NORGE [B] (11) **UTLEGNINGSSKRIFT** Nr. 129227

STYRET
FOR DET INDUSTRIELLE
RETTSVERN

(51) Int. Cl. H 04 1 9/04

(52) Kl. 21a[1]-21

(21) Patentsøknad nr. 147.772
(22) Inngitt 5.3.1963
(23) Løpedag 5.3.1963
(41) Søknaden alment tilgjengelig fra 11.4.1973
(44) Søknaden utlagt og utlegningsskrift utgitt 11.3.1974
(30) Prioritet begjært fra: 6.3.1962 Nederland, nr. 275586

(71)(73) Philips USFA N.V.,
Schouwbroekseweg 49,
Eindhoven, Nederland.

(72) Roelof Maarten Marie Oberman,
17 Van Pabstlaan, Voorburg og
Antonie Snijders, 28 Enschedelaan
's-Gravenhage, begge: Nederland.

(74) Siv.ing. Kjell Gulbrandsen.

(54) Anordning til behandling av tilstanden for elementgrupper.

Foreliggende oppfinnelse angår en anordning til behandling av den binære tilstand av en gruppe nøkkelelementer, forsynt med en leseanordning for hvert element og forsynt med koplinger som kan styres av leseanordningene, og ved hvis utganger det fremkommer et "null" eller et "en" signal, alt etter tilstanden av det tilhørende element og der inngangen til en kopling er tilsluttet en signalkilde som er i stand til å sende et "null" eller et "en" signal.

En slik anordning er kjent fra det arbeidsområde det her er tale om og anvendes i chiffreringsmaskiner.

I den kjente maskin benyttes signalet som fremkommer ved utgangen av hver av koplingene som en nøkkel for koding og dekoding.

Inngangen til hver av koplingene er forbundet med signalkilden og det signal som fremkommer ved utgangen for hver kopling, er en angivelse av de tilstander det tilhørende nøkkelelement gjennomgår når det beveger seg trinnvis.

Dette kan vise seg å være en ulempe, fordi det kan føre til at hvert enkelt element kan gjenkjennes. Forsøk er blitt utført med å oppheve denne ulempe ved først å styre signalene som fremkommer ved koplingenes utganger, til en kommutator, slik at utgangene fra koplingene byttes om før signalene anvendes som nøkkel.

Når dette gjøres kan kommutatoren bevege seg trinnvis på samme måte som et nøkkelelement eller sammen med et nøkkelelement.

En anordning som benytter slik kommutator er komplisert og vanskelig å holde vedlike. I tillegg til dette vil det heldige resultat man kan oppnå med anordningen, være avhengig av at kommutatorens bevegelse ikke kan gjenkjennes.

Ved oppfinnelsen anvendes det ikke noen slik kommutator, og den ovennevnte ulempe oppheves på en måte som er enkel og lett å utføre, og oppfinnelsen er kjennetegnet ved at signalet som fremkommer ved utgangen av den siste kopling, inverteres ved en tilstandsforandring i et vilkårlig element.

Dette kan oppnås på en enkel måte ved å summere tilstandene for de to elementer som avleses av modul-2-anordningene.

Ved dette vil påvirkningen av alle elementene på nøklingen bli den samme, det vil si at hvert element er i stand til å forandre sin nøkkel f.eks. fra "null" til "en" ved å endre sin tilstand uavhengig av tilstandene for de andre elementer. Gjenkjennelsen av hvert enkelt separat element vil derfor være praktisk talt umulig, og oppfinnelsen blir enkel og lett å holde i orden.

Anordningen har den ytterligere fordel, slik det fremgår tydelig av de utførelsesformer som beskrives i det følgende, at den lett kan utvides med samme type elementer uten at det blir vanskelig å ha den nødvendige oversikt.

En utførelsesform for anordningen i henhold til oppfinnelsen er kjennetegnet ved at koplingene er forbundet i serier, og at det som koplinger fortrinnsvis benyttes modul-to-kretser.

Det er imidlertid også mulig å anordne modul-to-kretsene

i noen forskjellige grupper, slik at man får en modul-to-krets for dette formål styrt av to leseanordninger fra to modul-to-kretser eller av en modul-to-krets og en leseanordning.

Ved denne utførelsesform kan påtrykningstiden for tilstanden i nøkkelelementene være kortere enn ved en seriekopling.

