Octrooiraad

(10)A Terinzagelegging (11) 8201077

Nederland (19) NL

(54) **Kommunikatiesysteem, bevattende een centrale dataverwerkende inriching, toegangsstations en externe stations, waarbij een kryptografische kontrole is voorzien op vervalsing van een extern station, alsmede externe stations voor gebruik in zo een kommunikatiesysteem.**

(51) Int.Cl³.: G06F 3/04, G06F 3/02, G06F 15/21, H04L 9/02.

(71) Aanvrager: N.V. Philips' Gloeilampenfabrieken te Eindhoven.

(74) Gem.: Ir. R.A. Bijl c.s.
Internationaal Octrooibureau B.V.
Prof. Holstlaan 6
5656 AA Eindhoven.

(21) Aanvrage Nr. 8201077.

(22) Ingediend 16 maart 1982.

(32) - -

(33) - -

(31) - -

(62) - -

(43) Ter inzage gelegd 17 oktober 1983.

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

N.V. PHILIPS' GLOEILAMPENFABRIEKEN TE EINDHOVEN.

"Kommunikatiesysteem, bevattende een centrale dataverwerkende inrichting, toegangsstations en externe stations, waarbij een kryptografische kontrôle is voorzien op vervalsing van een extern station, alsmede externe stations voor gebruik in zo een kommunikatiesysteem".

De uitvinding betreft een kommunikatiesysteem, bevattende een centrale dataverwerkende inrichting en een aantal daarmee gekoppelde, op verschillende plaatsen opgestelde toegangsstations, alsmede een groep externe, draagbare, stations van zakformaat, waarbij een extern station met een toegangsstation via een bidirektioneel werkend informatiekanaal koppelbaar is, waarbij het toegangsstation in kwestie een berichtvormer bevat om een bericht te vormen en een enkodeur om het zo gevormde bericht te ontvangen en middels een eerste versleutelinformatie te enkoderen en een zo gevormd eerste kodebericht aan het informatiekanaal toe te voeren, en waarbij het externe station in kwestie een eerste dekodeur bevat om het eerste kodebericht te ontvangen en middels een aan de eerste versleutelinformatie gepaard eerste verontsleutelinformatie te dekoderen om een eerste hervormd bericht aan een digitale verwerkingsinrichting in het betreffende externe station toe te voeren, en waarbij in een initiatie toestand van het externe station een alsdan ermee gekoppeld en coexistent initiatiestation voorzien is van een generator voor het aan het extern station toevoeren van de eerste verontsleutelinformatie. De centrale dataverwerkende inrichting is bijvoorbeeld de beheersinrichting van een databank met medische gegevens die alleen aan gekwalificeerde aanvragers ter beschikking mag komen, dat is dan een aanvrager die zich bedient van een voorafbepaald en als zodanig geïdentificeerd werkstation. Dit werkstation vormt dan een extern station en het toegangsstation is dan bijvoorbeeld een "aansluit"- of "front end" processor die een centrale processor van bepaalde deeltaken ontlast. In het algemeen kan de centrale dataverwerkende inrichting fysiek gedistribueerd zijn. In dit geval is het informatiekanaal bijvoorbeeld een datanetwerk met verschillende aansluitprocessors hetwelk bovendien voor allerlei taken gebruikt kan worden, zowel vertrouwelijke als openbare. Er moeten evenwel maatregelen getroffen worden opdat binnen zo'n netwerk geen onbevoegd opvragen van vertrouwelijke informatie plaats kan vinden. Slechts als "rechthebbend" geïdentificeerde werkstations mogen van de vertrouwelijke informatie gebruik maken en de toegangsstations

hebben de taak om voor elke kategorie van vertrouwelijke informatie de bokken van de schapen te scheiden. In een ander toepassingsgebied is de centrale dataverwerkende inrichting de beheerder van een krediet-systeem, waarin bijvoorbeeld gelduitgifte mogelijk is op vertoon van elektronische, en met het kommunikatiesysteem koppelbare, krediet kaarten. Ook in dit geval is het noodzakelijk dat een extern station als legitiem geïdentificeerd wordt. Het is een doelstelling van de uitvinding om te verschaffen de mogelijkheid tot kryptografische kontrôle op vervalsing van zo een extern station (bijvoorbeeld werkstation of elektronische kredietkaart) in een dergelijk kommunikatiesysteem, waarbij het legitimeren niet gekoppeld is aan de fysieke plaats in het kommunikatiesysteem waar zich het extern station bevindt, en waarbij de legitimatie plaatsvindt doordat in beide richtingen slechts gekodeerde, en met vrijwel onoverkomelijke moeilijkheden door een niet-geautoriseerde toegang dekodeerbare berichten plaats vindt, zodat ook het simuleren van een legitiem extern station onmogelijk wordt, een en ander zodanig dat het niet nodig is dat elk toegangsstation voor elk extern station een separate ver(ont)sleutelinformatie moet memoriseren. De uitvinding realiseert de doelstelling doordat hij het kenmerk heeft dat het extern station in kwestie een tweede enkodeur bevat om het eerste hervormd bericht te ontvangen en middels een tweede versleutelinformatie die onafhankelijk is van de eerste versleutelinformatie te enkoderen en een zo gevormd tweede kodebericht aan het informatiekanaal toe te voeren, en waarbij het toegangsstation in kwestie een tweede dekodeur bevat om het tweede kodebericht te ontvangen en middels een aan de tweede versleutelinformatie gepaarde tweede verontsleutelinformatie te dekoderen om een tweede hervormd bericht te vormen, dat in de initiatietoestand het initiatiestation is voorzien van een tweede generator voor het aan het extern station toevoeren van de tweede versleutelinformatie, dat het toegangsstation een derde generator bevat om genoemd eerste bericht onvoorspelbaar te genereren, en een vergelijkelement om het eerste bericht en het tweede hervormd bericht te vergelijken en bij overeenstemming een legitimatiebevestiging te genereren en dat genoemde eerste verontsleutelinformatie en tweede versleutelinformatie voor een aantal externe stations onderling identiek en voorts daarin onuitleesbaar zijn.

De uitvinding betreft mede een draagbaar, extern station, te gebruiken

in zo een kommunikatiesysteem en als een kredietkaart gegeometriseerd. Voor zulke kredietkaarten bestaat een ISO-standaard, maar andere afmetingen van de maat van een visitekaartje en ongeveer 1 tot enkele millimeters dik zijn ook voordelige realisaties. Het is daarbij gunstig als het voorzien is van respektievelijke lussen voor kontaktloze overdracht van informatie- en voedingsenergie vanuit een toegangsstation en overdracht van informatie-energie terug naar het toegangsstation, en dat een schuifregister serieel is opgenomen tussen twee van genoemde lussen voor tijdelijke opslag van ontvangen informatie. Dit levert een eenvoudige en veilige realisatie.

