

OCTROOIRAAD



NEDERLAND

Openbare Leestafel

OCTROOI Nr. 107306

KLASSE 97 cf.

Int. Cl. H 04 L 9/07.

NEDERLANDSE ORGANISATIE VOOR
TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TEN
BEHOEVE VAN DE RIJKSVERDEDIGING te 's-Gravenhage.

Uitvinder: Ir. RUDOLF SLEGTENHORST te Wassenaar.

Stelsel voor geheime berichtgeving.

Aanvraag Nr. 265358, ingediend 31 mei 1961, 12 uur 10 min.

Gem.: Drs. E. W. van Popta c.s. te 's-Gravenhage.

1

De uitvinding heeft betrekking op een stelsel voor geheime berichtgeving, waarbij het uit tweewaardige tekenelementen bestaande klare bericht vertoeferd wordt door een storingspatroon van eindige lengte, welk storingspatroon bestaat uit een aantal subpatronen met onderling verschillende aantallen tweewaardige tekenelementen, waarbij elk subpatroon opgewekt wordt door een bijbehorende subpatroongenerator.

Een dergelijk stelsel is bekend uit het Britse octrooi-schrift Nr. 694.757.

Het storingspatroon, dat bij het stelsel volgens de uitvinding wordt toegepast, wordt opgewekt met behulp van een aantal elektronische cyclisch werkende schakelingen. Omdat deze elektronische cyclisch werkende schakelingen een analogon vormen van een draaiend wiel worden deze schakelingen aangeduid als elektronische wielen.

Ieder van deze wielen heeft een aantal standen. Deze aantallen zijn voor alle wielen verschillend en hebben bij voorkeur geen gemeenschappelijke deler. Ieder elektronisch wiel wekt een instelbaar nul-één patroon op, waarvan het aantal enen plus het aantal nullen gelijk is aan het aantal standen van het wiel. Deze patronen worden subpatronen genoemd. Een eerste gebruikelijke methode is, dat men de subpatronen met ongelijke cyclische lengten met behulp van een logische schakeling optelt volgens de rekenregels: een even aantal enen geeft een nul, een oneven aantal enen geeft een één. Het door deze sommering verkregen patroon wordt gebruikt als storingspatroon, zowel wanneer alle wielen onafhankelijk van elkaar regelmatig voortstappen, als wanneer het voortstappen van enkele wielen bepaald wordt door de toevallige enen- en nullencombinatie van de door de wielen opgewekte subpatronen.

Een tweede bekende methode is dat men de enen- en nullencombinatie van de onafhankelijk van elkaar of in afhankelijkheid van elkaar bewegende wielen gebruikt als instelcombinatie voor een hulporgaan dat de karakters voor het storingspatroon opwekt.

Het toepassen van een dergelijk storingspatroon heeft twee nadelen, die beide hun oorzaak vinden in het feit, dat de storingspatronen van zender en ontvanger een gelijk aantal standen doorlopen moeten hebben, wil de ontvanger het bericht kunnen ontcijferen.

Het eerste nadeel is, dat een elektronisch werkend ontvangtoestel geen juiste gegevens over het doorlopen

2

aantal standen bevat als de voedingsspanning uitgvallen is geweest of als storende impulsen één of meer elektronische wielen in een onjuiste stand hebbe gebracht.

Het tweede nadeel is, dat bij deelname in een net va cryptoabonnees alle abonnees tegelijk moeten beginne met het doorlopen van de standen van het storingspatroon uitgaande van gelijke beginstanden.

Volgens de uitvinding worden deze nadelen tegengaan, doordat elke subpatroongenerator ten gevolge van het optreden van bepaalde, in het vertoeferde bericht voorkomende, naar wens te kiezen groepen van elementen, in een vastgekozen stand (nulstand) gezet kan worden.

Opgemerkt wordt dat uit de openbaargemaakte Duitse octrooiaanvraag („Auslegeschrift“) 1.076.73 bekend is op gezette tijden een nulzet-codegroep in het cryptosignaal in te lassen, die bij optreden zender en ontvanger beide aanleiding geeft hun storingspatrone in een overeengekomen stand, nulstand genoemd, te brengen. In gevallen waarin men veel hinder ondervindt van lokale stoorimpulsen, die het gelijk lopen der storingspatronen in gevaar brengen, zou men deze nulzet-codegroep enkele malen per cyclusperiode van het storingspatroon kunnen inlassen. Dit leidt tot een verkorting van de effectieve lengte van het storingspatroon.