Utførelsesformen for oppfinnelsen er kjennetegnet ved at koplingene er vendere som har bipolare innganger og bipolare utganger og at inngangen for den vender som styres av den første leseanordning blir koplet til utgangen fra signalkilden via en vender med en bipolar utgang og ved at leseanordningen kan kople inngangen for hver vender til dens utgang enten i kryss eller rett gjennom.

Nok en utførelsesform er kjennetegnet ved at hver leseanordning er koplet til en inngang av en av et antall "OG" portkretser som på sin side blir koplet i serie med hensyn til tiden ved at deres andre innganger syklisk og etter tur blir koplet til signalkilden og hvis utganger er koplet sammen og til inngangen for en binær enhetsteller som ved sin utgang er koplet til en anordning som utløser signalet etter hver syklus.

Det er klart at de ovennevnte utførelsesformer ikke på noen måte må betraktes som begrensende oppfinnelsens omfang.

Oppfinnelsen skal i det følgende forklares nærmere under henvisning til tegningene der de ovennevnte utførelsesformer er gjengitt skjematisk og der:

Fig. 1 viser en anordning med modul-to-kretser som er koplet i serie,

fig. 2 viser en modul-to-krets anvendt i fig. 1,

fig. 3 viser en anordning med modul-to-kretser som er styrt av to anordninger og to modul-to-kretser,

fig. 4 viser en symmetrisk utførelsesform for den anordning som er vist på fig. 3,

fig. 5 viser en anordning som kan sammenliknes med fig. 1 for samtidig chiffrering og dechiffrering av samtlige elementer i et symbol fra et alfabet med fem enheter,

fig. 6 viser en utførelsesform for anordningen med vendere og

fig. 7 viser en anordning med "OG" portkretser som er koplet i serie med hensyn til tiden.

På disse figurer betegner like henvisningstall like komponenter.

På fig. 1 betegner tallene 1,2,3 og 4 nøkkelelementer som kan beveges i trinn på en uregelmessig måte, og som kan innta et ulike antall tilstander, hvilke tilstander enten er "null" eller "en".

Leseanordningen 9,10,11 og 12 leser eller avsøker tilstandene for elementene 1,2,3 og 4.

Leseanordningene 9,10,11 og 12 styrer koplingene 41,42,43 og 80 som her er utført som modul-to-kretser.

Modul-to-kretsen er koplet til en signalkilde 44 ved hjelp av en bryter 81.

Kilden 44 som ved den viste utførelsesform er betegnet som et jordsymbol, kan i prinsippet sende et signal som enten er et "null" signal eller et "en" signal.

Ved de modul-to-kretser som her anvendes (se fig. 2), betraktes en nullspenning eller jord koplet til inngangen 128 eller A som et "en" signal, mens en negativ spenning eller en åpen klemme ved 128 eller A oppfattes av modul-to-kretsen som om et "null" signal var blitt sendt.

Modul-to-kretsen 80 er koplet til en utgangsklemme 82.

Elementene 1,2,3 og 4 beveger seg i trinn på en uregelmessig måte når anordningen er i drift.

Her kan man anta at bryteren 81 på et bestemt tidspunkt slutter kretsen, og at kilden 44 sender en "en" til modul-to-kretsen 41.

Videre antar man at anordningen 9 leser et "null" og sender dette null videre til en modul-to-krets 41. En "en" vil da likeledes fremkomme ved utgangen av kretsen 41, hvilken "en" så vil føres videre til inngangen for kretsen 42.

Hvis nu anordningen 10 på elementet 2 leser et ytterligere "null", vil en "en" fremkomme ved utgangen av kretsen 42.

Hvis imidlertid anordningen 10 leser en "en", vil et "null" fremkomme ved utgangen av kretsen 42, noe som også vil være tilfellet hvis anordningen 9 hadde lest en "en" og anordningen 10 hadde lest et "null".

På denne måte kan man fortsette, idet utgangen fra hver modul-to-krets alltid fremkommer som et "null" eller en "en" alt etter tilstanden for de tilsvarende elementer og tilstanden for foregående elementer.

Ved å bygge inn vendeinnretninger kan tilstanden for et bestemt element eller tilstandene for ett eller flere elementer om det ønskes, vendes om.

Hvert av elementene for nøkkelen S som fås ved utgangsklemmen 82, kan nu kombineres med et element fra en tekst K for å danne et element i en kryptotekst C i henhold til formelen:

$$S - K = C$$

Klarteksten K kan innføres i kretsen, f.eks. som skjematisk vist ved bryteren 81 som kan bryte og slutte kretsen for dette formål.