KORTE BESCHRIJVING VAN DE FIGUREN

De uitvinding wordt nader uitgelegd aan de hand van enkele figuren.

Fig. 1 geeft een blokschema van een kommunikatiesysteem waarmee de uitvinding realiseerbaar is.

Fig. 2 geeft een blokschakeling van een extern station.

Fig. 3 geeft een stroomdiagram van de interaktie tussen een toegangsstation en een extern station.

BESCHRIJVING VAN EEN VOORKEURSUITVOERING

Fig. 1 geeft een blokschema van een kommunikatiesysteem waarmee de uitvinding realiseerbaar is en waarvan in eerste instantie de normale werktoestand, dus niet de initiatietoestand wordt beschreven. Het kommunikatiesysteem bevat een centrale dataverwerkende inrichting. Dit is bijvoorbeeld (30) een rekenmachine met een processor, een programmageheugen, een tussen- of kladblok (scratch-pad) geheugen, een achtergrond geheugen, aanpassingseenheden voor randapparatuur, zoals een afbeeldinrichting met kathodestraalbuis of een drukker, een verdere aanpassingseenheid voor een extern informatiekanaal en een interne busverbinding om gegevens en besturingssignalen tussen de opgesomde onderdelen te transporteren. In het beschreven systeem funktioneert zo'n rekenmachine als beheersinrichting voor een verder niet aangegeven gegevensbestand of een gelduitgiftesysteem, dat met elektronische kredietkaarten werkt. Noch de fysieke organisatie van deze gelduitgifte, noch de rekenmachine zelf worden, kortheidshalve, beschreven. Via de bidirektionele verbinding 27 is de centrale data verwerkende inrichting 30 aangesloten op de systeembus, respektievelijk het systeemnetwerk 31. De toegangsstations 20, 46 zijn eveneens via bidirektionele verbindingen,

zoals verbinding 28, op bus/netwerk 31 aangesloten. Het aantal toegangsstations kan veelal groot zijn, voor een kredietkaartensysteem bijvoorbeeld 100 of meer, voor een beheerssysteem van een databank bijvoorbeeld 10 of meer. Door de indikaties 22, 24 is een extern informatiekanaal aangegeven, dit kan opgebouwd zijn met twee simplex (unidirektionele) verbindingen, het kan ook half- of volledig-duplex zijn uitgevoerd. Met indikaties 26, 48, 50 zijn drie externe stations aangegeven (het laatste is in de gegeven situatie niet met een toegangsstation gekoppeld). Per toegangsstation kan er hoogstens een enkel extern station aanwezig zijn, zoals hier aangegeven, dit aantal kan evenwel ook veel groter zijn, bijvoorbeeld doordat het toegangsstation middels een tijdmultiplexorganisatie met verscheidene externe stations afwisselend kommuniceert. Het informatiekanaal kan fysiek als een galvanisch, fiber- of draadloos medium zijn uitgevoerd. Het extern station 26 kan in de eerste plaats zijn gerealiseerd als een werkstation of "intelligente terminal": het kan in principe dezelfde soort opbouw bezitten als de centrale dataverwerkende inrichting, maar anderzijds ook met hulpmiddelen die beperkter zijn in aantal en/of kapaciteit. Een andere uitvoering kan er een zijn zoals deze beschreven is in de Nederlandse Octrooiaanvrage 7802132, overeenkomstige Amerikaanse Octrooiaanvrage Ser. No. 010879 indieningsdatum 9 februari 1979, van dezelfde aanvrager. In deze dokumenten is beschreven een draagbaar reserveringselement dat met een toegangsstation koppelbaar is, zodat tweezijdige data-uitwisseling mogelijk is. Het reserveringselement is uitgevoerd als een enigszins verdikte (enkele mm) kredietkaart. Door toevoeging van een kleine microcomputer zijn in zo'n reserveringselement ook mathematische en/of andere bewerkingen uitvoerbaar. Toevoeging van een toetsenbord en multi-karakterafbeeldingsmiddelen vervolmaken zo'n kredietkaart tot een kompakt en elementair werkstation. De kredietkaart kan na legitimatie door het toegangsstation recht geven op uitkering van een geldbedrag of andere materiële verstrekkingen. Eventueel kan een extern station in de krediet-kaart-achtige uitvoering (draagbaar!) ook gebruikt worden om een drager te legitimeren als toegangsgerechtigd tot bepaalde plaatsen of lokaliteiten, eventueel in kombinatie met een aan deze drager separaat medegedeeld wachtwoord. Op zichzelf is het gebruik van wachtwoorden en de logische bewerking daarvan, hetzij in het toegangsstation, hetzij in het externe station, bekend.

De legitimatie van het extern station in isolement verloopt nu als volgt: eerst doet het extern station verzoek tot legitimatie. Dit verzoek is gerealiseerd als datasignaal, eventueel voorzien van voorloop (preamble), afsluit- (postamble) en synchronisatie-informatie. Het is ook mogelijk dat het toegangsstation voortdurend deze synchronisatie verzorgt, bijvoorbeeld door een klokpatroon op de lijn 22. In het later te bespreken uitvoeringsvoorbeeld is het dataverkeer gepartioneerd in datawoorden van 16 bits die in een informatieverkeerswoord van 32 bits zijn ondergebracht. Na ontvangst van het legitimatieverzoek, hetwelk eventueel een gepretendeerde identiteit inhoudt, genereert het toegangsstation een eerste bericht M. Dit bericht kan een willekeurige inhoud hebben, bijvoorbeeld gegenereerd zijn door een toevalsgenerator 32, door een aantal bitposities van een door de eerder genoemde klok aangestuurde teller, en dergelijke. Dit bericht wordt in de enkodeur 34 geënkodeerd middels een versleutelinformatie. Deze versleutelinformatie kan de enige zijn, of wel geselekteerd uit een groep aanwezige versleutelinformaties door de gepretendeerde identiteit van het externe station. Op basis van het eerste bericht M wordt zo middels de eerste versleuteloperatie EC een eerste kodebericht C1 geformeerd: C1 = EC (M). De versleutelinformatie, indien bekend, geeft slechts na zeer gekompliceerde en daardoor tijdrovende bewerkingen de voor het dekoderen van kodebericht C1 noodzakelijke verontsleutelinformatie. In feite is een dergelijke bewerking onmogelijk langdurig . Het omgekeerde kan even tijdrovend zijn, zodat ook de versleutelinformatie niet uit de verontsleutelinformatie af te leiden is. In dat geval worden ze beide uit een gemeenschappelijke basisinformatie afgeleid bij het initiëren van het gehele kommunikatiesysteem (dat is dus niet tijdens het initiëren van een enkel extern station, zoals later wordt besproken). In andere gevallen kan evenwel het afleiden van de versleutelinformatie uit de verontsleutelinformatie zeer wèl doenlijk zijn, ook al is het omgekeerde in elk geval onmogelijk. Steeds is na het beëindigen van de initiatietoestand in het extern station 26 de benodigde verontsleutelinformatie voorhanden, nadat deze al dan niet over de lijn 22 (of eventueel op een andere manier) aan dat station is overgedragen. Deze verontsleutelinformatie kan evenwel niet worden uitgelezen, en kan dus ook niet later aan hetzelfde of een ander toegangsstation 20 worden toegeleid. Zo kan dus uit het kodebericht C1 en middels de verontsleutelinformatie DC in de dekodeur

