



NORGE

(19)[NO]

STYRET
FOR DET INDUSTRIELLE
RETTSVERN

Må ikke fjernes

[C] (11) Patent nr. **113572**

(51) Int. Cl⁸ H 04 L 9/04

(21) Patentsøknad nr. 144575

(22) Inngitt 30.05.62

(24) Løpedag 30.05.62

(45) Patent meddelt 13.02.70

Offentliggjort: 11.02.85

(30) Prioritet begjært 31.05.61, Nederland, nr. 265358

(54) Oppfinnelsens benevnelse **KOMMUNIKASJONSSYSTEM FOR OVERFØRING AV
HEMMELIGE MELDINGER.**

(73) Patenthaver **NEDERLANDSE ORGANISATIE VOOR TOEGPAST-NATUUR-
WETENSCHAPPELIJK ONDERZOEK TEN BEHOEVE VAN DE
RIJKSVERDEDIGING,
Haag,
Nederland.**

(72) Oppfinner **RUDOLF SLEGTENHORST,
Wassenaar,
Nederland.**

(74) Fullmerktig **Siv.ing. Kjell Gulbrandsen,
Bryns Patentkontor A/S, Oslo.**

(56) Anførte publikasjoner **Ingen.**

Foreliggende oppfinnelse angår et kommunikasjonssystem for hemmelig overføring av meldinger der det for koding av meldingene som består av numerisk kodede signaler hvorav hvert signal er dannet av en gruppe kodeelementer med bestemte verdier, benyttes et interferensmønster som er kjent både av sender og mottaker, og som omfatter et begrenset antall kodeelementer som er anordnet i henhold til samme tidsramme som kodetruppene i den egentlige melding.

Et slikt system er kjent fra Britisk patent nr. 694.757.

Interferensmønsteret som benyttes i denne oppfinnelse, frembringes ved hjelp av et antall elektroniske kretser som arbeider syklisk. Fordi disse syklisk arbeidende elektroniske kretser er en analogi til et roterende hjul, betegnes disse kretser som elektroniske hjul.

Hvert av disse hjul har et antall stillinger. Dette antall kan være forskjellig for hvert av hjulene, og hvis så er tilfellet, bør antallene fortrinnsvis ikke ha noen felles divisor. Hvert elektronisk hjul frembringer et innstillbart null-én mønster, der antall enere i mønsteret lagt til antall null er lik det antall stillinger hjulet har. Disse mønstre kalles undermønstre.

En vanlig fremgangsmåte består i å summere opp undermønstrene ved hjelp av en logisk krets i henhold til reglene: et like antall enere betraktes som null, mens et ulike antall enere betraktes som en ener. Det mønster man får ved denne addisjon benyttes som interferensmønster både når samtlige hjul beveger seg regelmessig i trinn uavhengig av hverandre, da antallene av stillinger er forskjellige, og når trinnbevegelsen av noen av hjulene bestemmes av den tilfeldige kombinasjon av enere og null i de undermønstre hjulene frembringer.

En annen kjent metode består i å benytte kombinasjoner av enere og null fra de hjul som beveger seg uavhengig av eller avhengig av hverandre som justeringskombinasjonen for en hjelpeanordning som frembringer symbolene for interferensmønstre.

Anvendelsen av et slikt interferensmønster har to ulemper som begge skyldes det faktum at interferensmønstrene i senderen og mottakeren må passere gjennom et likt antall stillinger hvis mottakeren skal være i stand til å dechifrere meldingen.

113572

Den første ulempe er at en elektronisk arbeidende mottaker ikke inneholder noen korrekte data om antall stillinger som har passert hvis tilførselsspenningen et øyeblikk er blitt slått av, eller hvis forstyrrende pulser har stilt et eller flere av de elektroniske hjul i en gal stilling.

Den annen ulempe er at alle abonnenter som tar del i kommunikasjonsnettverket for hemmelige sendere må starte samtidig og gå gjennom stillingene for interferensmønstret, og de må alle starte ut fra identiske startstillinger.

