(19) SUOMI - FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN
FINNISH PATENT AND REGISTRATION OFFICE

(10) **FI 885698 A7**

(12) **JULKISEKSI TULLUT PATENTTIHAKEMUS**
PATENTANSÖKAN SOM BLIVIT OFFENTLIG
PATENT APPLICATION MADE AVAILABLE TO THE PUBLIC

(21) Patenttihakemus - Patentansökan - Patent application 885698

(51) Kansainvälinen patenttiluokitus - Internationell patentklassifikation - International patent classification
H04L 9/00

(22) Tekemispäivä - Ingivningsdag - Filing date **09.06.1986**

(23) Saapumispäivä - Ankomstdag - Reception date **08.12.1988**

(41) Tullut julkiseksi - Blivit offentlig - Available to the public **08.12.1988**

(43) Julkaisupäivä - Publiceringsdag - Publication date **12.06.2019**

(86) Kansainvälinen hakemus - Internationell ansökan - International application **09.06.1986 PCT/SE1986/000275**

(71) Hakija - Sökande - Applicant

1 • **Datakonsult i Malmö Ab,** Trollenäsgatan 8 217 73 Malmö, Sverige, SVERIGE, (SE)

(72) Keksijä - Uppfinnare - Inventor

1 • **Santesson, Stefan,** Sverige, SVERIGE, (SE)

(74) Asiamies - Ombud - Agent

Forssén & Salomaa Oy, Lautatarhankatu 8 B, 00580 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning - Title of the invention
Koodaus- ja dekoodauslaite
Krypterings- och dekrypterinsanordning

Koodaus- ja dekoodauslaite
Krypterings- och dekrypterinsanordning

Tämän keksinnön kohteena on sarjamaisesti siirrettyjä tietoja varten tarkoitettu koodauslaite, joka käsittää tulon koodattavaa bittijonoa varten, lähdön koodattua bittijonoa varten, sekoitusyksikön, jossa on ensimmäinen tulo koodattavaa bittijonoa varten, toinen tulo koodibittejä varten mainitun bittijonon koodaamista varten ja lähtö koodattua bittijonoa varten, koodiyksikön, joka käsittää siirtorekisterin ja muistin, jota osoitetaan biteillä siirtorekisteristä.

Keksintöön liittyy myös koodauslaitteeseen liittyvä sarjamaisesti siirrettyjä tietoja varten tarkoitettu dekoodauslaite, joka käsittää tulon dekoodattavaa bittijonoa varten, lähdön dekoodattua bittijonoa varten, sekoitusyksikön, jossa on ensimmäinen tulo dekoodattavaa bittijonoa varten, toinen tulo koodibittejä varten mainitun bittijonon dekoodaamista varten ja lähtö dekoodattua bittijonoa varten, koodiyksikön, joka käsittää siirtorekisterin ja muistin, jota osoitetaan biteillä siirtorekisteristä.

Tietokoneiden käyttö ja erityisesti tietokoneiden välisten tietojen siirto on aiheuttanut vakavia turvallisuusongelmia. On nimittäin suhteellisen yksinkertaista kuunnella tiedonsiirtoa, ja tätä myötä on olemassa vaara, että luottamuksellisia tietoja joutuu vääriin käsiin. Tämän välttämiseksi siirrettävät tiedot koodataan usein.

Tiedonsiirto tapahtuu binaarisessa muodossa ja useimmissa tähän mennessä tunnetuissa koodausjärjestelmissä koodaus tapahtuu bittitasolla siten, että sanoman muodostavien ykkösten ja nollien jono sekoitetaan koodauslaitteessa koodibittien jonon kanssa. Sanoman dekoodauksen yhteydessä koodattu bittijono sekoitetaan saman koodibittijonon kanssa, jolloin sanoma saadaan selväkielisenä.