36 een bericht M1 worden hervormd volgens M1 = DC (C1). De blokken 37, 39 stellen verdere intermediaire elementen van het extern station 26 voor, die ook op andere posities in de door de ontvangen signalen afgelegde weg geplaatst kunnen zijn, zoals regeneratiemiddelen, opslagmiddelen, en middelen om aan het hervormde bericht extra informatie toe te voegen. Zo kan het hervormde bericht over een zeer specifiek tijdsinterval worden vertraagd, eventueel onder besturing van (een deel van) de inhoud van het bericht M1 zelf. Verder kan bijvoorbeeld een gegeven dat de identiteit van het betreffende extern station 26 aangeeft, aan het bericht M1 worden toegevoegd. In het extern station 26 is voorts een verdere versleutelinformatie ET aanwezig om in enkodeur 38 uit het hervormde en eventueel bijgewerkte bericht M1 een teruggaand kodebericht te vormen: volgens C2 = ET (M). Bij deze verdere versleutelinformatie behoort weer een verdere verontsleutelinformatie welke niet aan de verdere versleutelinformatie te ontlenen is. Deze verontsleutelinformatie DT is in het toegangsstation 20 aanwezig, maar kan daaruit niet uitgelezen worden, op dezelfde manier als de eerste verontsleutelinformatie niet kan worden uitgelezen uit het extern station 26. Zo kan in de dekodeur 40 uit het teruggaande kodebericht C2 een tweede hervormd bericht geproduceerd worden volgens M2 = DT (C2) voor de relatie tussen de verdere versleutelinformatie en de verdere versleutelinformatie geldt weer hetzelfde als eerder is vermeld voor de relatie tussen de eerste versleutelinformatie en de eerste versleutelinformatie: met name is het dus in feite onmogelijk om de verdere versleutelinformatie te rekonstrueren. De informaties M2 en M zijn nu direkt aan elkaar gelieerd, mits in beide gevallen (C1 èn C2) de versleutelinformatie en verontsleutelinformatie bij elkaar behoorden. In dat geval is bijvoorbeeld M2 = M en het externe station legitimeerbaar, bijvoorbeeld doordat in vergelijkelement 42 de gelijkheid tussen M en M2 wordt gekontroleerd. Het uitgangssignaal "gelijk" daarvan kan bijvoorbeeld een blokkeringselement tussen de verbindingen 28 en 22/24 doorlaatbaar maken, zodat het extern station met de centrale dataverwerkende inrichting kan kommuniceren. Het betreffende datatransport kan ongekodeerd zijn, ofwel versleuteld volgens een eenvoudige kode, ofwel in bijzondere gevallen volgens dezelfde kode als voor de legitimatie werd gebruikt. Het datatransport kan dan betreffen een zoek- of vraagaktie in de databank, respektievelijk een uitgifteverzoek aan

het gelduitgiftesysteem. Het kontrôleren daarbij op voldoende saldotegoed op de aangesproken rekening kan op een gebruikelijke manier plaats vinden. Een voordelige kode, en de versleutel/verontsleutelinformaties daarvoor, zijn kiesbaar op een manier die gepubliceerd is in een artikel door R.C. Merkle en M.E. Hellmann, Hiding information and signatures in trapdoor knapsacks, I.E.E.E. Tr. Inf. Theory, vol IT 24, no. 4, sept. 1978, p. 525 ff, respektievelijk in de Nederlandse Octrooiaanvrage 7810063.

DE OPBOUW VAN EEN EXTERN STATION

Fig. 2 geeft een blokschema van de opbouw van een draagbaar element dat is te gebruiken in een systeem volgens de uitvinding. Goeddeels is zo'n draagbaar element, alsmede een reserveringssysteem voor autobusjes, waarin dat draagbaar element onder andere werkt als "intelligent plaatsbewijs", reeds beschreven in het Amerikaanse octrooischrift 4298793 (PHN 9052) van dezelfde aanvrager, welk octrooischrift hierin wordt geïncorporeerd bij wijze van referentie. Kortheidshalve worden een aantal weinig specifieke onderdelen van dat element hier niet nader gespecificeerd. Er zijn getekend twee induktieve opneemlussen 102, 103 met respektievelijk 10 en 1 winding; deze zijn gepositioneerd langs de omtrek van een vierkant van ongeveer 5x5 cm. De signaaloverdracht tussen deze lussen en overeenkomstige lussen in het toegangsstation is goed als ze bij overeenkomstige en evenwijdige positie een onderlinge afstand van bijvoorbeeld 2-6 mm hebben. De frekwentie van de gebruikte signalen is bijvoorbeeld in het gebied van 100 kHz. De lussen zijn uitgevoerd als gedrukte bedrading, met een windingsdikte van ongeveer 0,2 millimeter (iets meer voor de lus 103 omdat deze als zendlus meer energie dissipeert). De overdracht van de voedingsenergie vindt eveneens draadloos plaats, waarbij gelijkspanningen van +70, +5, 0, -28 volt worden gevormd. Deze subsystemen zijn kortheidshalve niet nader getoond. De lus 102 is geschikt om het informatiesignaal op te vangen dat wordt uitgezonden volgens een bekend frequentie-gemoduleerd systeem met een grondfrequentie van ongeveer 100 kHz, een modulatiediepte van 10% dus ongeveer 10 kHz, en een bitsnelheid in het gebied rond 1 kHz. Het element 115 is een detektor voor de frequentiemodulatie en bevat een bekende fasegekoppelde lus (PLL). Het uitgangssignaal hiervan wordt samen met het signaal van lus 102 aan de dekodeur 104 voor het frekwentie-gemoduleerde signaal