In het stelsel volgens de uitvinding wordt aan ieder wiel ten minste één nulzet-codegroep toegevoegd. Aan verschillende wielen worden verschillende nulzet-codegroepen toegevoegd. Hierdoor wordt bereikt dat ieder wiel onafhankelijk van de overige op door statistisch wetten bepaalde tijdstippen in de nulstand wordt gebracht.

Door toepassing van het nulzetten van de wielen ontstaat een voorkeur voor die combinaties van de subpatronen waarvoor één of meer der wielen in de nulstand verkeert, waardoor niet alle codegroepen van het storingspatroon een gelijke kans van optreden bezitten. Dit is onvermijdelijk, maar het effect is niet storend als men ervoor zorgt dat ieder wiel gemiddeld ten minste een volledige omwenteling maakt tussen twee opeenvolgende nulzet-commando's.

Indien het nodig is de kans op het optreden van een nulzet-codegroep afwijkend te kiezen van de kans op het optreden van een codegroep in het cryptosignaal kan aan een combinatie van elementen in de cryptocodegroepen de betekenis van nulzet-commando worden

den gehecht. Door bijvoorbeeld in een cryptotelexcode aan een bepaalde codegroep en aan een bepaalde waarde van het eerste element van de volgende codegroep de betekenis van nulzet-commando te hechten, wordt een kans van optreden van het nulzetten verkregen van $\frac{1}{64}$ als het cryptosignaal statistisch homogeen is. In het laatste geval werd aan de zes elementen nog de eis gesteld dat zij zich zouden bevinden op de eerste tot en met vijfde plaats van één codegroep en op de eerste plaats van de volgende codegroep. Door deze eis te laten vallen en zes op opeenvolgende informatieposities in het cryptosignaal voorkomende elementen te beschouwen kan een geheel andere kans van optreden van het nulzet-commando worden verkregen. Hieruit blijkt dat er enige vrijheid is in de keuze van de kans op het optreden van een nulzet-commando.

Bij het volgens bepaalde statistische wetten optreden van een combinatie van elementen in het cryptosignaal waaraan mede de betekenis van een nulzet-commando wordt gehecht, brengen zender en ontvanger beide het elektronische wiel, waarvoor het betreffende commando geldt, in de nulstand, van waaruit het vervolgens op de normale wijze zijn standen doorloopt.

Het effect van genoemde nulzet-commando's is, dat na verloop van een tijd waarvoor de mathematische verwachting berekend kan worden, voor ieder der elektronische wielen ten minste één nulzet-commando is opgetreden, zodat daarna de storingspatronen van de zender en van de ontvanger die het signaal gedurende het genoemde verloop van tijd heeft waargenomen, tegelijkertijd dezelfde standen aannemen.

In het hieronder volgende wordt een schakeling waarbij de wielen in de nulstand worden gezet op mede door statistische wetten bepaalde tijdstippen nader toegelicht. In de toelichting wordt dit gemakshalve aangeduid als „statistische nulzet”.

Het storingspatroon wordt hier samengesteld uit drie subpatronen die respectievelijk 8, 11 en 13 standen hebben. Het storingspatroon heeft 8.11.13 = 1144 standen.

Het subpatroon met 8 standen wordt opgewekt door een elektronisch wiel bestaande uit drie trekkers X, Y, Z met complementaire uitgangsspanningen x, x', y, y' en z, z' , die elk de toegekende waarden 1 en 0 kunnen hebben. De 6 uitgangsspanningen vormen de ingangsspanningen van een 6×8 diodematrix. De acht uitgaande lijnen zijn aangesloten op een OF-poort via stoppen die al of niet de geleiding naar de OF-poort verzorgen. De drie trekkers X, Y, Z zijn als een binaire teller geschakeld met trekker X als minstwaardige en trekker Z als meestwaardige trekker. Bij toevoer van opeenvolgende telimpulsen aan de telimpulsingang van de teller worden achtereenvolgens ieder der acht uitgaande lijnen van de diodematrix geselecteerd. Dit is een gebruikelijke manier voor het elektronisch opwekken van een cyclische willekeurige rij enen en nullen. Een dergelijke methode wordt weergegeven door de som van acht logische produkten.