Det ville være mulig delvis å fjerne disse ulemper ved å innføre en nullstillingskodegruppe i kodesignalet på bestemte tidspunkter, idet tilstedeværelsen av en slik kodegruppe ville få både sender og mottaker til å bringe interferensmønstrene til en på forhånd bestemt stilling som kan kalles nullstilling. Under forhold der man har meget forstyrrelser som skyldes lokale interfererende pulser og som kan påvirke den synkrone utvikling av interferensmønstrene, kunne den nevnte nullstillingskodegruppe innføres et par ganger under hver syklus for interferensmønsteret. Dette vil føre til en forkortning av den effektive lengde av interferensmønsteret. Ved denne forkortelse av interferensmønsterets effektive lengde er den fremgangsmåte der nullstillingskodegrupper stiller mønsteret i en på forhånd bestemt stilling, ikke egnet for kommunikasjonssystemer for overføring av hemmelige meldinger. Ved på avtalte tidspunkter å innføre en nullstillingskodegruppe for hvert undermønster i stedet for en nullstillingskodegruppe for mønsteret, er det mulig å oppnå at den effektive lengde av interferensmønsteret ikke forkortes, mens en gal stilling av ett eller flere av de elektroniske hjul hvis den oppstår, hurtig korrigeres allikevel. I et kryptosignal der imidlertid alle slags binære kombinasjoner benyttes som kryptokodegrupper, har man ikke tilbake noen frie kodegrupper som kunne benyttes som nullstillingskodegrupper.

Innføringen av nullstillingskodegrupper i et kodet signal hvori noen kodegrupper fremdeles er frie ville føre til at forbindelsens virkningsgrad ville falle betydelig.

Oppfinnelsen angår således et kommunikasjonssystem for overføring av hemmelige meldinger som kodes binært med hovedserier av elementer, der hver hovedserie dannes av en rekke underserier som alle har forskjellig antall elementer, og der hver underserie frembringes av en elektronisk krets, og den er i det vesentlige kjennetegnet ved at det for hver underserie er anordnet elektroniske innretninger for innstilling av underseriene i en på forhånd bestemt tilstand (nulltilstand) ved opptreden av spesielle bestemte grupper elementer som frem-

kommer i den kodede melding, og som kan velges etter ønske.

Det er sørget for minst en nullstillingskodegruppe for hvert hjul. Forskjellige nullstillingskodegrupper er anordnet for forskjellige hjul. På denne måte oppnår man at hvert hjul, uavhengig av andre, bringes til nullstilling ved bestemte tidspunkter, bestemt av statistiske lover.

Denne bruk av nullstilling av hjulene fører til en foretrukken bruk av de kombinasjoner av undermønstre for hvilke ett eller flere av hjulene er i nullstilling, slik at ikke alle kodegrupper i interferensmønsteret har samme sannsynlighet for å fremkomme eller oppstå. Dette er uunngåelig, men virkningen er ikke forstyrrende hvis man passer på at hvert hjul stort sett fullfører minst en hel omdreining mellom to på hverandre følgende nullstillingsmeldinger.

Etter en tilbakestilling til null vil minst ett av hjulene være i en på forhånd bestemt stilling (nullstilling), mens de andre kan være en hvilken som helst av et antall mulige stillinger.

Antar man at antallet stillinger for de forskjellige hjul ikke har noen felles divisor eller nevner vil det totale antall stillinger hjulene kan gjennomgå uten nullstilling, være lik produktet av antallet av stillinger for alle hjul. Hvis man har M -hjul med $k_1, k_2, \dots, k_m$ -stillinger vil det totale antall stillinger være produktet av $k_1, k_2, \dots, k_m$ eller skrevet på vanlig måte $\prod_{k=1}^m n_k$.

Når hjulene beveges frem regelmessig i trinn, vil rekken av enere og null være periodisk.

I dette tilfelle vil mønstret være periodisk og alle posisjoner inntas etter tur og mønstret gjentas etter $\prod_{k=1}^m n_k$ trinn.

Dette betyr at de samme rekker av stillinger av hjulene vil bli gjentatt hvis det ikke innføres noen nullstilling. Erfaring har vist at gjentatt bruk av samme nøkkelrekke muliggjør en forholdsvis lett dechiffrering av de kodede meldinger.