Tähän mennessä tunnetuissa koodauslaitteissa koodibittien tuottaminen kestää kuitenkin kauan, ja tiedonsiirrossa esiintyy tämän vuoksi vii-

veitä. Tämä aiheuttaa sen, että on joko laskettava nopeutta, jolla lähettäjä lähettää tietoja, tai järjestettävä koodausyksikköön puskureita. Jälkimmäisessä tapauksessa on suoritettava toimenpiteitä sen estämiseksi, ettei tietoja huku vastaanottavan yksikön antaessa signaalin siitä, ettei se ole enää valmis vastaanottamaan tietoja. Toinen vaikeus esiintyy koodibittien tuottamisen synkronisoinnin yhteydessä. Tietyissä laitteissa (ks, esim. GB 1 388 035) tietojensiirto keskeytetään tasaisin aikavälein sen valvomiseksi, että koodauslaitteessa ja dekoodauslaitteessa olevat koodibitit ovat synkronisoituja. Kolmas ongelma syntyy silloin, kun koodaus- ja dekoodauslaite yhdistetään tietojensiirroon keskeytyksen jälkeen. Tämäm yhdistymisen tulee tapahtua mielellään nopeasti ja yksinkertaisesti ilman, että tietoja hukkuu tai että tietoja, jotka antavat ohjeet koodibittien tuottamisesta, siirretään.

Yllämainitut ongelmat aiheuttavat sen, että tunnetut koodauslaitteet ovat hyvin kalliita, koska synkronointi- ja yhdistämisongelmien ratkaisemiseksi vaaditaan monia ja monimutkaisia piirejä ja koska niitä ei voida myöskään käyttää järjestelmissä, joissa edellytetään suuria siirtonopeuksia.

Rinnakkaissiirron yhteydessä yllämainitut synkronointi- ja yhdistämisongelmat on kuitenkin ratkaistu US-patenttiasiakirjassa 4 431 865 esitetyn koodauslaitteen avulla, joka käsittää logiikkayksikön, jossa koodattavat rinnakkaisesti siirretyt sanat sekoitetaan koodisanojen kanssa koodattujen sanojen aikaansaamiseksi. Koodisanat tuotetaan siten, että logiikkayksiköstä tulevat lähtösignaalit, eli koodatut sanat, syötetään osoituspiiriin, joka käsittää rinnakkais-sarjamuuntimen, siirtorekisterin ja valintapiirin. Valintapiiri valitsee osan tai kaikki bitit rekisteristä muistin osoittamista varten, joka sisältää logiikkayksikköön syötettävät koodisanat. Laite sisältää lisäksi tietokoneen, joka hoitaa koodisanojen syötön muistiin ja joka voi tämän syötön aikana sulkea rekisterin ja valintapiirin. Tätä koodauslaitetta vastaava dekoodauslaite on rakennettu vastaavalla tavalla sillä poikkeuksella, että logiikkayksikössä sekoitetaan koodatut sanat koodisanojen kanssa dekoodatun tekstin saamiseksi.

Kuten sanottu, tämä laite on kuitenkin tarkoitettu käytettäväksi rinnakkaisessa tiedonsiirrossa, eikä sitä voida käyttää muutoksitta sarjamuotoisen tiedonsiirron yhteydessä. Laite on lisäksi tarkoitettu kaukokirjoittimien ja vastaavien tietojen koodaukseen. Se ei ole siis tarkoitettu suojaamaan siirrettyjä tietoja epärehellisiltä henkilöiltä, jotka ovat kiinnostuneita käyttämään hyväksi tietoja kaupallisesti ja/tai laittomasti pakottamatta ihmisiä maksamaan liittymismaksua tämäntyyppisten palveluiden käyttämisestä. Ne, jotka onnistuvat dekoodaamaan siirretyt tiedot eivät pääse myöskään käsiksi mihinkään salaisiin tietoihin vaan ainoastaan tietoihin, joita voidaan mahdollisesti hyödyntää omaan käyttöön. Tämän vuoksi tämä laite ei ole suunniteltu täyttämään korkeita turvallisuusvaatimuksia, joita koodauslaitteille on asetettava, jotka on tarkoitettu käytettäviksi tiekoneiden väliseen tietojensiirtoon ja erityisesti sellaisten tietojen siirtoon, joiden tulee pysyä salaisina pitkän aikaa siirron jälkeen ja joita ei siis voida dekoodata jälkikäteen. Yllämainitun laitteen ongelmana on nimittäin se, että jokaista koodattavaa sanaa varten luodaan ainoastaan yksi osoite muistiin ja että tässä osoitteessa olevaa koko sanaa käytetään koodaamiseen. Jos sama tietojono lähetetään useita kertoja peräkkäin, on olemassa vaara, että koodaus tapahtuu samalla tavoin, mikä helpottaa olennaisesti asiaankuulumatonta dekoodausta. Jos dekoodauslaite edelleen varastetaan, mikään ei estä sitä, että aikaisemmin kuunnellut tiedot dekoodataan dekoodauslaitteen avulla.