toegevoerd. Deze laatste werkt als lokale klok en genereert een aan de bitsnelheid aangepaste klokpulsreeks met in dit geval een terugkeerfrekwentie van ongeveer 2,5 kHz. Deze dataklok wordt over lijn 107 toegevoerd aan het vertragingselement 119, en aan poort 111. De vertragingstijd van element 119 blokkeert dan vooralsnog de poorten 112 en 113 en stelt middels ingang 114 het schuifregister 123 in de nulstand (reset) waarin het voorlopig ook blijft. Zo worden inschakelverschijnselen overbrugd. De dekodeur 104 produceert voorts op lijn 115 de uit het ingangssignaal hervormde datasignalen (vooralsnog wordt in schuifregister 123 echter niets opgeslagen), en voorts alternerend op de lijnen 116, 117 een tweevoudige klokpuls voor de vooralsnog ondoorlaatbare poort 113. Als het betreffende draagbare element, in tegenstelling tot het bovenstaande, niet of niet goed, langs het toegangsstation is gepositioneerd, blijft daarentegen de gehele schakeling in rust. Na een tijd van ongeveer 0,03 sekonde is de vertraagtijd van element 119 beëindigd en worden de poorten 113 en 112 doorlaatbaar. Ook verdwijnt het signaal op terugstelingang 114 van het schuifregister 123 dat daarmee dus de serieel op ingangslijn 115 ontvangen databits achtereenvolgens opslaat. Het schuifregister 123 heeft een kapaciteit van 32 bits en als er verder niets gebeurt worden de ontvangen bits na enige tijd via de seriële uitgang 100 van het schuifregister 123 toegevoerd aan de data-enkodeur 118. Deze laatste wordt bestuurd door de tweevoudige klokpulsen op lijnen 116, 117 die doorgelaten worden door poort 113. De uitgang van data enkodeur 118 is aangesloten op de zendlus 103 om databits te kunnen overvoeren naar het toegangsstation.
Het element 124 is een woorddetektor die op de drie eerste en de drie laatste posities van het schuifregister 123 is aangesloten om middels een aantal start- en stopbits van voorgeschreven waarde te detekteren dat een 32-bits informatiewoord aanwezig is. Als in het schuifregister 123 zo'n informatiewoord aanwezig is wordt dit een halve klokpulsperiode later door de woorddetektor 124 gedetekteerd. Het detektiesignaal wordt toegevoerd aan de poorten 120 en 111. Door het signaal van poort 111 start de tijdgenerator 121. In de eerste plaats geeft de tijdgenerator 121 een signaal af aan de poort 112 waardoor deze blokkeert en schuifregister 123 dus geen verdere datakloksignalen ontvangt. Door het openen van de poort 120 ontvangt de funktiedekodeur 122 de vijf bits C1, C2, A, B, C van het in het schuifregister 123 aanwezige

informatiewoord. In de eerste plaats geeft de dekodeur 122 over lijn 125 een signaal aan de tijdgenerator 121 ter sturing van de daarin te genereren blokkeringstijd voor poort 112. De signalen van de bits C1, C2 worden voorts doorgelaten naar het besturingselement 125, dat de signalen van de bits C1, C2 ook naar het geheugen 126 doorstuurt. Voor de door deze bits bestuurde funktie zie later. Op lijn 127 ontvangen het geheugen 126 en het besturingselement 125 ook een vijfbits adres dat afkomstig is van vijf voorafbepaalde bitposities van het schuifregister 123. Afhankelijk van de waarden van de bits C1, C2 wordt in het geheugen 126 een lees-, wis-, schrijf- of loze geheugenaktie uitgevoerd. Het besturingselement 125 bevat vaste informatie van twee geheugenadressen in geheugen 126 die niet gebruikt worden. Deze twee geheugenadressen werken voor de versleutelings-ontsleutelingsprocessor 101 als leesbesturingskommando, respektievelijk als schrijfbesturingskommando: de desbetreffende besturingssignalen worden overgevoerd over de lijnen 105, 106. Onder besturing van een van deze twee geheugenadressen wordt geheugen 126 niet geaktiveerd, bijvoorbeeld door het tegenhouden of veranderen van één der ontvangen bits C1, C2. Anderzijds kan de lijn 99 een signaal terugsturen naar de funktiedekodeur 122 om het afbeelden (zie later) van de informatie van zo'n beveiligde adresplaats te verhinderen. Een als beschreven beveiligd adres kan opgeslagen worden in de vorm van een vaste bedrading middels een logische poort, bijvoorbeeld het adres (00000) door een vijfingangs logische NIET-OF-poort. Genoemd blokkeren, respektievelijk veranderen kan ook met een logische poort gebeuren.

Als er kommunikatie nodig is tussen het geheugen 126, dan wel processor 101, en het schuifregister 123 ontvangt poort 129 een besturingssignaal van de funktiedekodeur 122 over lijn 128. Poort 129 is uitgevoerd als zogenaamde "tri-state buffer" en heeft drie toestanden, respektievelijk 1, 0, en "door een hoge impedantie afgesloten". In de eerste twee gevallen is deze poort in beide richtingen doorlaatbaar en wordt de logische toestand bepaald door een van buiten opgedrukt signaal. De richting van het signaaltransport wordt bepaald door een desbetreffende aansturing van de signaalbron (elementen 101, 123, 126). In de toestand van hoge impedantie is desgewenst kommunikatie mogelijk tussen geheugen en afbeeldinrichting zoals nader wordt uitgelegd. In geval van kommunikatie met het schuifregister wordt daaruit gelezen via lijn 130

of daarin geschreven via lijn 131. Alle datapaden van/naar poort 129 hebben een breedte van zestien bits. In geval van laden van informatie in het schuifregister geeft daartoe de funktiedekodeur 122 een signaal op lijn 132, terwijl door een signaal vanuit de tijdgenerator 121 op lijn 133 de poort 134 het laadsignaal (parallel laden) aan het schuifregister 123 toevoert. De funktie van geheugen 126 wordt bestuurd volgens de volgende twee-bits-kodes (C1, C2):01: woord wissen; 00: woord schrijven in het geheugen vanuit het schuifregister; 10: woord lezen uit het geheugen en inschrijven in het schuifregister en/of de afbeeldelementen (zie later); 11: niets doen. Het geheugen 126 is een lees/schrijfgeheugen met statische opslag en willekeurige toegang en heeft in dit voorbeeld een kapaciteit van 32 woorden à 16 bits (type ER 2050 General Instrument).