Når null innføres som foreslått i denne sak, vil hjulene, etter hver nullstilling, starte fra en tilfeldig valgt stilling som opptrer i den periodiske rekkefølge og fra denne stilling vil et bruddstykke av den periodiske rekke

113572

bli gjengitt inntil en ny nullstilling innføres, og rekken hopper til et annet bruddstykke av det periodiske mønster. Mønstret består således av et antall bruddstykker av det periodiske mønster. Lengden av disse bruddstykker er variabel da fremkomsten av neste nullstilling vil avhenge av sannsynlighetsfaktorer. Det kan vises at det totale antall av disse bruddstykker er lik

$$\sum_{k=1}^m n_k - \sum_{k=1}^m (n_k - 1) = N$$

Mønstret består således av N bruddstykker av det periodiske mønster som er fordelt tilfeldig i det periodiske mønster, og videre er lengden av disse bruddstykker underkastet sannsynlighetsfaktorer.

Det vil være klart at ved å innføre nullstilling i alle undermønstre får man et ikke-periodisk mønster av ubestemt lengde og at mønstret er forskjellig for forskjellige meldinger.

Hvis det er nødvendig å velge sannsynligheten for fremkomst av en nullstillingskodegruppe til forskjell for sannsynligheten for fremkomst av en kodegruppe i det kodede signal, kan betydningen av en nullstillingsmelding være den samme som betydningen av en hvilken som helst kombinasjon av elementer i den kodede gruppen. Ved f.eks. å gi nullstillingsmeldingen samme betydning som en bestemt kodegruppe og en bestemt verdi av det første element i den neste kodegruppe i et kodet telekssignal, vil man få en sannsynlighet på $\frac{1}{64}$ for fremkomst av nullstillingen hvis kodesignalet er statistisk homogent. I dette sistnevnte tilfelle ble det videre krevet at seks elementer skulle plasseres på første til femte plass i en kodegruppe og i den første plass i den neste kodegruppe. Ved å frafalle dette krav og ved å ta i betraktning seks elementer som finnes i på hverandre følgende informasjonsstillinger i det kodede signal, vil man få en helt annen sannsynlighet for fremkomst av nullstillingsmeldingen. Av dette skulle det være klart at man her har en viss frihet i valg av sannsynligheten for fremkomst av en nullstillingskommando.

Når det, i henhold til bestemte statistiske lover, oppstår en kombinasjon av elementer i det kodede signal der elementene også inneholder en nullstillingskommando, vil både sender og mottaker bringe det elektroniske hjul, som kommandoen er bestemt for, til nullstilling og med dette som utgangstilling vil det elektroniske hjul gjennomløpe sine stillinger på normal måte.

Virkningen av de nevnte nullstillingskommandoer er at ved enden av en tidsperiode hvis fremkomst kan beregnes matematisk, vil minst én nullstillingskommando ha kommet frem for hvert av de elektroniske hjul, slik at etter dette vil interferensmønstrene både for sender og mottaker som er tilført signalet under den nevnte tidsperiode, samtidig innta identiske stillinger.

I det følgende skal det gjengis et eksempel på en krets der hjulene nullstilles ved tidspunkter som er samstemte i henhold til statistiske lover. I den forklarende del av denne beskrivelse er dette for enkelhets skyld angitt som "statistisk nullstilling".

Interferensmønsteret er her sammensatt av tre undermønstre som har 8, 11 og 13 stillinger. Interferensmønsteret har $8 \cdot 11 \cdot 13 = 1144$ stillinger.

Undermønsteret som har åtte stillinger, frembringes av et elektronisk hjul som omfatter tre triggeranordninger X, Y, Z som har komplementære utgangsspenninger x, x' , y, y' og z, z' , som hver kan ha verdiene en og null. De seks utgangsspenninger danner inngangsspenningene for en $6 \cdot 8$ diode matriks. De åtte utgående liner er ved hjelp av brytere, koplet til en "eller"-port. De tre utløseranordninger X, Y, Z er koplet som et binært telleverk i hvilket triggeren X er den utløser som er minst i verdi, mens utløseren Z har den høyeste verdi. Når på hverandre følgende klokkepulser mates til telleverkets klokkepulsinnang, blir hver av de åtte utgående linjer for diodematriksen valgt etter hverandre. Dette er den vanlige måte for elektronisk frembringelse av en kvasitilfeldig rekke av enere og nuller. En slik fremgangsmåte representeres av summen av åtte logiske produkter.