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

waarin f_0 t/m f_7 de waarden 1 hebben voor een aanwezige stop en de waarde 0 voor een afwezige stop en waarin F_8 het subpatroon is. De acht produkten sluiten elkaar onderling uit, dat wil zeggen als een willekeurig gekozen produkt 1 is zijn alle ander nul. De subpatronen met 11 en met 13 standen worden ieder opgewekt door een elektronisch wiel dat vier trekkers met uitgangsspanningen x, x', y, y', z, z' en w, w' bevat. Trekker W is de meestwaardige trekker. De teller voor 11 standen is zo geschakeld dat na het binaire oplopend doorlopen van de standen $xyzw = 1111$ t/m $x'yzw' = 1111$ de stand $x'y'z'w' = 1111$ volgt, waarna de cyclus weer vanaf $xyzw = 1111$ herhaald wordt. Het overslaan van de standen $xy'zw' = 1111$ t/m $xy'z'w' = 1111$ vindt plaats met behulp van een EN-poort, die, als de conditie $x' \cdot y \cdot z \cdot w' = 1$ wordt vervuld de vol-

gende telimpuls tot de trekkers Y en Z toelaat, waardoor deze in de standen $y' = 1$ en $z' = 1$ worden gebracht. Tegelijkertijd blokkeert een poort die gesloten is als de conditie $(x' \cdot y \cdot z \cdot w')' = 0$ wordt vervuld de toegang voor de telimpuls tot de telimpulsingang van de teller.

De teller voor 13 standen doorloopt in normale binaire volgorde de standen $xyzw = 1111$ t/m $x'y'zw' = 1111$. Een EN-poort die uitsluitend geopend is bij de conditie $x' \cdot y' \cdot z \cdot w' = 1$ laat de telimpuls door tot trekker Z. Tegelijkertijd blokkeert een poort die gesloten is als voldaan wordt aan de conditie $(x' \cdot y' \cdot z \cdot w')' = 0$ de toegang van de telimpuls tot de telimpulsingang van de teller. Door deze maatregelen is de volgende stand van de teller $x'y'z'w' = 1111$ waarna de cyclus zich herhaalt.

De subpatronen F_{11} met 11 standen en F_{13} met 13 standen worden weergegeven door de som van 11 en 13 logische produkten

$$F_{11} = f_1xyzw + f_2x'yzw + f_3xy'zw + f_4x'y'zw + f_5xyz'w + f_6x'yz'w + f_7xy'z'w + f_8x'y'z'w + f_9xyzw' + f_{10}x'yzw' + f_{11}xy'z'w' + f_{12}x'y'z'w'$$

$$F_{13} = f_1xyzw + f_2x'yzw + f_3xy'zw + f_4x'y'zw + f_5xyz'w + f_6x'yz'w + f_7xy'z'w + f_8x'y'z'w + f_9xyzw' + f_{10}x'yzw' + f_{11}xy'z'w' + f_{12}x'y'z'w' + f_{13}xyzw'' + f_{14}x'yzw'' + f_{15}xy'zw'' + f_{16}x'y'zw''$$

Uit de drie subpatronen F_8 , F_{11} en F_{13} wordt de optelling zonder overdracht het patroon F bepaald. Als logisch-algebraïsche aanduiding voor optellen zonder overdracht wordt hier gebruikt

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

Door het toepassen van de rekenregel

$$A \oplus B \oplus C = AB'C' + A'BC' + A'B'C + AB'C + A'B'C' + A'BC' + A'B'C + ABC$$

blijkt dat het patroon F verkregen kan worden door toepassing van vier EN-poorten met drie ingangen en één OF-poort met vier ingangen.