De funktiedekodeur is naast het beschrevene geschikt voor het dekoderen van de drie bits A, B, C die de funktie van de afbeeldinrichting besturen. De afbeeldinrichting bevat in dit voorbeeld twee funktiebepalers 135, 136, twee aanstuurinrichtingen 137, 138 en twee afbeeldelementen 139, 140, laatstgenoemde elk voor twee zevensegmentskarakters. De af te beelden informatie verschijnt als een achtbits kode op lijn 141. In de elementen 135, 136 wordt deze vertaald in twee zevensegments kodes. Verder ontvangt hoogstens één van de elementen 135, 136, een energeringssignaal van de funktie dekodeur 122 over lijn 142, respektievelijk 143. Het energeringssignaal kan twee frequentiekomponenten bevatten, namelijk één van ongeveer 50 Hz en één van ongeveer 6000 Hz. Voorts ontvangen de elementen 135, 136 van tijdgenerator 121 een selektief signaal om de afbeeldelementen 139, 140 slechts gedurende een voorafbepaald tijdsinterval te bekrachtigen. In het bovenstaande is de frequentie van 50 Hz bedoeld voor het inschrijven, de frequentie van 6000 Hz voor het uitwissen. De aanstuurelementen 137, 138 vormen een impedantieaanpassing, als eerder gesteld zijn de voedingsaansluitingen kortheidshalve weggelaten.

Als de in de tijdgenerator 121 gegenereerde tijd is afgelopen dan verdwijnt het blokkeringssignaal voor poort 112 en ontvangt het schuifregister 123 weer klokpulsen. Hierdoor wordt de informatie in het schuifregister 123 doorgeschoven en detekteert het element 124 niet meer de vereiste kombinatie van start- en stopbits. Daardoor blokkeren de poorten 111 en 120, zodat er geen sturing meer is voor de tijdgene-

rator 121 respektievelijk de funktiedekodeur 122. De inhoud van het schuifregister wordt aldus voortgeschoven naar data-enkodeur 118 en daarop middels spoel 103 uitgezonden. Hierbij wordt een logische "1" voorgesteld door een overgang op de positieve flank van de oneven èn op de negatieve flank van de even klokpuls binnen een bitcel, een logische 0 alleen door het laatste.

In het geheugen/afbeeldsysteem zijn de voornaamste datastromen van schuifregister naar geheugen en/of afbeeldinrichting, en van geheugen naar schuifregister en eventueel afbeeldinrichting. Daarmee zijn de kodebits A, B, C respektievelijk: 111: afbeelding onveranderd; 001: inschrijven busnummer; 010: inschrijven bestemmingsnummer; 011: inschrijven busnummer en wissen bestemmingsnummer; 100: inschrijven bestemmingsnummer en wissen busnummer; 101: wissen busnummer; 110: wissen bestemmingsnummer; 000: wissen busnummer, wissen bestemmingsnummer. Op het ogenblik dat een informatiewoord door de woorddetektor 124 wordt gedetekteerd moeten de startbits 1-3 de juiste waarde "11x" bezitten, en de stopbits 30-32 de waarde "110". Bit 3 is een reservebit. De vijf bits 4-8 vormen een adres voor geheugen 126, respektievelijk processor 101. De bits 9-16 vormen data voor het geheugen 126, respektievelijk voor processor 101. De bits 17-24 vormen data voor geheugen 126, processor 101 en/of de afbeeldinrichting 126. De bits 27, 28, 29 besturen eveneens middels funktiedekodeur 122 de werkmode van de afbeeldinrichting. Deze twee bit-stellen kunnen dus onderling onafhankelijke waarden hebben. De bits 30, 31 hebben als stopbit de verplichte waarde "1". De bit 32 heeft als verdere stopbit de verplichte waarde "0". Als genoemde vijf start/stopbits een ander informatiepatroon bezitten wordt door de inrichting 124 geen woord gedetekteerd en ontvangt het schuifregister 123 dus steeds schuifpulsen via poort 112.

De versleutelings/ontsleutelingsprocessor 101 is in parallel met het geheugen 126 aangesloten en werkt naar buiten als een zogenaamde "zwarte doos". Onder besturing van signalen, op de lijnen 105, 106 wordt een ingangsregister geschreven, respektievelijk een uitgangsregister gelezen, terwijl de overige elementen van de processor een connectie met de buitenwereld bezitten: ze kunnen dus niet onder uitwendige besturing worden uitgelezen. Deze processor kan grotendeels van een gebruikelijk type zijn, met dood geheugen, lees-schrijfgeheugen, arithmetische en logische eenheid, verscheidene registers, een en ander onderling verbonden

door een interne bus. Door de informatie van het dood geheugen kan het verontsleutelingsalgorithme, respektievelijk het versleutelingsalgorithme worden uitgevoerd op de ontvangen informatie. De processor 101 is aangesloten op de poort 129 en op de besturingslijnen 105, 106. Voorts ontvangt hij nog klokpulsen van de lijn 117 die gebruikt worden om de interne klok te synchroniseren. Laatstgenoemde werkt op een voldoend hoge frekwentie om de ver(ont)sleutelingsalgorithmes in een redelijk geachte tijdsduur te voltooien. Element 200 is een adresdekodeur om een voorafbepaald adres op lijn 127 te dekoderen dat werkt als leesadres voor de processor 101. De te verontsleutelen informatie wordt telkens met 16 bits tegelijk dan toegevoerd aan het ingangsregister van processor 101 totdat een voldoende hoeveelheid informatie is ontvangen. Deze informatie wordt dan dus ook telkens in zulke pakketten door het toegangsstation afgeleverd. Daarna wordt de verontsleuteling en dan de hèrversleuteling uitgevoerd. Daarna werkt element 200 om een tweede voorafbepaald adres op lijn 127 te dekoderen dat werkt om een informatie afgifte door de processor te besturen ; eveneens weer verdeeld over evenzovele 16-bits informatiewoorden als noodzakelijk. In de initiatietoestand vindt een verontsleuteling, herversleuteling niet plaats doordat een ander deel van het microprogramma, in processor 101 dan slechts eenmalig wordt uitgevoerd. Een mogelijke uitvoeringsvorm is dat na de initiatie, die verder, wat betreft het datatransport op de beschreven manier plaats vindt, door een speciaal signaal op klem 201 intern in de processor een onomkeerbare verandering wordt aangebracht. Dit kan bijvoorbeeld betreffen het doorbranden van een zekering. Daarna wordt het beschreven initiatiedeel van het microprogramma nooit meer uitgevoerd, maar wordt er direkt ver(ont)sleuteld. Op zichzelf zijn de berekeningen, respektievelijk andere verwerkingsstappen van de microprogramma's gebruikelijk; het bijzondere van de kode wordt steeds gegeven door de versleutel/ontsleutelinformatie.