Ved hver puls fra en pulsgenerator som ikke er vist og som styrer den trinnvise bevegelse av nøkkelelementene 1,2,3 og 4, bestemmes det så av elementene i klarteksten som skal sendes, om bryteren 81 skal brytes eller slutte.

Dechiffrering kan foretas i henhold til formelen:

$$S - C = K$$

Nu bestemmer elementet i kryptoteksten om bryteren 81 skal bryte eller slutte kretsen. På denne måte kan anordningen påtrykke tilstanden på nøkkelelementene for å danne en nøkkel, en kryptotekst eller en klar tekst, alt etter ønske. Tekstene fremkommer ved utgangsklemmen 82.

Det er mulig å utvide anordningen ganske enkelt ved å føye til ett eller flere sett som hvert omfatter et nøkkelelement, en leseanordning og en modul-to-krets. På tegningen er settene 100, 101, 102 og 103 for tydelighets skyld vist omrammet med stiplede linjer.

Fig. 2 viser en utførelsesform for en modul-to-krets. Inngangen A er alltid tilkoplet den foregående modul-to-krets, mens utgangen B er koplet til den etterfølgende krets.

Utgangen fra leseanordningen 10 er også koplet til en modul-to-krets.

Hvis inngangen A og utgangen fra anordningen 10 begge enten viser en "en" eller et "null", vil et null fremkomme ved utgangen B. Hvis på den annen side inngangen A ikke viser samme signal som utgangen fra anordningen 10, vil en "en" fremkomme ved utgangen fra modul-to-kretsen.

På fig. 3 vises en anordning med fire nøkkelelementer 1, 2, 3 og 4, og deres tilstander avsøkes av fire anordninger 9,10,11 og 12.

Anordningene 10 og 11 styrer modul-to-kretsen 125.

Modul-to-kretsen 125 summerer tilstanden for elementene 2 og 3.

Modul-to-kretsen 126 styres på sin side av modul-to-kretsene 124 og 125, og ved utgangen 82 for anordningen får man resultatet av de modul-to summerte tilstander for elementene 1 til og med 4.

Fig. 3 viser videre et skifteregister 132. Inngangen 130 til skifteregisteret 132 er koplet til anordningens utgang 82, og utgangen 131 er koplet til inngangen 128 for anordningen.

Hvis ved denne anordning et klart symbol innføres i skifteregisteret på kjent måte, kan symbolet chiffreres til et kryptosymbol som deretter fremkommer over skifteregisteret i stedet for det klare symbol.

For å tydeliggjøre den følgende forklaring kan det antas at alle fire nøkkelelementer flytter seg i trinn regelmessig og i urviserretningen, og at et klart symbol (01001) er blitt innført i skifteregisteret 132.

I praksis vil imidlertid nøkkelelementene vanligvis ikke bevege seg regelmessig i trinn og heller ikke beveger alle seg i samme retning.

Den høyre del av det klare symbol fra registeret, "en" tilføres modul-to-kretsen 124 sammen med "null" tilstanden for det første nøkkelelement.

Et "en" signal vil da fremkomme ved utgangen for kretsen 124. Som en følge av "null" tilstanden for elementet 2 og tilstanden "en" for elementet 3 vil et "en" signal også fremkomme ved utgangen for kretsen 125.

Kretsen 126 vil da sende et "null" signal til kretsen 127, fordi kretsen 127 er blitt tilført to "en" signaler.

Ved utgangsklemmen 82 fremkommer så et "null" signal som føres tilbake til skifteregisteret og der lagres i dettes venstre del.

Symbolet i skifteregisteret er nu blitt til (00100), og som er resultat av den ovennevnte regelmessige trinnvise forflytning fremover, vil tilstandene for samtlige fire nøkkelelementer være en "en".

Den høyre del av dette symbol blir så chiffrert med tilstandene i elementene, og dette resulterer igjen i et "null" signal ved utgangen 82, slik at symbolet i registeret nu vil være (00010).

På den tid da samtlige fem elementer i den egentlige tekst

er blitt chiffrert, vil kryptosymbolet (00100) ha fremkommet i skifteregisteret.

Det skulle være klart at symbolet i den klare tekst kan omdannes fra kryptosymbolet på en tilsvarende måte.

Arrangementet med et skifteregister ble valgt som en løsning som er særlig hensiktsmessig for chiffrering. Chiffreringen kan imidlertid utføres med anordningen i henhold til oppfinnelsen på mange andre måter.