$$F_8 = f_1xyz + f_2x'yz + f_3xy'z + f_4x'y'z + f_5xyz' + f_6x'yz' + f_7xy'z' + f_8x'y'z'$$

der f_0 til og med f_7 har verdien 1 for en bryter som er lukket, og verdien 0 for en åpen bryter og der F_8 er undermønstret. De åtte produkter vil gjensidig utelukke hverandre, noe som betyr at hvis et tilfeldig valgt produkt er lik 1 vil alle de andre produkter være 0. Hvert av de undermønstre som har 11 og 13 stillinger frembringes av et elektronisk hjul som har fire utløseranordninger hvis utgangsspenninger er x, x' , y, y' , z, z' og w, w' . Utløseren W er den trigger som har den høyeste verdi. Telleverket for 11 stillinger er koplet på en slik måte at etterat stillingene $xyzw = 1111$ til $x'yzw' = 1111$ er blitt passert på en binært oppadstigende måte, følger stillingen $x'y'z'w' = 1111$, hvorefter syklusen gjentas fra stillingen $xyzw = 1111$. Hoppet over stillingene $xy'zw' = 1111$ til $xy'z'w' = 1111$ foregår ved hjelp av en "og"-port som hvis betingelsen $x'yzw = 1$ oppfylles, slipper inn den neste klokke-

113572

puls til triggerne Y og Z, slik at disse bringes til stillingene $y' = 1$ og $z' = 1$. Samtidig vil en sperreanordning som er lukket når betingelsen $x'yzw'=0$ er tilfredsstillet, blokkere innføringen av klokkepuls gjennom inngangen for telleverket for klokkepulsene.

Telleverket for 13 stillinger passerer gjennom stillingene $xyzw = 1111$ til og med $x'y'zw' = 1111$ i en normal binær rekkefølge. En "og"-port som kun er åpen under forholdene $x'y'zw' = 1$, slipper klokkepuls inn triggeren Z. Samtidig vil en port som er lukket når betingelsen $(x'y'zw')' = 0$ tilfredsstilles, blokkere inngangen for klokkepuls til telleverket for klokkepulsene. Som et resultat av disse foranstaltninger vil den neste stilling av telleverket være $x'y'z'w' = 1111$ hvorefter syklusen gjentas.

Undermønsteret F_{11} har elleve stillinger og F_{13} har tretten stillinger som representeres av summen av 11 og 13 logiske produkter.

$$\begin{aligned}
 F_{11} &= f_1xyzw + f_2x'yzw + f_3xy'zw + f_4x'y'zw \\
 &\quad f_5xyz'w + f_6x'yz'w + f_7xy'z'w + f_8x'y'z'w \\
 &\quad f_9xyzw' + f_{10}x'yzw' + f_{11}xy'zw' + f_{12}x'y'zw' \\
 &\quad + f_0x'y'z'w' \\
 F_{13} &= f_1xyzw + f_2x'yzw + f_3xy'zw + f_4x'y'zw \\
 &\quad + f_5xyz'w + f_6x'yz'w + f_7xy'z'w + f_8x'y'z'w \\
 &\quad + f_9xyzw' + f_{10}x'yzw' + f_{11}xy'zw' + f_{12}x'y'zw' \\
 &\quad + f_0x'y'z'w'.
 \end{aligned}$$

Fra de tre undermønstre F_8 , F_{11} og F_{13} bestemmes mønsteret F ved hjelp av addisjon uten mente. Som logisk-algebraisk indikasjon for en addisjon uten mente kan man gjøre bruk av følgende formel:

$$F = F_8 \oplus F_{11} \oplus F_{13}.$$

Ved å anvende den aritmetiske regel $A \oplus B \oplus C = AB'C' + A'BC' + A'B'C + ABC$ synes det som om mønstret F kan fremkomme ved å anvende fire "og"-porter, hver med tre innganger og en "eller"-port med fire innganger.

I det foregående blir, under overgangen fra stillingen $x'yzw' = 1111$ i undermønsteret med elleve stillinger og fra stillingen $x'y'zw' = 1111$ i undermønsteret med tretten stillinger, klokkepulsene bare sluppet inn til de triggere som ikke var i stillingen svarende til $x'y'z'w' = 1111$. Det gjør imidlertid ingen forskjell for korrekt funksjon av kretsen om klokkepulsene i det ovennevnte tilfelle ble sluppet til de fire triggere X,Y,Z,W på en slik måte at

de tvinges til stillingene $x' = 1, y' = 1, z' = 1, w' = 1$.