BESCHRIJVING VAN HET STROOMDIAGRAM

Fig. 3 geeft het stroomdiagram van het legitimatieproces. Blok 200 stelt voor de start, waarbij dus de respektievelijke spanningen op peil komen, de klokpulsen geaktiveerd worden en de registers op nul teruggesteld, voor zover noodzakelijk. Blok 202 stelt voor de detektie door de woorddetektor. Als deze geen woord detekteert voert het systeem een wachtlus 204 uit. Als een woord wordt gedetekteerd, wordt in blok

206 gedetekteerd of de microprocessor 101 wordt geadresseerd met een schrijfoperatie. Als dat niet zo is wordt een tweede wachtlus 208 doorlopen. Als de microprocessor wèl wordt geadresseerd (deze detektie verifieert dus 5 woordbits, 5 adresbits en twee besturingsbits, dus in totaal 12 bits) wordt in blok 210 de data (16 bits) uit het betreffende woord naar een aantal beginregisters van de processor geschreven, in blok 212 wordt de daarbij behorende aanwijzer (intern adres) opgehoogd. In blok 214 wordt gedetekteerd of alle kodewoorden (vast aantal) zijn ontvangen. Als dat niet zo is gaat het systeem terug naar blok 202. Als alle woorden zijn ontvangen wordt in blok 218 het verontsleutelingsalgorithme (het eerste) uitgevoerd met behulp van het in het dode geheugen opgeslagen programma, en de in het geprogrammeerde geheugen opgeslagen verontsleutelingsinformatie. Direkt daaropvolgend wordt met behulp van de tweede versleutelinformatie het gedekodeerde bericht opnieuw versleuteld (blok 220). Dit gebeurt in een volgorde van stappen. In blok 222 wordt gedetekteerd of de laatste stap is voltooid. Zolang dat niet zo is keert het systeem weer terug naar blok 220. Als de laatste stap is voltooid wordt in blok 224 het gekodeerde bericht naar een aantal uitgangsregisters gevoerd. Alleen deze registers en geen andere opslagpositie van de processor kunnen naarbuiten toe uitgelezen worden. Ze worden aangewezen door dezelfde aanwijzer als in blok 212: deze telt nu de andere richting uit. De blokken 226-234 vormen een pendant met de blokken 202, 206, 210, 212, 214: alleen worden nu de uitgangsregisters gelezen in de serieel ontvangen datawoorden. Als het laatste woord is uitgelezen (blok 234) is het proces klaar (blok 236).

De procedure in het toegangsstation is overeenkomstig, alleen begint het gehele proces daar met het genereren van een toevallige informatie die direkt wordt versleuteld in een blok dat overeenkomt met blok 220 in Fig. 3. (zij het met behulp van de eerste versleutelinformatie). Daarna wordt de informatie overgestuurd (overeenkomst met de blokken 224 tot en met 234) en vervolgens afgewacht tot de opnieuw versleutelde informatie terug ontvangen wordt (overeenkomstig met de blokken 204 tot en met 214). Deze laatste wordt verontsleuteld (overeenstemming met blok 218 zij het met behulp van de tweede verontsleutelinformatie) en met de oorspronkelijk versleutelde informatie vergeleken. Als er overeenstemming bestaat is het externe station als legitiem bevonden en kunnen datakommunikatieprocessen worden gestart zoals deze in de geïncorporeerde referentie zijn beschreven, respektievelijk kunnen

de operaties tot realisering van een geld- of gegevensuitgifte door het systeem (toegangsstation of centrale dataverwerkende inrichting) worden gerealiseerd. Op laatstgenoemde op zichzelf heeft de uitvinding geen betrekking.

De initiatie van het externe station kan ook op overeenkomstige manier plaatsvinden, waarbij in fig. 3 dan bijvoorbeeld een loze versleutelinformatie gebruikt wordt als de eerste versleutelinformatie.Ook het verontsleutelen in blok 218 is dan een loze operatie. De data zelf die in het initiatieproces worden overgestuurd representeren dan de eerste verontsleutelinformatie en de tweede versleutelinformatie. Tijdens het ontvangen van deze informaties in het station hebben één of meer adresbits van het geheugen een bepaalde waarde. Na het initiëren met de twee genoemde informaties wordt voor de met de betreffende adresbitwaarden geassocieerde geheugenadressen een verdere schrijfoperatie onmogelijk gemaakt. Deze adresplaatsen kunnen daarna extern niet meer gelezen worden en in het geheel niet meer geschreven. Zo is de informatie beveiligd tegen fraudeurs. De initiatiebewerkingen worden uitgevoerd in een of meer speciaal daartoe bestemde initiatiestations. Deze initiatiestations kunnen goeddeels opgebouwd zijn overeenkomstig de andere toegangsstations. In dat geval heeft de generator niet het karakter van een toevalsgetalvormer, maar van een geheugenfunktie waarin de versleutel, respektievelijk verontsleutelinformaties voor het toegangsstation zijn opgeslagen, zodat aldus de verontsleutelinformaties goed beveiligd zijn. De beschreven procedures kunnen nog in omgekeerde richting worden uitgevoerd, waarbij dus het externe station een onvoorspelbare informatie genereert die middels twee versleutel/verontsleutelinformaties geverifieerd wordt: zo is ook de identiteit van het toegangsstation door het externe station verifieerbaar.

CONCLUSIES:

1. Kommunikatiesysteem, bevattende een centrale dataverwerkende inrichting (30) en een aantal daarmee gekoppelde, op verschillende plaatsen opgestelde toegangsstations (20, 46), alsmede een groep externe, draagbare, stations van zakformaat (26, 48, 50) waarbij een extern station met een toegangsstation via een bidirektioneel werkend informatiekanaal (22, 24) koppelbaar is, waarbij het toegangsstation in kwestie een berichtvormer (32) bevat om een bericht te vormen en een enkodeur (34) om het zo gevormde bericht te ontvangen en middels een eerste versleutelinformatie te enkoderen en een zo gevormd eerste kodebericht aan het informatiekanaal toe te voeren, en waarbij het extern station in kwestie een eerste dekodeur (36) bevat om het eerste kodebericht te ontvangen en middels een aan de eerste versleutelinformatie gepaarde eerste verontsleutelinformatie te dekoderen om een eerste hervormd bericht aan een digitale verwerkingsinrichting (37) in het betreffende externe station toe te voeren, en waarbij in een initiatietoestand van het externe station een alsdan ermee gekoppeld en coëxistent initiatiestation voorzien is van een generator voor het aan het extern station toevoeren van de eerste verontsleutelinformatie, met het kenmerk, dat het extern station in kwestie een tweede enkodeur (38) bevat om het eerste hervormd bericht te ontvangen en middels een tweede versleutelinformatie die onafhankelijk is van de eerste versleutelinformatie te enkoderen en een zo gevormd tweede kodebericht aan het informatiekanaal toe te voeren, en waarbij het toegangsstation in kwestie een tweede dekodeur (40) bevat om het tweede kodebericht tweede verontsleutelinformatie te dekoderen om een tweede hervormd bericht te vormen, dat in de initiatietoestand het initiatiestation is voorzien van een tweede generator voor het aan het extern station toevoeren van de tweede versleutelinformatie, dat het toegangsstation een derde generator bevat om genoemd eerste bericht onvoorspelbaar te genereren, en een vergelijkelement (42) om het eerste bericht en het tweede hervormd bericht te vergelijken en bij overeenstemming een legitimatiebevestiging te genereren en dat genoemde eerste verontsleutelinformatie en tweede versleutelinformatie voor een aantal externe stations onderling identiek en voorts daarin onuitleesbaar zijn.