Fig. 4 viser en symmetrisk utførelsesform for den anordning som er vist på fig. 3, og denne utførelsesform er meget enkel og rett frem. Det skulle være klart at de anordninger som er vist på figurene i forbindelse med fire nøkkelelementer, alltid kan utvides.

På fig. 5 er det vist en anordning som er hensiktsmessig for samtidig innføring av symboldelene i et alfabet med fem enheter. På denne figur er hvert nøkkelelement forsynt med en rekke anordninger slik at de kodede eller dekodede symboler fra femenhetsalfabetet på en gang fremkommer ved endeklemmene 82_1 ..... til 82_5.

Figuren trenger ingen ytterligere forklaring.

En "en" i symbolet som på fig. 5 fører til at bryteren 81 bryter, kan også omformes slik at den vil få bryteren 81 til å slutte den tilhørende krets. I prinsippet kan en omformeranordning innbygges på et hvilket som helst sted i kretsen.

Fig. 6 viser en anordning som arbeider med vendere.

Anordningen 9,10,11 og 12 styrer venderne på en slik måte at inngangsklemmene koples til utgangsklemmene enten i kryss eller rett gjennom.

Ved utgangsklemmene 62 eller 82' vil man da få signaler som er mottatt på de to klemmer.

Fig. 7 viser en anordning der tilstandene for nøkkelelementene avsøkes etter tur og frigjøres ved utgangen etter modul-to-summering.

Anordningen har igjen fire nøkkelelementer 1,2,3 og 4, med en "null"-"en" del.

Anordningene 9,10,11 og 12 fører tilstandene i nøkkelelementene 1,2,3 og 4 til "OG" portkretsene 65,66,67 og 68. Kilden 44 vil, alt etter hvorledes den er innstilt, sende et signal som enten kan være et "null" eller en "en" og er koplet til portkretsene 65,66,67 og 68 via en drevet deleinnretning 70.

Portkretsene 65,66,67 og 68 er koplet i serie med hensyn

til tiden, idet de koples syklisk den ene etter den annen, til signalkilden 44. Hvis nu signalkilden sender en "en" og leseanordningen 9 leser en "en" i det første element 1, da vil portkretsen 65 bryte og ved utgangen fra denne portkrets 65 vil man få et "en" signal.

I alle de andre tilfeller vil et "null" signal fremkomme ved utgangen for "OG" portkretsen, det vil si i alle de tilfeller der den ene av de to, enten nøkkelelementet eller kilden eller begge sender et "null".

Utgangen fra "OG" portkretsen 65 er koplet til inngangen for en binær enhetsteller 69.

Hvis den binære enhetsteller 69 viste at et "null" og en "en" fremkom ved inngangen, ville en "en" fremkomme ved tellerens utgang. Hvis på den annen side den binære enhetsteller 69 ved sin inngang hadde en "en" og en "en", ville et "null" fremkomme ved utgangen. Hvis et "null" fremkommer ved inngangen, vil den binære enhetsteller 69 forbli i den tilstand den har.

Som man vil se blir "OG" portkretsen 65,66,67 og 68 koplet syklisk, den ene etter den annen, til kilden 44, og ved dette vil den binære enhetsteller 69 alt etter tilstanden for elementene, skifte, eller den vil la vær å skifte.

Den binære enhetsteller 69 vil således summere utgangssignalene fra "OG" portkretsene sammen etter modul-to-prinsippet.

Den binære enhetsteller 69 er tilkoplet en utløserkrets 110 som etter at en syklus er ferdig og før en ny syklus starter, får tilført en puls ved C som bevirker videreføring av den tilstand den binære enhetsteller har til anordningens utgangsklemme 82.

Den tilstand som føres videre, vil alltid være et "null" signal eller et "en" signal. Den representerer summen av modul-to-addisjonen av tilstandene for elementene 1,2,3 og 4.

Kryptoteksten eller den normale tekst kan tilføres til "OG" portkretsen 83 ved 81 i form av et signal "en" eller "null". Armen 71 i deleinnretningen 70 forbinder alltid portkretsen 83 med kilden 44 før avslutning av en syklus. Hvis det signal som sendes av tekstdelen, og det signal som sendes av kilden, begge er "en" vil portkretsen 83 åpne , og vil sende en "en" til den binære enhetsteller 69. Delene av teksten vil her påvirke den binære enhetsteller 69 på samme måte som nøkkelelementene 1,2,3 og 4 ved hjelp av de ovennevnte portkretser 65,66,67 og 68.