Denne mulighet kan man dra fordel av når statistisk nullstilling burde finne sted, for tilførsel av den neste klokkepuls til triggerne X,Y,Z,W på en slik måte at disse tvinges til stillingene $x' = 1, y' = 1, z' = 1, w' = 1$, mens samtidig innføringen av klokkepuls til klokkepulsinnngangen for telleverket blokkeres.

I dette eksempel er det gjort bruk av et kodet telekssignal med fem elementer. Hvis det i dette kodede signal dukker opp en kombinasjon av elementer som i den europeiske telekskode Nr. 2 er kalt K, vil det undermønster som har tretten stillinger bringes til nullstilling $x'y'z'w' = 1111$. Når bokstaven Q dukker opp, blir undermønsteret som har elleve stillinger, brakt til stillingen $x'y'z'w' = 1111$. Når bokstaven U fremkommer, bringes undermønsteret, som har åtte stillinger, til stillingen $x'y'z' = 111$. Hvis man setter 0 for et element med mellomrompolaritet og 1 for et element med tegn-polaritet, vil koderetten være:

K 11110

Q 11101

U 11100

I det kodede signal der hver bokstav har en sannsynlighet på $\frac{1}{32}$ for å dukke opp vil sannsynligheten for statistisk nullstilling være $\frac{1}{32}$ for hvert av undermønstrene. I eksemplet er denne sannsynlighet øket til $\frac{2}{32}$.

Dette er oppnådd ved bare å la det annet til og med det femte element i hver kombinasjon virke som nullstillingskommando. Derfor vil nullstillingskommandoen i dette tilfelle være

1 1 1 1 0

og 0 1 1 1 0 for undermønsteret som har tretten stillinger

1 1 1 0 1

og 0 1 1 0 1 for undermønsteret som har elleve stillinger

1 1 1 0 0

og 0 1 1 0 0 for undermønsteret som har åtte stillinger.

Nullstillingskommandoene gjenkjennes ved å føre alle tegn i det kodede signal ved senderen såvel som på mottakeren gjennom et syvtrinns forskyvningsregister. På det tidspunkt da startelementet befinner seg i det siste trinn og stopp-elementet i det første trinn, vil elementene i trinnene fra to til og med seks være elementer fra én til og med fem hvis de inneholder ett og samme tegn.

113572

Dette øyeblikk kjenner man fra en synkroniseringskrets av vanlig type og som ikke vil bli beskrevet i denne sak. Hvis elementene fra to til og med fem i rekkefølge kalles b, c, d, e, og hvis det øyeblikk da stopp- og startelementene står på riktig sted kalles n vil betingelsene for statistisk nullstilling være henholdsvis:

$$\begin{aligned}(nbc)de' &= 1 \\(nbc)d'e &= 1 \\(nbc)d'e' &= 1\end{aligned}$$

Betingelsen $nbc = 1$, som i det følgende kalles a = 1 tilveiebringes ved hjelp av en "og"-port med tre innganger.

Betingelsene

$$ade' = 1 \qquad ad'e = 1 \qquad \text{og} \qquad ad'e' = 1$$

tilveiebringes av tre "og"-porter, hver med tre innganger.

Kretsen i henhold til det eksemplet som er beskrevet, vil bli nærmere forklart ved hjelp av figurene 1 til 6.

Ved hjelp av fig. 1 vil funksjonene av noen av de symbolske kretser som benyttes på figurene 2 til og med 6 bli nærmere forklart.

Figurene fra 2 til og med 5 representerer kretser som benyttes til frembringelse av interferensmønstre med nullstilling.

Fig. 6 representerer kretsen for utledning av nullstillingskommandoene.

På fig. 1 er 1 en trigger T med utgangsspenninger t og t'. Pulsporten 2 tillater videreføring av en puls som tilføres ved punktet 3 og kommer frem til triggeren 1 hvis triggerspenningen 4 har verdien 1, og sperreanordningen vil blokkere videreføring av pulsen til triggeren hvis triggerspenningen har verdien 0. Porten 5 arbeider med samme måte som porten 2. Pulsportene 2 og 5 arbeider fullstendig uavhengig av hverandre. En puls som fremkommer, bringer triggeren i en slik stilling at utgangsspenningen på den side hvorfra pulsen kom har verdien 0.

