontvangsignalen gedecodeerd.

In vergelijking met de IFF-transponder is de ondervraag-
inrichting (fig. 2) beduidend eenvoudiger opgebouwd. De in-
richting bestaat uit de eigenlijke ondervraaginrichting AF en
35 het radiotelefonietoestel SF2. In het bijzonder moet het sleutel-
apparaat 10 met de randregisters SR1, SR2, SR3; SIR1, SIR2,
SIR3 per ondervraging alleen een sleuteltekst genereren en kan
dus vereenvoudigd worden. De inrichtingen voor de identiteits-
test voor de codewoorden vervallen. Er is aanvullend in de on-
40 dervraaginrichting een ruisgenerator RG nodig. Deze wekt per

8005672



ondervraging een nieuw, van de vorige ondervraging onafhankelijk, variabel gegevensdeel op. Het variabele gegevensdeel wordt in de gegevensbeveiligingsinrichting 11 onder toevoeging van redundantie omgewerkt (schakelaar SA2 in de stand a, 5 schakelaar SA3 in de stand a), zodat er in de transponder een foutonderscheiding mogelijk is. De laatste bit van het variabele gegevensdeel stelt het ondervraagnummer voor. Hiertoe wordt de schakelaar SA2 in de stand b gebracht. De in de gegevensbeveiligingsinrichting 11 door veeltermdeling ontstane testbits 10 worden bij toepassing van systematische codes aan het variabele gegevensdeel toegevoegd of vastgemaakt.

De schakelaar SA3 bevindt zich dan in de stand b. Het ondervraagsignaal heeft dientengevolge de volgende opbouw: codewoord; variabel gegevensdeel; testbits voor de foutonderscheiding. 15

In detail zijn de volgende besturingshandelingen nodig :

Synchroon met het uitzenden van het ondervraagsignaal wordt door de zender de sleuteltekst uit het bufferregister PR1 gelezen. Bij een verknopingsselement V wordt de versleutel- 20 ling van het ondervraagsignaal teweeggebracht. Het in een codewoordregister CR opgeslagen, vast ingestelde codewoord wordt eerst uitgezonden (SA1 in de stand a). Hierop aansluitend wordt de schakelaar SA1 in de stand b gebracht. De schakelaars SA2, SA3 en SA4 staan nu in de stand a.

25 Het in de ruisgenerator RG opgewekte variabele gegevensdeel wordt eenmaal in het scramblerregister SCR A geladen. Aan de andere kant wordt in de gegevensbeveiligingsinrichting 11 de deling door de generatorveelterm teweeggebracht en worden tevens de variabele gegevens uitgezonden. De laatste bit van 30 het variabele gegevensdeel is het ondervraagnummer, hiertoe wordt de schakelaar SA2 in de stand b gebracht. Gelijktijdig met het inlezen van het variabele gegevensdeel in het scramblerregister SCR A wordt het scrambler-register SCR B geladen met de in het bufferregister PR 2 aanwezige sleutelinformatie, zo- 35 dat aan het einde van dit proces dezelfde startvoorwaarde voor het opwekken van de scramblerreeks ingevoerd is als op de plaats van de transponder.

Na de overdracht van het variabele gegevensdeel wordt de schakelaar SA3 in de stand b gebracht en wordt het deelre- 40 sultaat - de testplaatsen - uit de gegevensbeveiligingsinrich-

8005672



ting 11 uitgelezen en uitgezonden. Rekening houdend met de in de transponder ontstane signaalverwerkingstijd, wordt de scrambler SCRA, SCRB via de schakelaar SA4 (stand b) gestart. De ontstane bitreeks wordt tezamen met de ontvanginstructie aan 5 het radiotelefonie-apparaat SF2 afgegeven.

In het radiotelefonie-apparaat SF2 (fig. 3) wordt de overdrachtfrequentie van het kenteken ingesteld en wordt de versluiertekst voor de ontsluiting van het kenteken ter beschikking gesteld. Een kentekencorrelator KK in het radiotelefonie-
10 apparaat "zoekt" nu het kenteken in het ontvangsignaal op. Wordt het kenteken ontdekt, dan wordt er bij een procesbeturing AST van de ondervraaginrichting AF een overeenkomstig signaal afgegeven, d.w.z. er is een "vriend"-melding binnengekomen. Een tweede ondervraging is dan niet nodig.