129227

Patentkrav.

1. Anordning til behandling av den binære tilstand ("null" eller "en") av en gruppe nøkkelelementer (1-4), forsynt med en leseanordning (9-12) for hvert element og forsynt med koplinger (41-43, 80) som kan styres av leseanordningene, og ved hvis utganger det fremkommer et "null" eller et "en" signal, alt etter tilstanden av det tilhørende element og der inngangen til en kopling er tilsluttet en signalkilde (44, 81) som er i stand til å sende et "null" eller et "en" signal, k a r a k t e r i s e r t v e d at anordningen er forbundet slik at signalet som fremkommer ved utgangen (82) fra den siste kopling (80) inverteres ved en forandring i tilstanden av et vilkårlig element.

2. Anordning som angitt i krav 1, k a r a k t e r i s e r t v e d at hver av koplingene er modul-to-kretser og styres av to leseanordninger (10, 11), av to modul-to-kretser (124, 125) eller av en modul-to-krets og en leseanordning (fig. 3).

3. Anordning som angitt i kravene 1 eller 2, k a r a k t e r i s e r t v e d at koplingene er vendere med bipolare innganger og bipolare utganger, og at inngangen for den vender som styres av den første leseanordning blir koplet til utgangen fra signalkilden via en vender med en bipolar utgang og at leseanordningene kan kople inngangen for hver vender til dens utgang enten i kryss eller rett gjennom.

4. Anordning som angitt i krav 1, k a r a k t e r i s e r t v e d at hver av leseanordningene er koplet til en inngang av en av et antall "OG" portkretser (65-68) som blir koplet i serie med hensyn til tiden ved at deres andre innganger syklisk og etter tur blir koplet til signalkilden, og hvis utganger er koplet sammen og til inngangen for en binær enhetsteller (69) som ved sin utgang er koplet til en innretning som utløser signalet etter hver syklus.

(56) Anførte publikasjoner: Ingen.

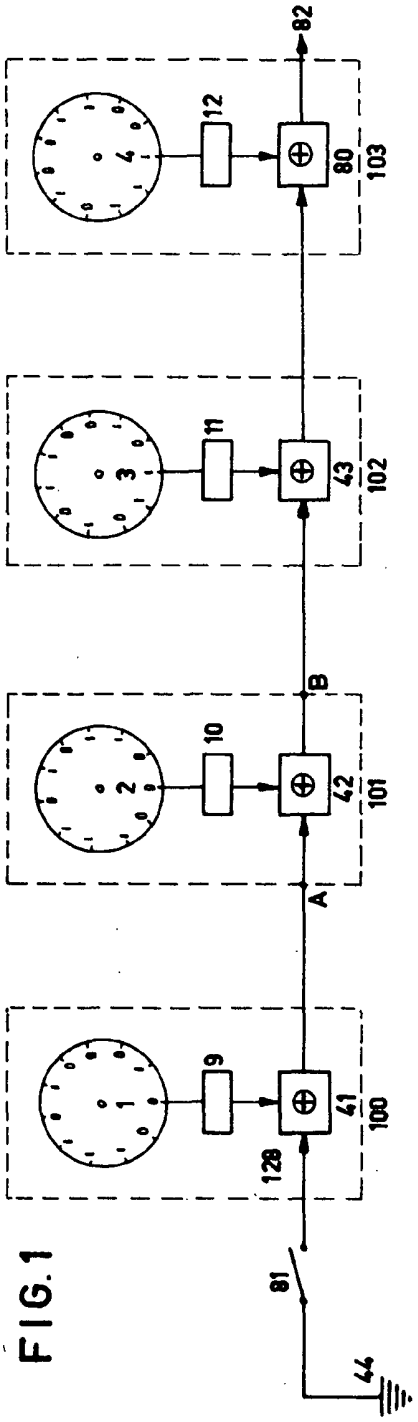
82
12
4
80
103
11
3
43
102
B
10
2
42
101
A
9
1
41
100
128
81
44