"og"-porten 6 fører en spenning 7 med verdien 1 bare hvis alle inngangsspenninger 8 har verdien 1 og i alle andre tilfelle en spenning med verdien 0. "eller"-portene 9 avgir en spenning 10 med verdiene 0 bare hvis alle inngangsspenninger 11 har verdien 0, og i alle andre tilfelle en spenning med verdien 1.

Inverteren 12 avgir et signal 13 som er lik det vendte inngangssignal 10.

Fig. 2 viser kretsen for undermønsteret med åtte stillinger. Triggeren 1, 2 og 3 danner et binært telleverk. De åtte "og" anordninger 5 representerer en diode matriks med seks innkommende og åtte utgående linjer. Bryterne 6 er justert i overensstemmelse med den ønskede rekkefølge av enere og null i det sykliske undermønster. Det ønskede undermønster fremkommer ved utgangen av "eller" anordningen 7 og inverteres av inverteren 8. Hvis man, som følge av fremkomst av et tegn som for undermønsteret med åtte stillinger har betydning som en nullstillingskommando, vil betingelsen $ad'e = 1$ være tilfredsstillet og "og"-porten 14 åpnet, noe som også fører til at pulsportene 9 åpner mens på grunn av venderen 10, tilførselen av klokkepulsene 11 til klokkepulsinnngangene 12 og 13 i triggeren 1 i telleverket blokkeres.

På fig. 3 ser man et diagram for utviklingen av undermønsteret som har elleve stillinger. "eller"-porten 16 og "og"-porten 15 avviker noe fra diagrammet på fig. 2. "og"-porten 14 svarer til "og"-porten 14 på fig. 2. "og"-porten 15 er anordnet med det for øye å redusere stillingene av telleverket fra 16 til 11. Nullstilling finner sted hvis $ad'e = 1$ eller hvis $x'yzw' = 1$ eller hvis begge disse signaler faller sammen.

Fig. 4 representerer diagrammet for undermønsteret med tretten stillinger.

Fig. 5 viser addisjon uten ment av de tre undermønstre.

Fig. 6 viser et skifteregister omfattende utløsere fra 20 til og med 26. Det kodede telekssignalet tilføres klemmen 27 og inverteres ved hjelp av inverteren 28. Tverrkoblingene mellom triggerne i skifteregisteret er avpasset til det faktum at utgangsspenningen for en trigger antar verdiene 0 på den side der pulsen fremkommer. Skiftpulsene 11 er de samme som klokkepulsene 11 på fig. 2, 3 og 4.

Skiftepulsene 11 avledes fra en synkroniseringskrets som ikke er vist på tegningen. Skiftpulsene sendes på tidspunkter på en slik måte i forhold til elementene i signalet 7 som må mates til klemme 27, at de nevnte elementer av-søkes omtrent på midten. Synkroniseringskretsen avgir også en sperreanordning 30 som har verdien 1 fra det tidspunkt da skiftpulsene fører et stoppelement inn i triggeren 20 til det tidspunkt da den neste skiftpuls fremkommer. "og"-portene 29 tilfører sperrespenningen $a = nbc$ for "og"-portene 14 på fig. 2, 3 og 4.

113572

P a t e n t k r a v

Kommunikasjonssystem for overføring av hemmelige meldinger som kodes binært med hovedserier av elementer, der hver hovedserie dannes av en rekke under-serier som alle har forskjellig antall elementer, og der hver underserie frembringes av en elektronisk krets, karakterisert ved at det for hver under-serie er anordnet elektroniske innretninger for innstilling av underseriene i en på forhånd bestemt tilstand (null-tilstand) ved opptreden av spesielle bestemte grupper elementer som fremkommer i den kodede melding, og som kan velges etter ønske.