Tämän keksinnön tavoitteena on tämän vuoksi saada aikaan sarjamaiseen tietojensiirtoon tarkoitettu koodaus- ja dekoodausjärjestelmä, joka täyttää ne erittäin korkeat turvallisuusvaatimukset, jotka asetetaan salaisten tietojen koodaamiseen tarkoitetuille järjestelmille sekä siirron aikana että sen jälkeen, jotka ovat halvempia kuin vastaavat tunnetut järjestelmät ja jotka eivät lisäksi aseta mitään olennaisia rajoituksia siirtonopeudelle ja joissa synkronointi- ja yhdistämisongelmat on ratkaistu.

Tavoite saavutetaan alussa mainitun tyyppisen koodauslaitteen avulla, jolle on tunnusomaista se, että siirtorekisterillä on tulo koodattua bittijonoa varten ja siitä, että koodauslaite edelleen käsittää toisen koodiyksikön, joka on kytketty ensimmäiseen koodiyksikköön ja käsittää

siirtorekisterin ja muistin, jota osoitetaan toisessa koodiyksikössä olevasta siirtorekisteristä tulevilla biteillä ja jonka lähtö on kytketty toiseen tuloon sekoitusyksikköön, sekä alussa mainitun tyyppisen dekoodauslaitteen avulla, jolle on tunnusomaista se, että siirtorekisterillä on tulo dekoodattavaa bittijonoa varten ja että dekoodauslaite edelleen käsittää toisen koodiyksikön, joka on kytketty ensimmäiseen koodiyksikköön ja käsittää siirtorekisterin ja muistin, jota osoitetaan toisessa koodiyksikössä olevasta siirtorekisteristä tulevilla biteillä ja jonka lähtö on kytketty toiseen tuloon sekoitusyksikköön.

Ylläkuvattu koodaus- ja dekoodausjärjestelmä antaa täysin tyydyttävän suojan ulkoa tulevia kuuntelu- ja dekoodausyrityksiä vastaan. Jotta voitaisiin myös taata, että kukaan, jolla on mahdollisuus päästä käsiksi koodatussa muodossa ja selväkielisenä olevaan sanomaan, ei voi selvittää muistin sisältöä käyttääkseen sitä myöhemmin hyväkseen kuunnellun tiedon dekoodaukseen, koodaus- ja dekoodausjärjestelmä voi käsittää lisäkoodiyksikön, jonka tulo on yhdistetty ensimmäiseen koodiyksikköön, joka sisältää siirtorekisterin ja koodibitit sisältävän muistin, jota osoitetaan siirtorekisteristä tulevilla biteillä ja jonka lähtösignaali muodostaa bittijonon koodaamiseen tarkoitetun koodibittien jonon. Kun tällainen ylimääräinen koodiyksikkö otetaan käyttöön, henkilön, joka pääsee käsiksi koodatussa muodossa sekä selväkielisenä olevaan sanomaan, on mahdotonta selvittää molempien koodiyksiköiden muistien sisältö.