In het voorgaande werd bij overgang van de stand $x'yzw' = 1111$ in het subpatroon van 11 standen respectievelijk van de stand $x'y'zw' = 1111$ in het subpatroon van 13 standen naar de stand $x'y'z'w' = 1111$ de telimpuls slechts toegelaten tot die trekkers die in de stand corresponderend met $x'y'z'w' = 1111$ stonden. Aan de goede werking van de schakeling wordt echter niets afgedaan als in bovengenoemde gevallen de telimpuls wordt toegelaten tot de trekkers X Y Z W zodanig dat ze in de standen $x = 1, y = 1, z = 1, w = 1$ worden gedwongen.

Van deze mogelijkheid wordt gebruik gemaakt indien statistische nulzet dient plaats te vinden. De eerstvolgende telimpuls toe te laten tot de teller X Y Z W, zodanig dat zij in de standen $x = 1, y = 1, z = 1, w = 1$ gedwongen worden, terwijl tegelijkertijd de toegang van de telimpuls tot de telimpulsingang van de teller wordt geblokkeerd.

In het uitvoeringsvoorbeeld wordt gebruik gemaakt van een gecijferd telexsignaal met 5 elementen. In dit gecijferde signaal de elementencombinaties treedt die bij de Europese telexcode Nr. 2 K wordt het subpatroon met 13 standen in de nulstand $x'y'z'w' = 1111$ gebracht. Bij optreden van karakter Q wordt het subpatroon met 11 standen in de nulstand $x'y'z'w' = 1111$ gebracht. Bij optreden van karakter U wordt het subpatroon met 8 standen in de nulstand $x'y'z'w' = 1111$ gebracht. Door voor een element met startpolariteit 0 te schrijven en voor één met startpolariteit 1 is de code voor in de tijd opeenvolgende elementen

K	1	1	1	1	0
Q	1	1	1	0	1
U	1	1	1	0	0

Bij het cryptosignaal, waarin ieder karakter een kans van optreden van $1/32$ heeft is de kans op statistische nulzet voor ieder der subpatronen $1/32$. In het voorbeeld n deze kans vergroot tot $2/32$. Dit wordt bereikt door alleen het tweede tot en met vijfde element van iedere combinatie te laten optreden als nulzet-commando. In dit geval zijn de nulzet-commando's dus

$\begin{matrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{matrix}$

voor het subpatroon met 13 standen

voor het subpatroon met 11 standen

voor het subpatroon met 8 standen

De nulzet-commando's worden herkend door alle karakters van het cryptosignaal, zowel aan zend- als aan ontvangzijde in een zeventraps schuifregister te leiden. Op het moment waarop in de laatste trap het startelement staat en in de voorste trap het stopelement zijn de elementen in de trappen twee tot en met zes de elementen één tot en met vijf van één karakter. Dit moment is bekend dank zij een synchronisatieschakeling van gangbaar type, waarvan de bespreking hier achterwege blijft. Als de elementen twee tot en met vijf achtereenvolgens b, c, d, e worden genoemd en het moment waarop stop- en startelement op de goede plaats staan n wordt genoemd, dan zijn de condities voor statistische nulzet respectievelijk.

$$\begin{aligned} (n.b.c).d.e' &= 1 \\ (n.b.c).d'.e &= 1 \\ (n.b.c).d'.e' &= 1 \end{aligned}$$

De conditie $n.b.c = 1$ hierna te noemen a = 1 wordt gerealiseerd met behulp van een EN-poort met drie ingangen.

De condities

$$a.d.e' = 1 \quad a.d'.e = 1 \quad \text{en} \quad a.d'.e' = 1$$

worden gerealiseerd door drie EN-poorten met ieder drie ingangen.

De schakeling volgens het uitvoeringsvoorbeeld wordt toegelicht aan de hand van de fig. 1 tot en met 6.

Aan de hand van fig. 1 wordt de functie van enkele symbolische schakelingen, die in de fig. 2 tot en met 6 gebruikt worden nader toegelicht.

Fig. 2 tot en met 5 geven de schakeling weer die gebruikt wordt voor opwekking van het storingspatroon met nulzet.

Fig. 6 geeft de schakeling voor afleiding van de nulzetcommando's weer.