15 Wordt er daarentegen binnen ^{een} bepaald tijdvenster (μ s - ms) geen kenteken ontdekt, dan wordt de tweede ondervraging gestart. De scrambler SCRA, SCRB wordt hiertoe meervoudig met klokpulsen gestuurd, zodat synchroon met het transponderradio-apparaat de bijbehorende frequenties en versluierteksten werk-
20 zaam worden. De tweede ondervraging is dan "met sukses bekroond" wanneer tenminste één van de kentekens onderscheiden wordt.

De besturing van de sleutelinrichting SAF voor het opwekken van de sleutelteksten gebeurt via een klokschakeling. Bij elk klok-tijdincrement kan hierbij een nieuwe sleuteltekst
25 gegenereerd en in de buffergeheugens 1 en 2 opgeslagen worden. Het is echter ^{ook} mogelijk, ^{slechts} om op het ondervraagtijdstip de klok-tijd op de sleutelinrichtingen in te laten werken; de sleuteltekst kan dan met het ondervraagsignaal stapvormig opgewekt worden.

C o n c l u s i e s

1. Inrichting voor vriend-vijand identifikatie onder toepassing van gecodeerde ondervragingen en antwoorden in samenhang met een ondervraaginrichting van de ondervragende post en met een transponder van de ondervraagde post, en met een radiotelefonie-inrichting voor de overdracht van versleutelde berichten tussen de ondervragende en de ondervraagde post, met het kenmerk, dat voor de storingsbestendige IFF-overdracht onder medegebruik van^{de} inrichtingen of delen van de inrichtingen van een storingsbestendig uitgevoerde radiotelefonie-inrichting (SF1, SF2), de overdracht van het antwoord (kenteken) van de ondervraagde post volgens de frequentiesprongwerkwijze via de radiotelefonie-inrichting (SF1) zodanig gebeurt, dat de ondervragende post (AF) als ondervraging een vast, aan de ondervraagde post bekend versleuteld codewoord tezamen met een versleuteld, een frequentie-adres bevattend, variabel gegevensdeel uitzendt, en gelijktijdig de antwoordontvanger van de radiotelefonie-inrichting (SF2) van deze post op de zendfrequentie van het te verwachten antwoord van de ondervraagde post instelt, en dat de ter beschikking stelling van de zendfrequenties van de ondervraagde post met behulp van een door het frequentie-adres gestuurde frequentiesyntetiseerschakeling gebeurt, en dat op een eerste antwoord van geringe redundantie wanneer nodig, een genummerd tweede antwoord met grote redundantie na elkaar op meerdere verschillende frequenties uitgezonden wordt.

2. Inrichting voor vriend-vijand identifikatie volgens conclusie 1, met het kenmerk, dat het variabele gegevensdeel in samenhang met een voor langere tijd geldige sleuteltekst (b.v. meerdere sekonden) voor de vorming van frequentie-adressen^{en} Voor de versluiering van het antwoord dienen.

3. Inrichting voor vriend-vijand identifikatie volgens conclusie 1 of 2, met het kenmerk, dat de versleuteling van ondervraging en antwoord in quasi-synchrone sleutelapparaten, die bijvoorbeeld door klokken (U1, U2) van beperkte nauwkeurigheid gestuurd zijn, in de ondervragende post (AF) en in de transponder gebeurt.

8005672

4. Inrichting voor vriend-vijand identifikatie volgens één der voorgaande conclusies, m e t h e t k e n m e r k , dat de versleuteling van ondervraging en antwoord bij quasi-synchrone sleutelapparaten door een start-stop bedrijf van de 5 sleutelapparaten (5, 10) gebeurt, doordat per tijdincrement (sek. tot millisek.) een nieuwe sleuteltekst opgewekt en opgeslagen wordt.

5. Inrichting voor vriend-vijand identifikatie volgens één der voorgaande conclusies, m e t h e t k e n m e r k , dat 10 de versleuteling door wisseling van het variabele gegevensdeel van ondervraging tot ondervraging veranderd wordt.

6. Inrichting voor vriend-vijand identifikatie volgens één der voorgaande conclusies, m e t h e t k e n m e r k , dat voor de ontsleuteling van het ondervraagssignaal telkens drie 15 sleutelteksten simultaan gebruikt worden.

7. Inrichting voor vriend-vijand identifikatie volgens één der voorgaande conclusies, m e t h e t k e n m e r k , dat het variabele gegevensdeel in een foutonderscheidingsinrichting (3) van de transponder op overdrachtfouten onderzocht 20 wordt.

8. Inrichting voor vriend-vijand identifikatie volgens één der voorgaande conclusies, m e t h e t k e n m e r k , dat voor het afgeven van een IFF-antwoord van de transponder een instelinformatie voor de frequentiesyntetiseerschakeling, een 25 informatie voor de versluiering van het kenteken en een zendinstructie aan de radiotelefonie-inrichting (SF1) afgegeven worden.