Tulisi kuitenkin olla mahdollista, että muistien erityisen ulkonäön selvittämisen sijasta voidaan määrittää paljon suurempi muisti, jonka tulisi voida toimia korvausmuistina molemmille muille muisteille. Yksi tapa tämän ongelman eliminoimiseksi on lisätä niiden bittien lukumäärää, joita tarvitaan siihen, että muistit voisivat saada tietyn osoitteensa. Yhden lisäsuoritusmuodon mukaisesti tämä keksintö käsittää tämän vuoksi molempien koodiyksiköiden välille järjestetyn siirtorekisterin, jonka tulo on yhdistetty ensimmäiseen koodiyksikköön, sekä EXOR-veräjän, joka vastaanottaa tuloissaan bittejä siirtorekisteristä ja jonka lähtö on yhdistetty toisen koodiyksikön siirtorekisteriin. Tällä tavoin osoitteiden lukumäärää korvausmuistiin voidaan lisätä

siten, että tämä muodostuu niin suureksi, että sitä on mahdotonta selvittää kohtuullisessa ajassa.

Lisäongelma, joka ratkaistaan tämän keksinnön avulla, liittyy sentyyppisiin tietoihin, jotka tulee pitää salaisina pitkän aikaa siirron jälkeen. Tähän mennessä tunnettuihin laitteisiin liittyy nimittäin vaara, että joku kuuntelee tiedonsiirtoa, varastaa myöhemmin dekoodauslaitteen ja dekoodaa myöhemmin kuunnellut tiedot. Tämän estämiseksi esillä oleva keksintö käsittää lisäsuoritusmuodon mukaisesti molempien koodiyksiköiden välille järjestetyn siirtorekisterin, jonka tulo on yhdistetty ensimmäiseen koodiyksikköön, sekä luku- ja kirjoitusmuistin, jota osoitetaan biteillä siirtorekisteristä ja jonka lähtö on yhdistetty toiseen koodiyksikköön. Laite sisältää lisäksi tietokoneen, joka on järjestetty tuottamaan koodibittejä ennaltamääritetyn algoritmin mukaisesti ja kirjoittamaan tuotetut koodibitit muistiin tasaisin väliajoin. Jos algoritmi on sellaista tyyppiä, joka tuottaa koodin, jota ei voida jäljittää matemaattisesti ajassa taaksepäin, dekoodauslaitteella on mahdotonta dekoodata aikaisemmin kuunneltuja tietoja. Tätä myötä täytetään turvallisuusvaatimus, joka edellyttää, että tiedot pysyvät salaisina siirron jälkeen.

Tämän keksinnön mukaisessa järjestelmässä aikaisemmin tunnettuun tekniikkaan liittyvät ongelmat on ratkaistu. Tämän vuoksi ei tarvita mitään erityisiä piirejä puskurointiin tai ohjaus-, valvonta- ja synkronointisignaaleiden käsittelyyn, vaan järjestelmä voidaan rakentaa muutamista standardipiireistä, minkä vuoksi järjestelmä on huomattavasti halvempi kuin muut vastaavat järjestelmät.

Esillä olevaa keksintöä kuvataan nyt suoritusmuotoesimerkin avulla oheisiin piirustuksiin viitaten. Kuvio 1 on lohkokaavio esillä olevan keksinnön mukaisesta koodauslaitteesta. Kuvio 2 on lohkokaavio kuvion 1 koodauslaitetta vastaavasta dekoodauslaitteesta. Kuvio 3 on lohkokaavio, joka esittää koodauslaitteen yhden suoritusmuodon kaksinkertaisilla koodausyksiköillä varustettuna. Kuvio 4 on lohkokaavio, joka esittää koodauslaitteen suoritusmuotoa varustettuna siirtorekisterillä ja koodiyksiköiden välisellä EXOR-veräjällä. Kuvio 5 on lohkokaavio, joka esittää koodauslaitteen yhtä suoritusmuotoa varustettuna siirto-

rekisterillä ja molempien koodiyksiköiden välisellä ohjelmoitavalla muistilla. Kuvio 6 on lohkokaavio, joka esittää koodauslaitteen yhtä suoritusmuotoa, joka käsittää molempien koodiyksiköiden välisen koodinkäsittelyjärjestelmän.