FIG. 1

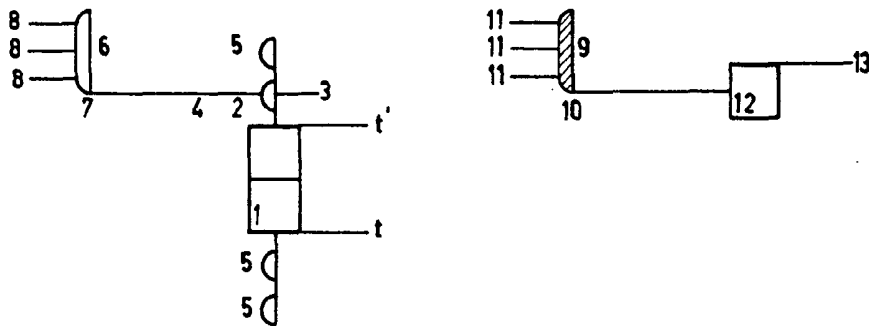


FIG. 5

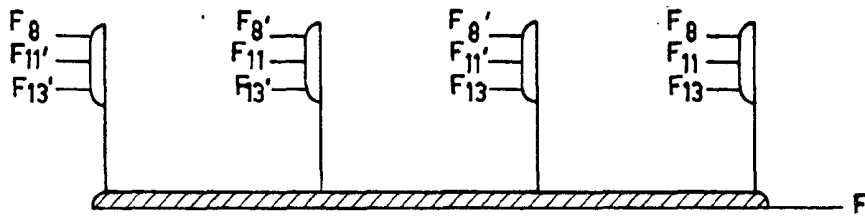
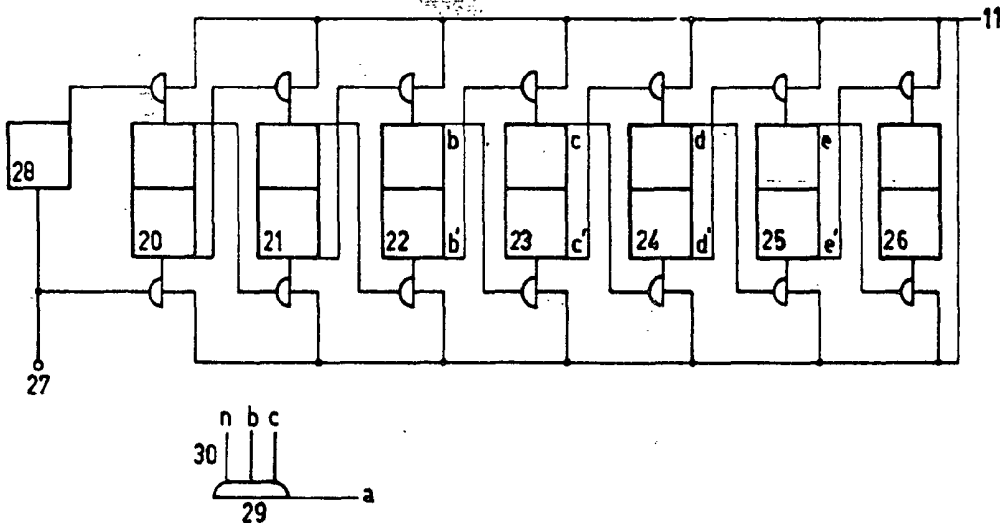