2. Draagbaar, extern station, te gebruiken in een kommunikatiesysteem volgens conclusie 1, met het kenmerk dat het als een kredietkaart is gegeometriseerd.

3. Draagbaar station volgens conclusie 2, met het kenmerk, dat het voorzien is van respektievelijke lussen (102, 103) voor kontaktloze overdracht van informatie- en voedingsenergie vanuit een toegangsstation en overdracht van informatie-energie terug naar het toegangsstation, en dat een schuifregister serieel is opgenomen tussen twee van genoemde lussen voor tijdelijke opslag van ontvangen informatie.

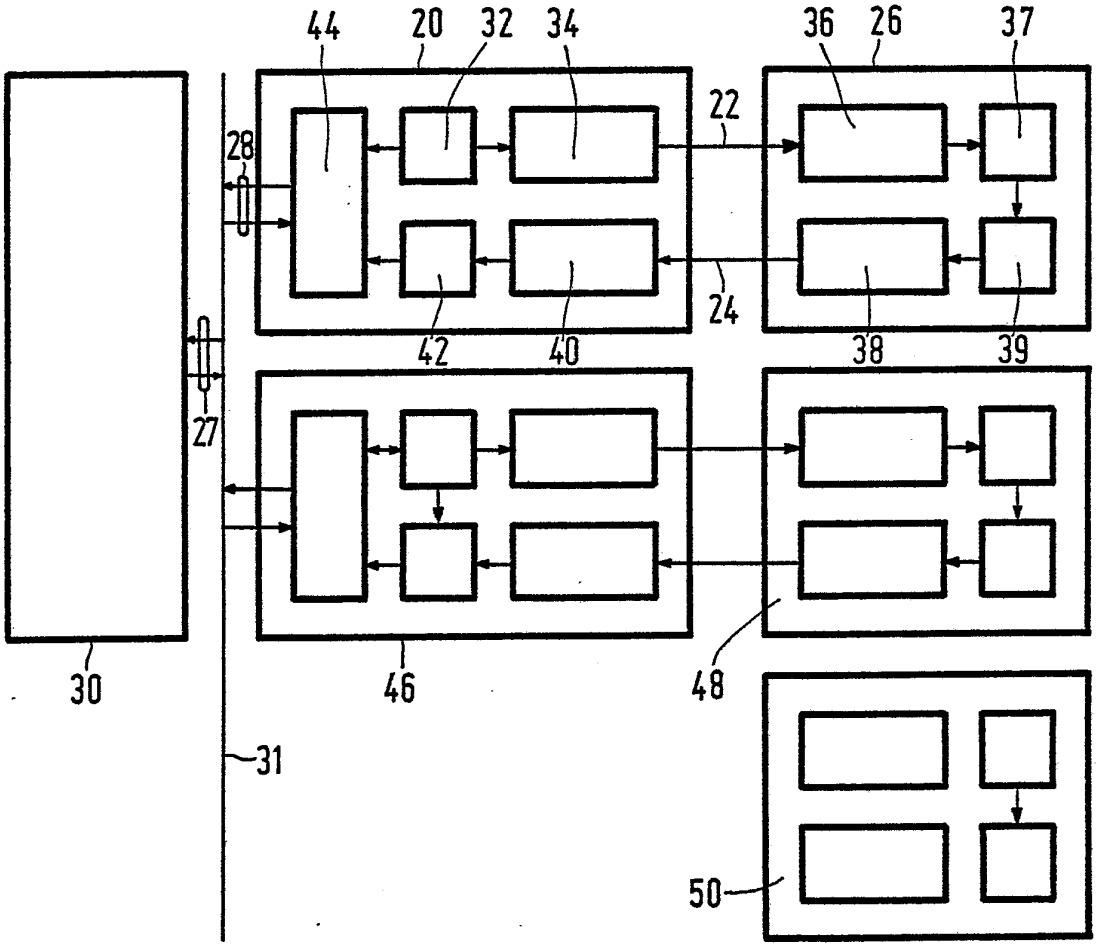