Kuviossa 1 esitetään koodauslaite, joka on tarkoitettu kytkettäväksi lähettävän ja vastaanottavan yksikön väliseen anneyhteyteen lähettävälle puolelle. Tämä koodauslaite sisältää olennaisesti tulon 1 lähettävältä yksiköltä tulevia selväkielisiä tietoja varten, lähdön 2 koodattuja tietoja varten, sekoitusyksikön 3, joka muodostuu EXOR-veräjästä, koodiyksiköstä 4 koodibittijonossa olevien koodibittien tuottamiseksi sekä elimistä 6,7,8, jotka ohjaavat laitteen tiettyjä valintoja ja joita kuvataan alla tarkemmin. Koodiyksikkö 4, jonka tulo on kytketty sekoitusyksikön 3 lähtöön, muodostuu 16-bittisestä siirtorekisteristä 9, muistista 5, joka voi olla vaihtosäesteinen ROM tai EPROM, sekä limittimestä 10. Siirtorekisterin 9 kolmetoista ensimmäistä bittiä on kytketty muistin 5 osoitetuloihin ja sen kolme viimeistä bittiä on kytketty limittimen 10 osoitetuloihin. Muistin 5 lähdöt on kytketty limittimen 10 tietotuloihin. Kuten yllä on mainittu, koodauslaitteessa voidaan suorittaa tiettyjä valintoja. Valinnat koskevat sitä, koodataanko tuleva tietobitti vai ei sekä ladataanko koodattu bitti siirtorekisteriin 9 vai ei. Valintoja ohjaa ohjausyksikkö 8, joka on ohjelmoitava. Sen ohjelma noudattaa sanaa (sana = vaihto) koodauksen välityksellä ja käynnistyy uudelleen seuraavan sanan alusta. Jokaista sanassa olevaa bittiä varten lähetetään signaali tuloon elimeen 7, joka voi muodostua loogisesta JA-veräjästä sen määrittämiseksi, koodataanko bitti vai ei, sekä signaalista elimen 6 tuloon, joka voi muodostua samaten JA-veräjästä sen määrittämiseksi, ladataanko koodattu bitti rekisteriin vai ei. Veräjä 7 vastaanottaa toiseen tuloonsa koodibitin limittimeltä 10, ja sen lähtö on kytketty sekoitusyksikköön 3. Veräjän 6 lähtö on kytketty rekisterissä 9 olevaan aktivointituloon.

Kuviossa 2 esitetty dekoodauslaite on tarkoitettu kytkettäväksi sen anneyhteyden toiseen päähän, johon koodauslaite on kytketty ennen vastaanottavaa yksikköä. Laite vastaanottaa tuloonsa 11 koodattuja tietoja koodauslaitteesta ja luovuttaa lähdöstään 12 dekoodattuja

tietoja vastaanottavalle yksikölle. Dekoodausyksikkö on rakennettu samalla tavoin kuin koodauslaite sillä poikkeuksella, että siirtorekisteri 19 on kytketty tuloon 11. Molemmat laitteet koostuvat siis ylipäätänsä samoista komponenteista ja sisältävät samat tiedot (muisteissa ja ohjausyksiköissä), minkä vuoksi dekoodauslaitetta ei tässä yhteydessä kuvata tarkemmin.

Seuraavassa kuvataan koodausjärjestelmän toimintaa aluksi koodibittien tuottamisesta lähtien. Koodausjärjestelmän ollessa toiminnassa siirtorekisteri 9 ladataan sekoitusyksikön 3 lähdöstä tulevilla koditetuilla biteillä. Rekisterissä olevilla kolmellatoista ensimmäisellä bitillä osoitetaan muistin 5 muistisolu. Muistisolun sisältö luovutetaan limittimen 10 tietotuloihin, joka valitsee rekisterissä 9 olevan kolmen viimeisen bitin avulla, mitkä osoitetussa muistisanassa olevasta kahdeksasta bitistä muodostavat koodibitin.