In fig. 1 is 1 een trekker T met uitgangsspanningen t en t'. De impuls-poort 2 laat een impuls aangeboden op punt 3 tot de trekker 1 toe, als de poortspanning 4 de waarde 1 heeft en blokkeert de toegang voor de impuls tot de trekker indien de poortspanning 4 de waarde 0 heeft. De impuls-poorten 5 hebben dezelfde werking als de impuls-poort 2. De impuls-poorten 2 en 5 werken volledig onafhankelijk van elkaar. Een toegelaten impuls brengt de trekker in een stand zodat de uitgangsspanning aan de zijde waar de impuls werd toegelaten de waarde 0 heeft.

De EN-poort 6 geeft een spanning 7 met de waarde 1 alleen af als alle ingangsspanningen 8 de waarde 1 hebben en in alle andere gevallen een spanning met de waarde 0. De OF-poort 9 geeft een spanning 10 met de waarde 0 alleen af als alle ingangsspanningen 11 de waarde 0 hebben en in alle andere gevallen een span-

ning met de waarde 1. De omkeerschakeling 12 levert een signaal 13, dat gelijk is aan het geïnverteerde ingangssignaal 10.

In fig. 2 is de schakeling voor het subpatroon van 8 standen getekend. De trekkers 1, 2 en 3 vormen een binaire teller. De acht EN-poorten 5 stellen een diodematrix met zes ingaande en acht uitgaande lijnen voor. De schakelaars 6 worden ingesteld in overeenstemming met de gewenste een en nul volgorde van het cyclisch subpatroon. Het gewenste subpatroon verschijnt aan de uitgang van de OF-poort 7 en wordt geïnverteerd door de omkeerschakeling 8. Als voldaan wordt aan de conditie $a.d'.e' = 1$ ten gevolge van het optreden van een karakter waaraan voor het subpatroon met acht standen de betekenis van een nulzet-commando wordt gehecht, wordt de EN-poort 14 geopend waardoor de impuls-poorten 9 worden geopend, terwijl dank zij de omkeerschakeling 10 de toegang van de telimpuls 11 tot de telimpulsingen 12 en 13 van trekker 1 van de teller wordt geblokkeerd.

In fig. 3 wordt het schema voor de opwekking van het subpatroon met 11 standen gegeven. Afwijkend ten opzichte van het schema in fig. 2 zijn de OF-poort 16 en de EN-poort 15. De EN-poort 14 komt overeen met de EN-poort 14 in fig. 2. De EN-poort 15 is aangebracht ten behoeve van de reductie van 16 tot 11 standen van de teller. Nulzet vindt plaats als $a.d'.e = 1$ of als $x'.y.z.w' = 1$ of als beide gebeurtenissen plaatsvinden.

Fig. 4 stelt het schema van het subpatroon met 13 standen voor.

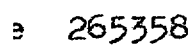
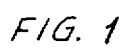
Fig. 5 stelt de optelling modulus 2 voor van de drie subpatronen.