9. Inrichting voor vriend-vijand identifikatie volgens één der voorgaande conclusies, m e t h e t k e n m e r k , dat 30 in de transponder een lineair teruggekoppeld schuifregister (4) aangebracht is, waarvan de startinformatie van het variabele gegevensdeel van de ondervraging en eventuele gedeelten van de bijbehorende sleuteltekst afgeleid is.

10. Inrichting voor vriend-vijand identifikatie volgens één 35 der voorgaande conclusies, m e t h e t k e n m e r k , dat door gedefiniëerde klokpulsen van het teruggekoppelde schuifregister (4) het frequentie-adres en de informatie voor de

8005672

versluiering van het antwoord (kenteken) verkregen en aan het radiotelefonie-apparaat (SF1) voor de afgifte van het antwoord toegevoerd worden.

11. Inrichting voor vriend-vijand identifikatie volgens één
5 der voorgaande conclusies, m e t h e t k e n m e r k , dat het teruggekoppelde schuifregister (4) voor het opwekken van een groot aantal kentekens op verschillende frequenties (tweede antwoord) meervoudig met een klokpulsreeks bestuurd wordt.

12. Inrichting voor vriend-vijand identifikatie volgens één
10 der voorgaande conclusies, m e t h e t k e n m e r k , dat met de door de verwerkingstijd van het ondervraagssignaal in de transponder ontstane vertragingstijden bij de decodering van de antwoorden in de ondervragende post rekening gehouden wordt.