FIG.1

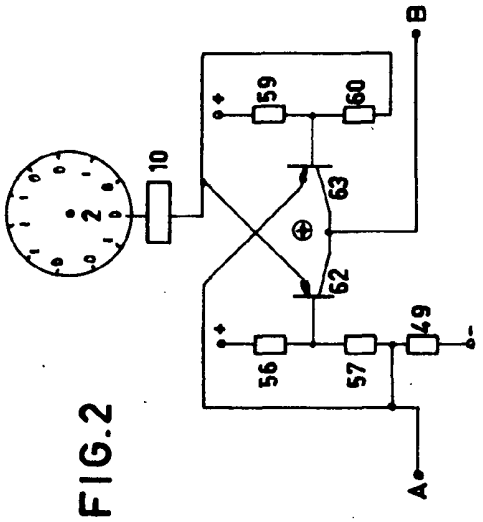
B
59
60
10
2
63
62
49
56
57
A

FIG.2

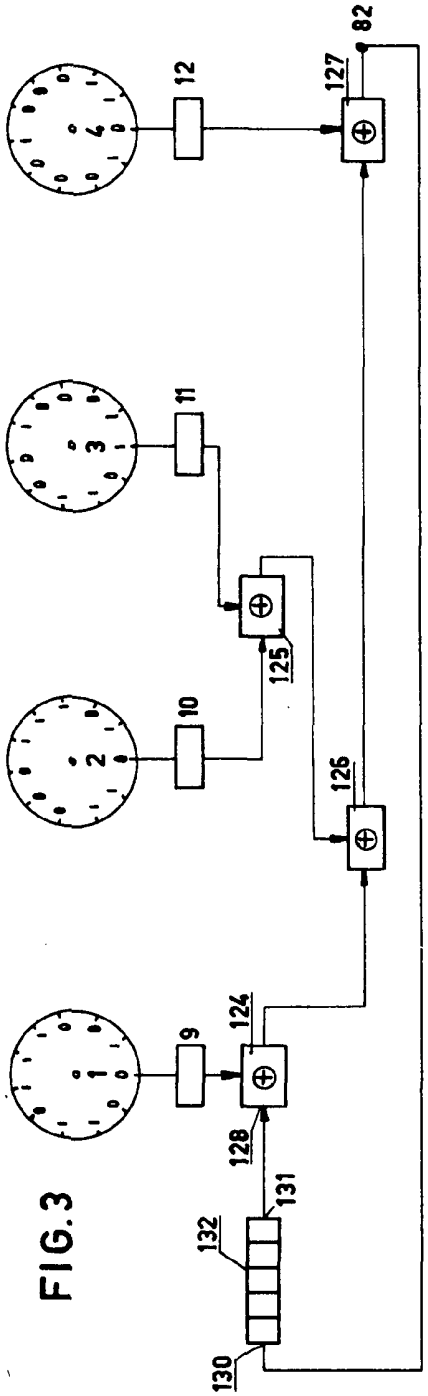
82
12
127
11
10
125
126
9
124
128
131
132
130