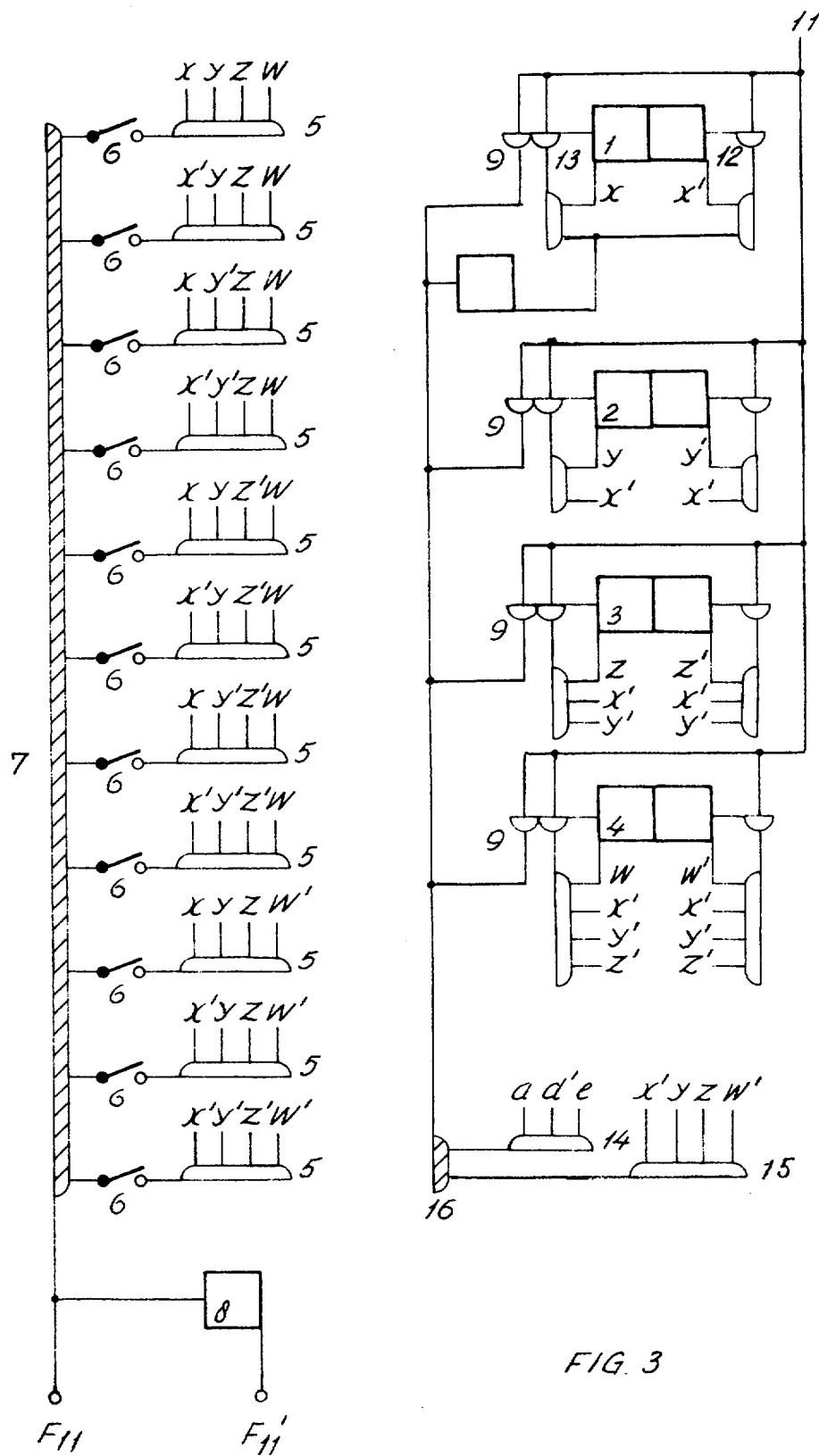
In fig. 6 wordt een schuifregister bestaande uit de 35 trekkers 20 tot en met 26 voorgesteld. Het cryptotexsignaal wordt aan de klem 27 toegevoerd en met behulp van de omkeerschakeling 28 geïnverteerd. De gekruiste verbindingen tussen de trekkers van het schuifregister hangen samen met het feit dat de uitgangsspanning van een trekker de waarde 0 aanneemt aan de zijde waar een impuls wordt toegelaten. De schuifimpuls 11 zijn dezelfde als de telimpuls 11 in fig. 2, 3 en 4.

De schuifimpuls 11 worden ontleend aan een niet getekende synchronisatieschakeling. De schuifimpuls liggen dusdanig ten opzichte van de elementen van het signaal 7 toegevoerd aan de klem 27 dat deze elementen ongeveer in het midden worden afgetast. De synchronisatieschakeling levert tevens een poortspanning 30 die de waarde 1 heeft vanaf het moment waarop de schuifimpuls een stopelement in trekker 20 plaatst tot het moment waarop de volgende schuifimpuls optreedt. De EN-poort 29 levert de poortspanning $a = n.b.c$ ten behoeve van de EN-poorten 14 in de fig. 2, 3 en 4.

Conclusie.

Stelsel voor geheime berichtgeving, waarbij het uit tweewaardige tekenelementen bestaande klare bericht gecijferd wordt door een storingspatroon van eindige lengte, welk storingspatroon bestaat uit een aantal subpatronen met onderling verschillende aantallen tweewaardige tekenelementen, waarbij elk subpatroon opgewekt wordt door een bijbehorende subpatroongenerator, met het kenmerk, dat elke subpatroongenerator ten gevolge van het optreden van bepaalde, in het gecijferde bericht voorkomende, naar wens te kiezen groepen van elementen, in een vastgekozen stand (nulstand) gezet kan worden.