Tämä koodibitin muodostamistapa toimii myös ennen kuin muita koodibittejä on ehditty ladata siirtorekisteriin 9 sekoitusyksikön 3 lähdöstä, koska jopa pelkästään nollat voivat muodostaa osoitteen muistiin ja limittimeen. Mitään erityistä aloitusrutiinia ei näin muodoin vaadita ennen koodausjärjestelmän käynnistämistä.

Kun koodattavan bittijonon bitti esitetään sekoitusyksikön 3 tuloon, ohjausyksikkö 8 luovuttaa veräjälle 7 signaalin, joka ilmoittaa, siirretäänkö limittimen 10 lähdössä oleva koodibitti sekoitusyksikön 3 tuloon ja sekoitetaan varsinaisen bitin kanssa, vai ohittaako tämä bitti sekoitusyksikön koodaamattomasti. Tämä valinta, jonka avulla bitti koodataan tai jonka avulla bittiä ei koodata, tekee järjestelmästä vielä varmemman ja mahdollistaa lisäksi sen, että esimerkiksi käynnistys- ja pysäytysbitit voivat ohittua koodaamattomina.

Ohjausyksikkö 8 luovuttaa edelleen signaalin veräjälle 6, joka ilmoittaa, ladataanko varsinainen bitti rekisteriin 9 vai ei sen ohitettua sekoitusyksikön 3. Jos bitti ladataan rekisteriin, muistin 5 ja limittimen 10 osoite muuttuu ja saadaan uusi koodibitti. Tietyissä tapauksissa voi olla suositeltavaa olla lataamatta bittejä sekoitusyksiköstä 3 rekisteriin 9 esimerkiksi lähtö- ja lopetusbittien yh-

teydessä, jotka koodittamattomina ohittaessaan näyttävät aina samanlaisilta. Tämän myötä järjestelmän turvallisuus lisääntyy.

Dekoodauslaite toimii samalla tavalla. Koska ohjelma on sama kuin ohjausyksikössä 18, samat bitit ladataan rekisteriin 19, samat muistisolut osoitetaan muistiin 15, jonka sisällön on luonnollisesti oltava sama kuin koodauslaiteen muistin 5 sisällön, tuotetaan samat koodibitit ja samat bitit ohittavat koodittamattomina sekoitusyksikön 13. Kooditetut bitit sekoitetaan siis samojen koodibittien kanssa kuin jotka sekoitettiin koodauslaitteessa olevien bittien kanssa, ja koska sekoitusyksikkö muodostuu EXOR-veräjästä, tämän lähtöön saadaan uudestaan alkuperäinen sanoma selväkielisenä.

Jos anneyhteyteen syntyisi väliaikainen keskeytys, ainoastaan ne tiedot, jotka syötetään ulos katkoksen aikan, häviäsivät. Kun kontakti toistetaan, molempien rekistereiden 9,19 sisältö voi olla täysin erilainen, mutta koska samat tiedot syötetään molempiin rekistereihin, laitteet synkronisoituvat jälleen pian. Laitteen synkronisoitumisaika riippuu ohjausyksikön ohjelmasta ja siirtorekisterin pituudesta. Tässä suoritusmuodossa tämä kestää max. kolme sanaa (yksi sana = yksi vaihto).

Ylläkuvattu koodausjärjestelmä on hyvin nopea. On mahdollista kommunikoida nopeudella jopa 2 MBaud dupleksi. Koodauslaitteen viive on minimaalinen. Tietobitti jättää sekoitusyksikön koodattuna arvon T/2 mukaan, joss T = se aika, jona tietobitti on aktiivinen. Tämä lyhyt viiveaika aiheuttaa sen, että portin RS-232 kättelylinjoja ei enää tarvitse käsitellä koodauslaitteessa vaan, että ne lähetetään vain käsittelemättöminä suoraan koodauslaitteen läpi.