FIG.3

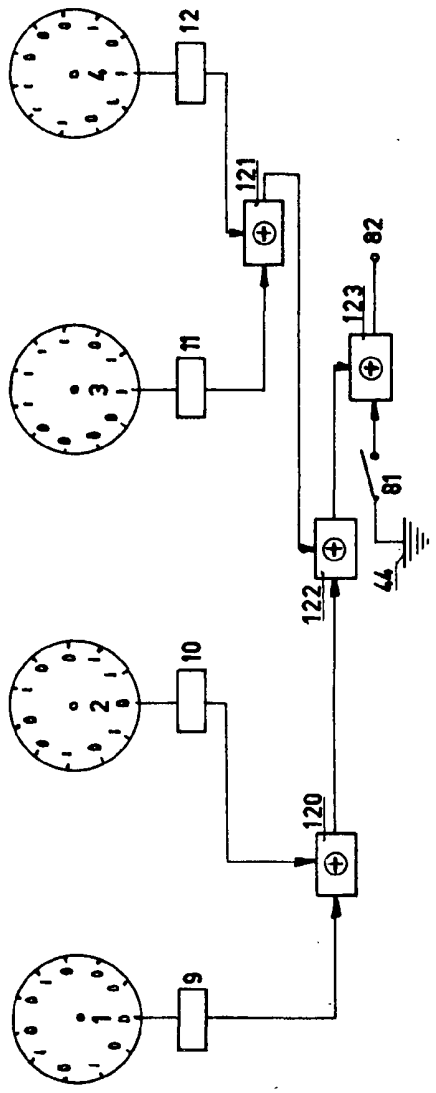
12
121
82
11
123
81
10
122
44
120
9

FIG.4

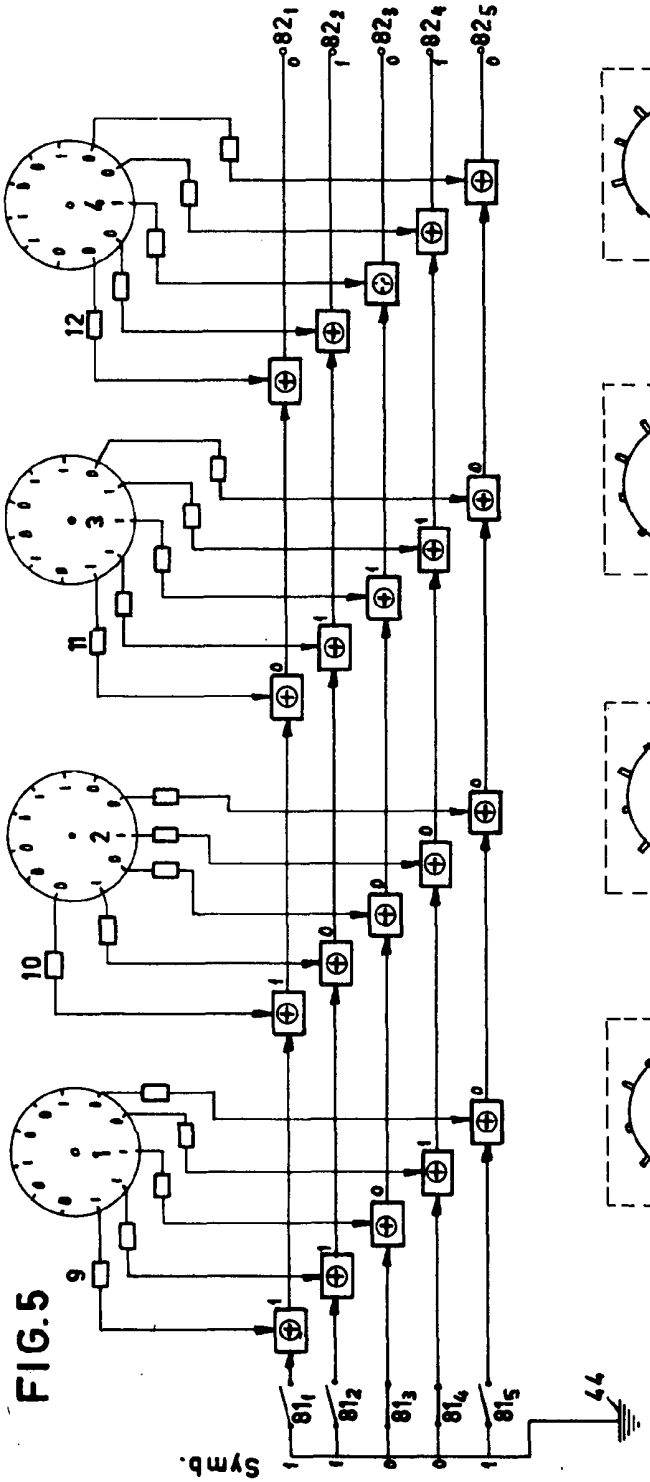
82_1
82_2
82_3
82_4
82_5
4
12
3
11
2
10
1
9
81_1
81_2
81_3
81_4
81_5
44
Symb.