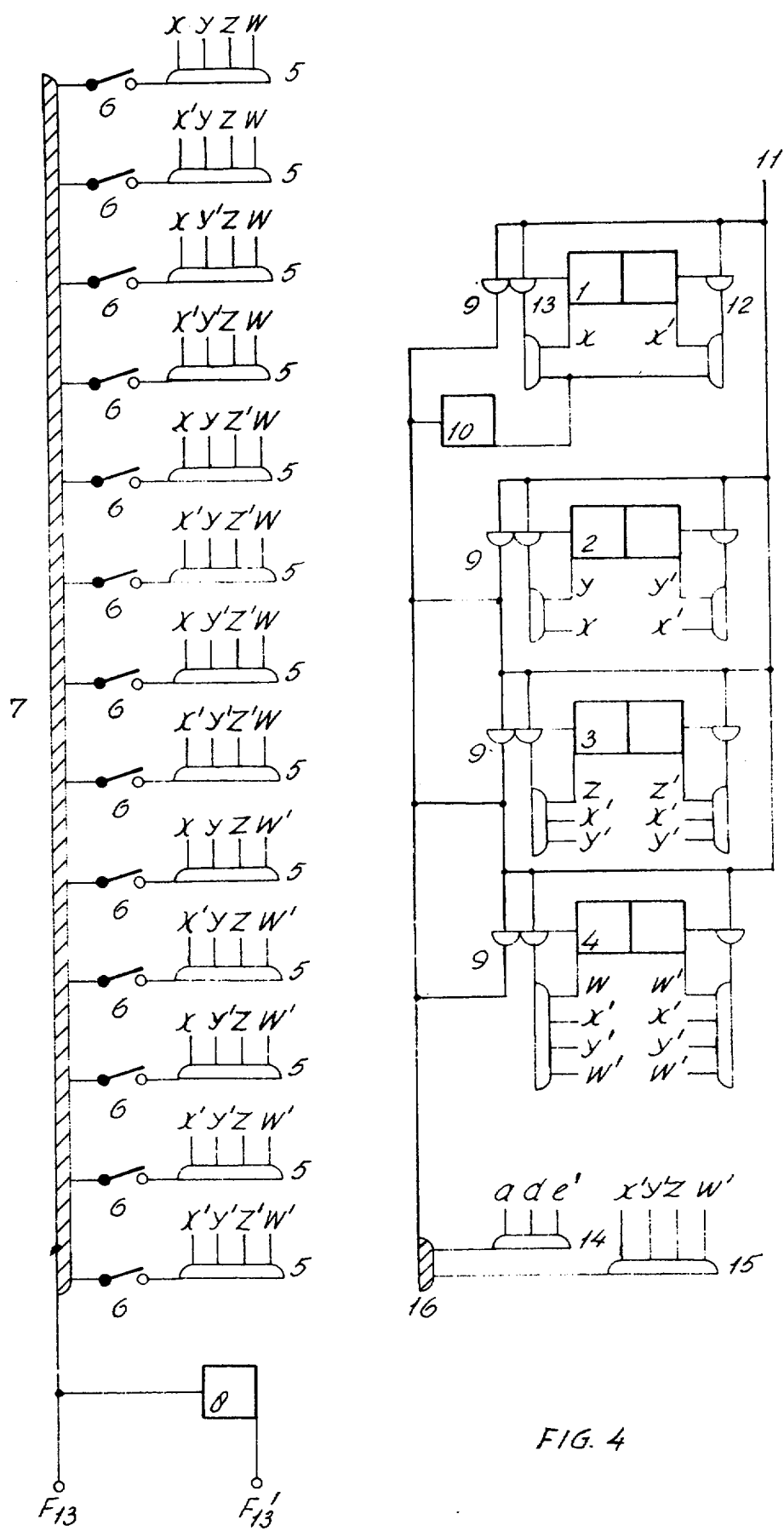


FIG. 4