8005672

1/3

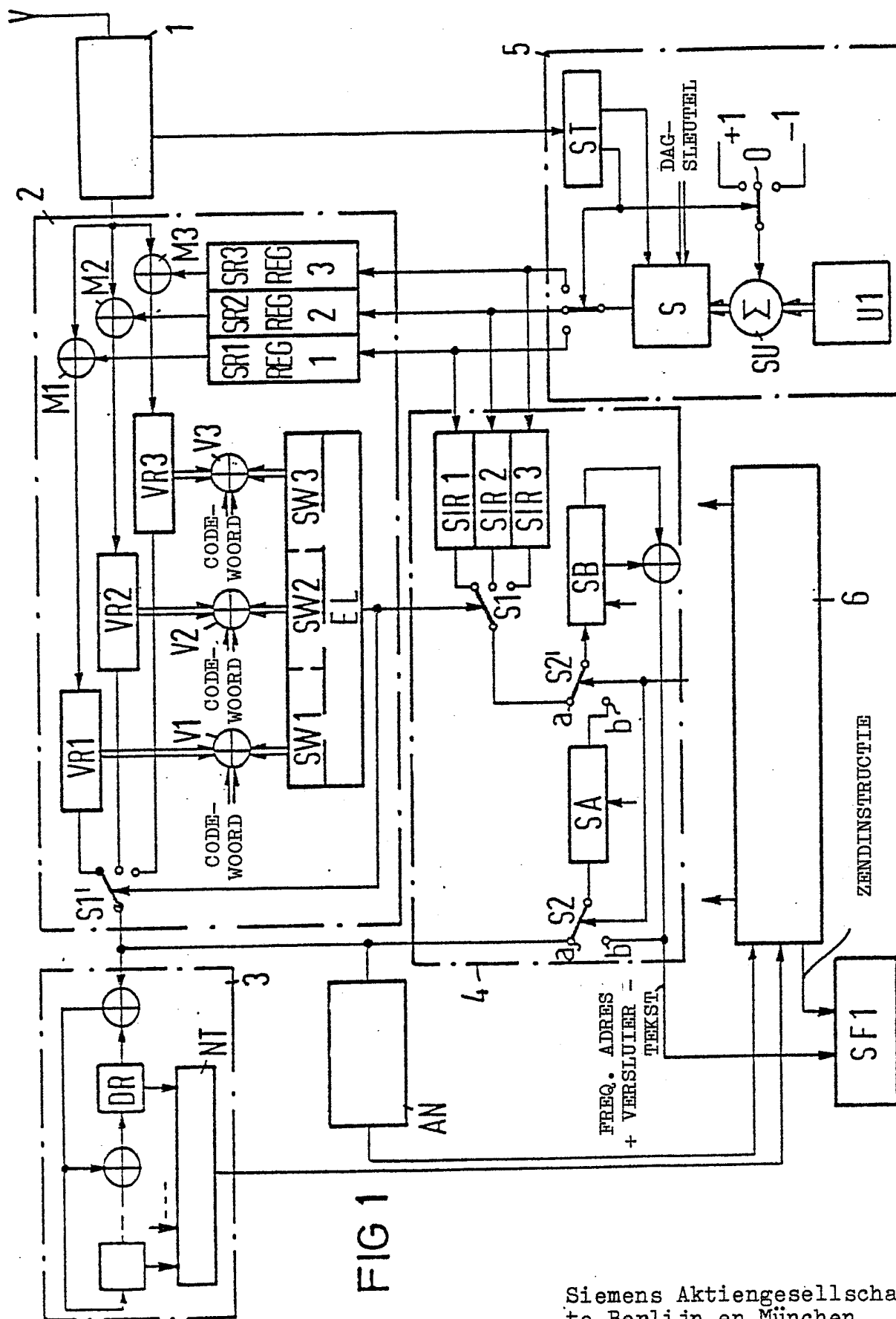


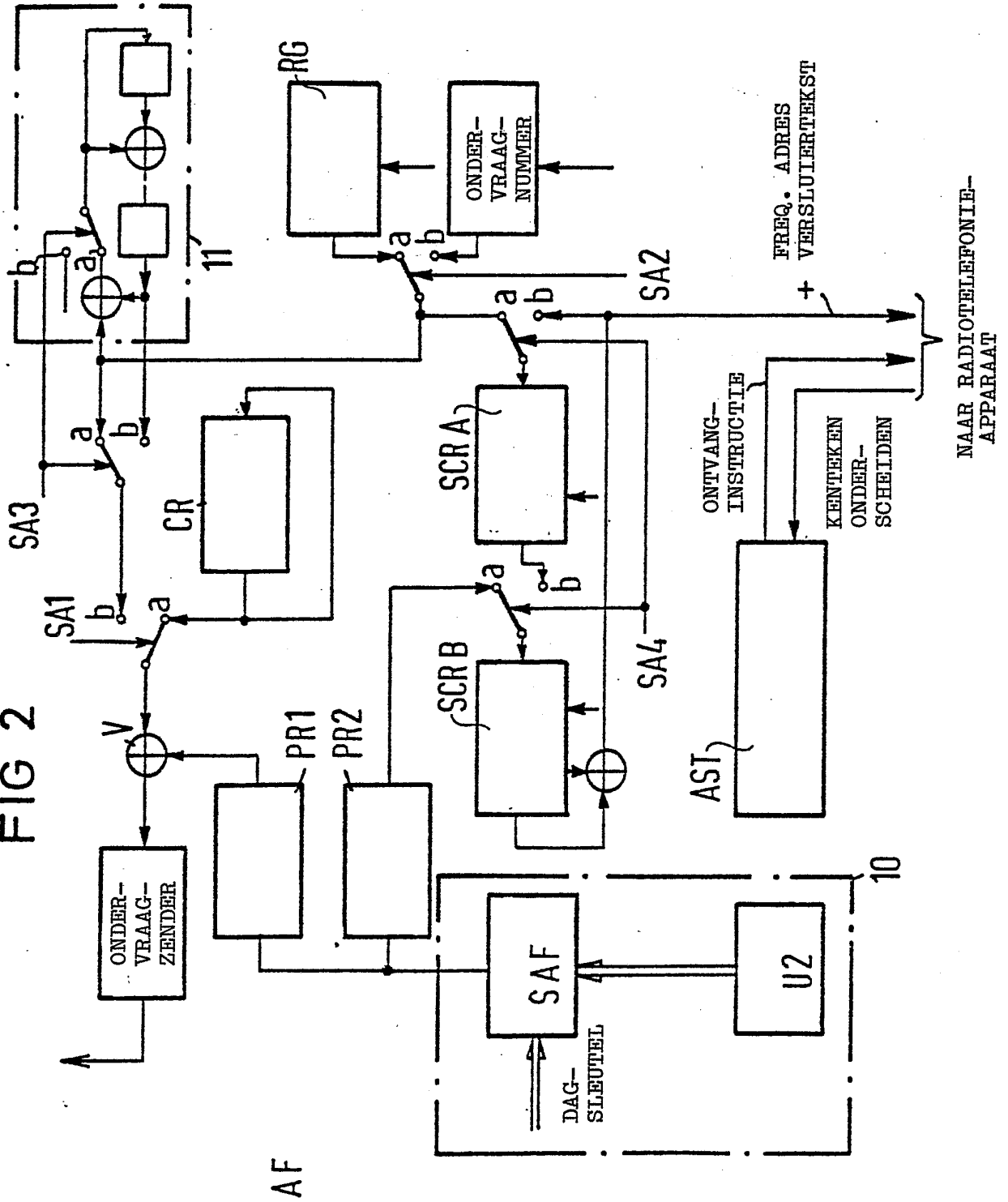
FIG 1

Siemens Aktiengesellschaft
te Berlin en München

8005672

2/3

FIG 2