FIG.1

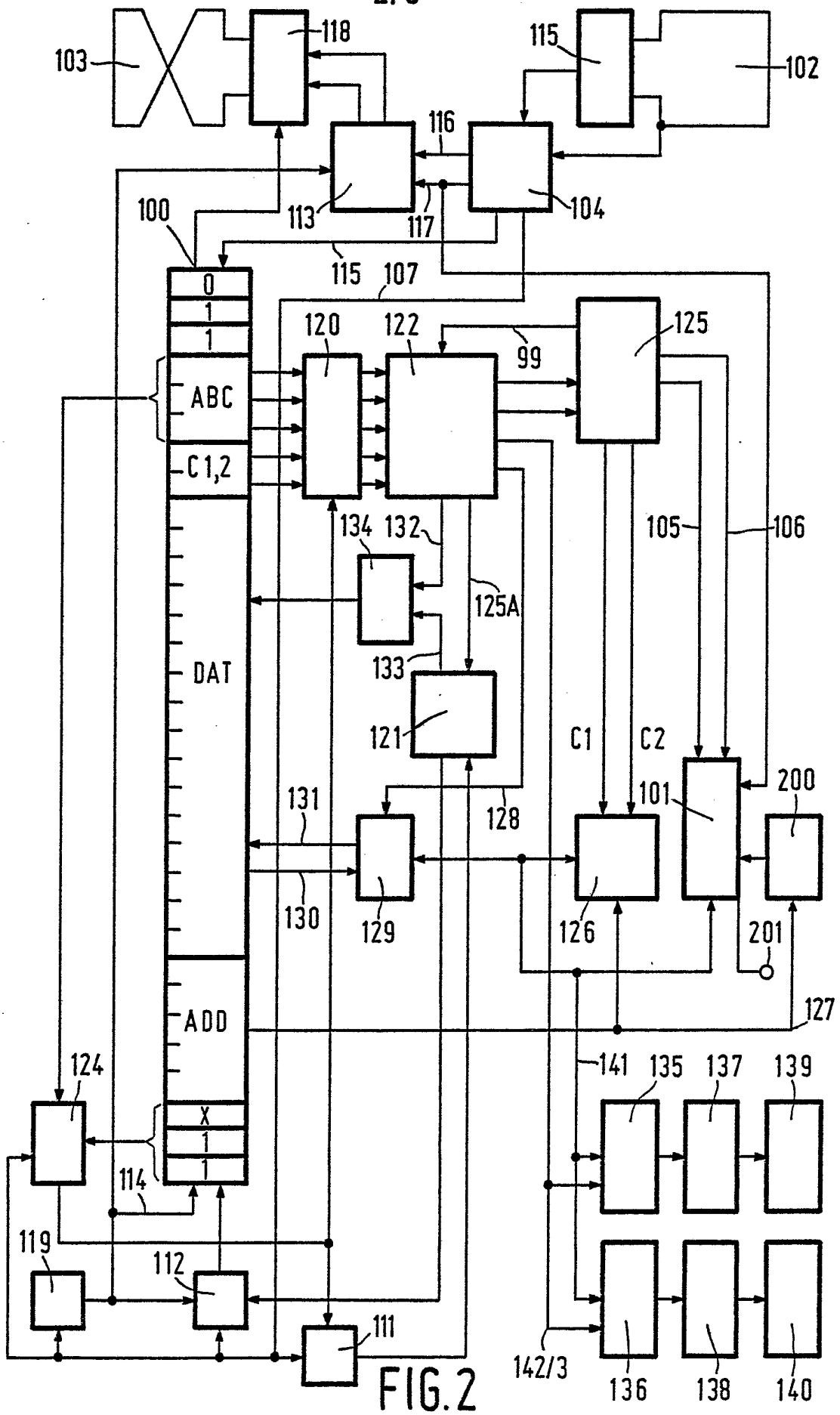
103
118
115
102
116
113
117
104
100
115
107
0
1
1
ABC
C 1,2
120
122
99
125
134
132
105
106
125A
133
121
DAT
C1
C2
200
101
131
128
130
129
126
201
127
ADD
124
141
135
137
139
X
1
1
114
119
112
111
142/3
136
138
140

FIG.2

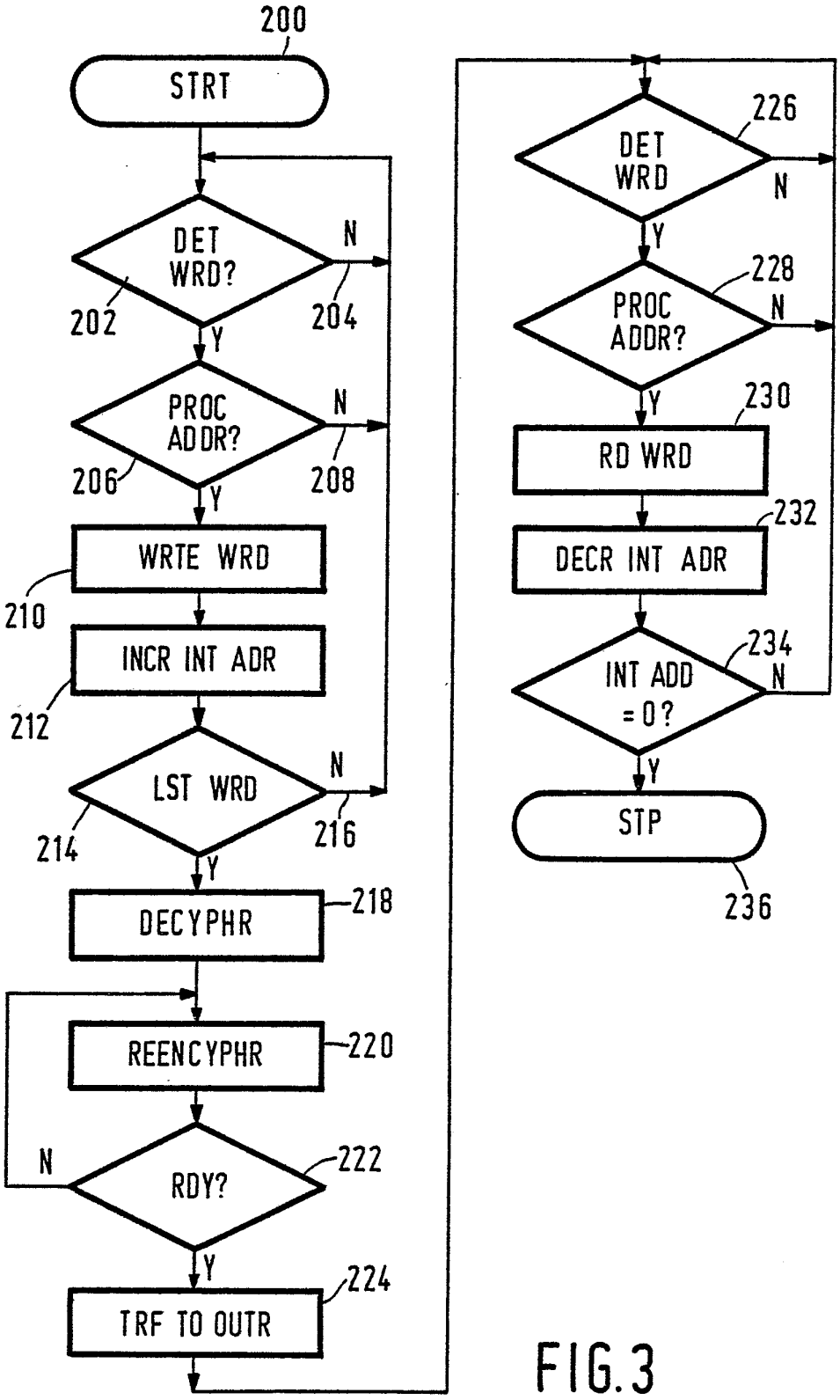
200
STRT
DET WRD?
202
N
204
Y
PROC ADDR?
206
N
208
Y
WRTE WRD
210
INCR INT ADR
212
LST WRD
214
N
216
Y
DECYPHR
218
REENCYPHR
220
N
RDY?
222
Y
TRF TO OUTR
224
DET WRD
226
N
Y
PROC ADDR?
228
N
Y
RD WRD
230
DECR INT ADR
232
INT ADD = 0?
234
N
Y
STP
236

FIG.3