FIG. 6



113572

FIG.2

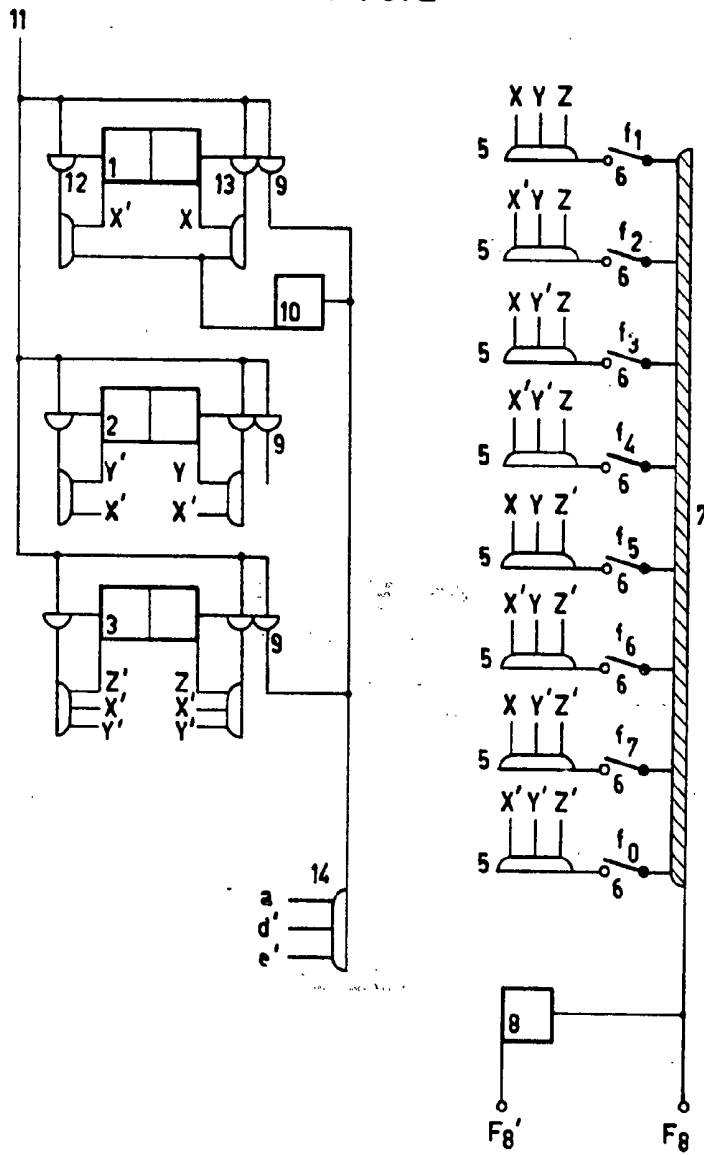
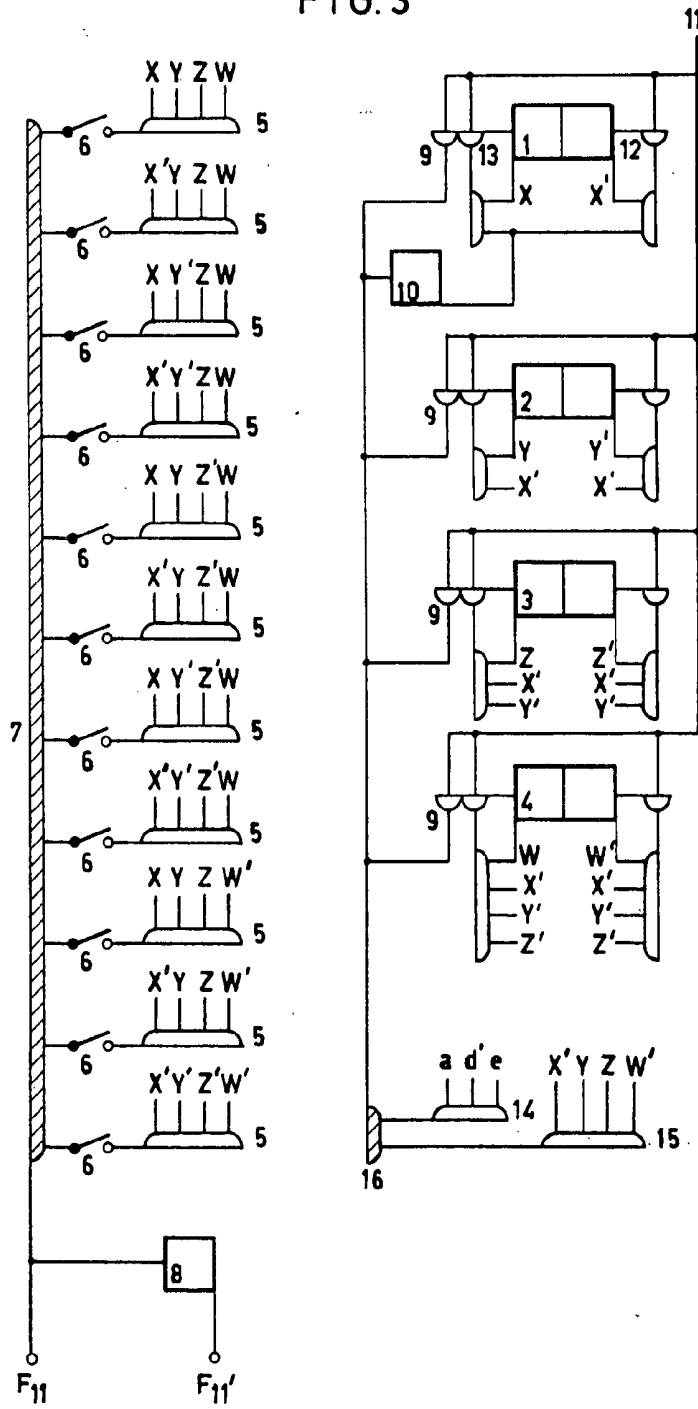


FIG. 3



113572

FIG. 4