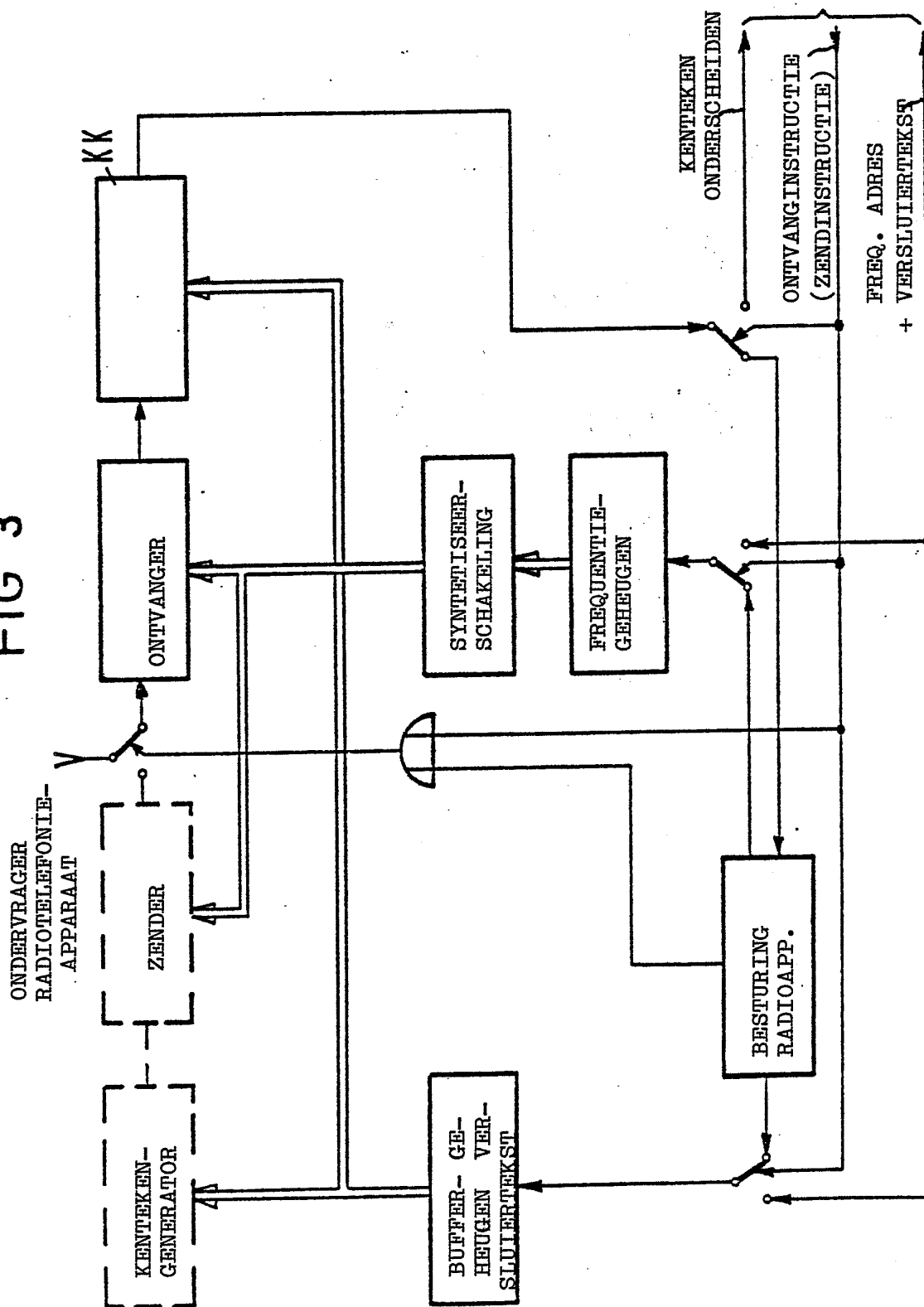


8005672

Siemens Aktiengesellschaft
te Berlin en München

8005672

FIG 3



3/3

SF 2

Siemens Aktiengesellschaft
te Berlijn en München

3 bladen
blad 3