FIG.5

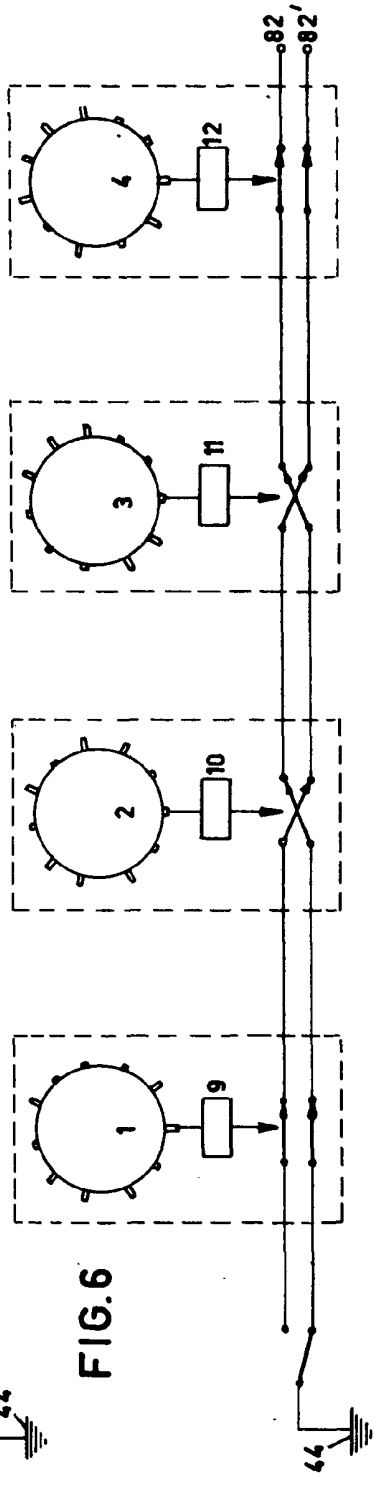
82
82'
4
12
3
11
2
10
1
9
44

FIG.6

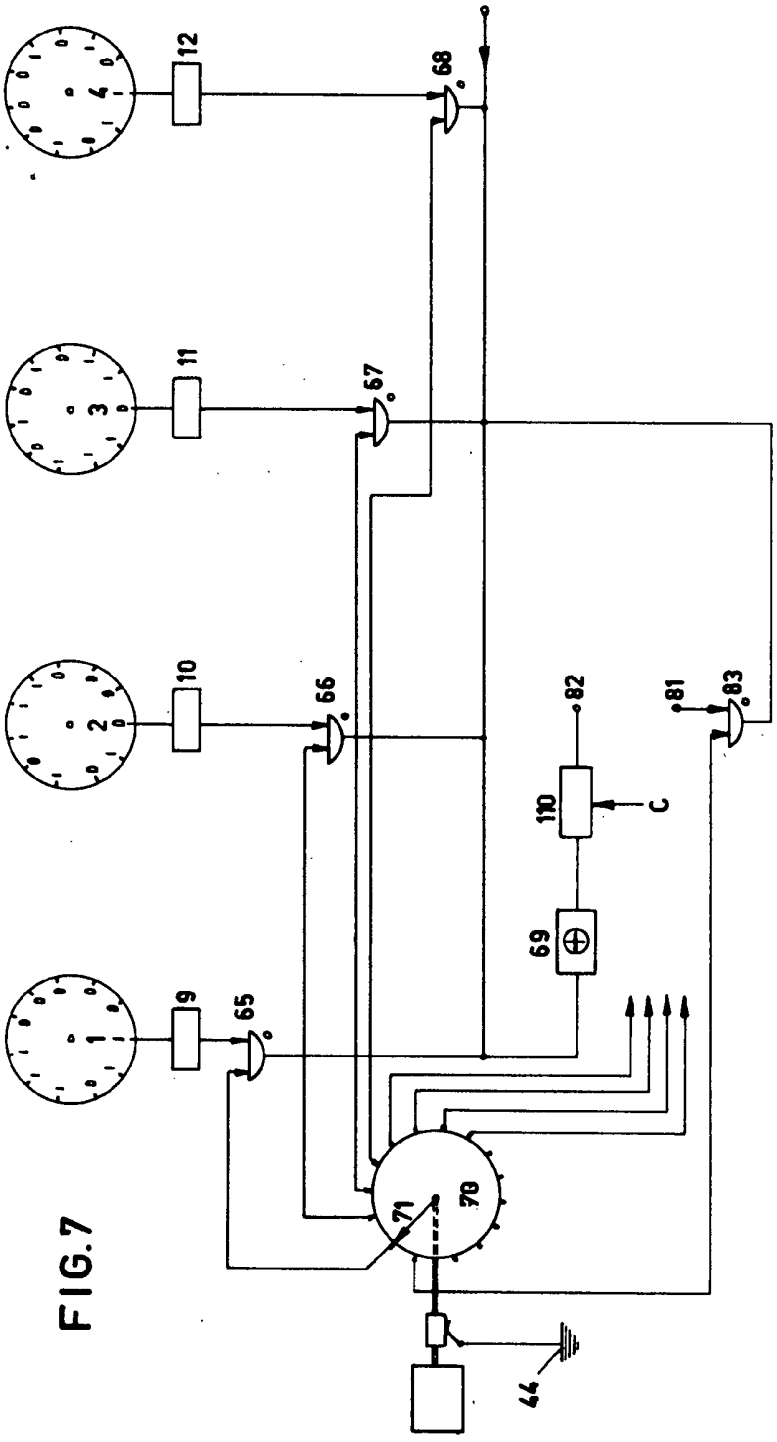

FIG.7