Huolimatta siitä, että koodausjärjestelmä on niin yksinkertaisesti rakennettu, se on täysin turvallinen myös sille, joka tuntee tarkasti kuinka se toimii. Koodauksen tulos riippuu koodattavasta sanomasta, muistin 5 sisällöstä ja ohjausyksikön 8 ohjelmasta. Jotta sanomat voitaisiin dekoodata, on oltava täten mahdollisuus päästä käsiksi muistin sisältöön ja ohjausyksikön ohjelmaan. Jos on olemassa pienintäkään epäilystä siitä, että muistin ja/tai ohjausyksikön sisältö

olisi tunnettu, muisti ja ohjausyksikön sisältö voidaan vaihtaa hyvin yksinkertaisesti. Ohjausyksikköön voi olla tallennettuina myös useita ohjelmia, jotka kytketään vuorotellen sisään ohjausyksikköön kuuluvan näppäimistön avulla.

Kuviossa 3 esitetään koodauslaitteen suoritusmuoto, joka estää sen, ettei kukaan, joka pääsee käsiksi selväkielisenä tai kooditetussa muodossa olevaan sanomaan, pysty selvittämään muistin sisältöä käyttämällä kaavaa "selväkielisenä EXOR koodattu teksti = koodi". Kuviossa 3 esitetään uudelleen kuviossa 1 esitetyt komponentit samoin viitenumeroin. Näillä yksiköillä on sama tehtävä kuin kuviossa 1 esitetyllä laitteella, joten sitä ei tämän vuoksi kuvata. Näiden komponenttien lisäksi laite käsittää toisen koodiyksikön 4', jonka tulo on kytketty ensimmäisen koodiyksikön 4 lähtöön ja joka on rakennettu samalla tavoin kuin tämä, nimittäin 16-bittisestä siirtorekisteristä 9', muistista 5', joka voi olla vaihtojärjestetty ROM tai EPROM, ja limittimestä 10'. Tässä keksinnön suoritusmuodossa koodiyksikön 4 tuottamat koodibitit syötetään siirtorekisteriin 9', jonka kolmetoista ensimmäistä bittiä käytetään muistin 5' osoittamiseen ja jonka kolme viimeistä bittiä toimivat tulosignaalina limittimeen 10' sen valitsemiseksi, mikä muistiin 5' osoitetun sanan bitti muodostaa koodibitin. Laitteen tässä suoritusmuodossa osoitteet ensimmäisessä koodiyksikössä olevaan muistiyksikköön 9 ja toisen koodiyksikön muistista 5' tulevat koodit eivät ole millään luettavalla tavalla suhteessa toisiinsa, ja tätä myötä on mahdotonta tulosignaalien kuuntelemisen kautta sekä järjestelmän lähtösignaalien kautta selvittää muistien 5 ja 5' sisältö. Tätä koodauslaitetta vastaava dekoodauslaite on rakennettu vastaavalla tavalla, joten sitä ei tämän vuoksi kuvata.

Kuviossa 4 on kuviossa 3 esitetty laite varustettu lisäksi siirtorekisterillä 40 ja EXOR-veräjällä 41. Siirtorekisteri 40 vastaanottaa tuloonsa koodiyksikön 4 tuottamat koodibitit. Siirtorekisterin 40 ensimmäistä ja viimeistä bittiä käytetään tulosignaaleina EXOR-veräjään 41, jonka lähtö on kytketty siirtorekisteriin 9' toiseen koodiyksikköön 4'. Kun nämä molemmat komponentit on sisällytetty laitteeseen, osoitteiden lukumäärä lisääntyy hyvin voimakkaasti, joita tarvittaisiin korvausmuistin luomiseksi muisteille 5 ja 5'. Jos siirtore-

kisterin 40 ja siirtorekistereiden 9 ja 9' pituus valitaan 16 bitiksi, tarvittavien osoitteiden lukumääräksi tulee $2,81 \times 10^{14}$. Kun siirtorekisteri 40 ja EXOR-veräjä 41 on tuotu mukaan, on mahdotonta kohtuullisessa ajassa luoda korjausmuisti molemmille muille muisteille. Kun järjestelmää käytetään oikein, eliminoituu lisäksi vaara, että koodausohjelmassa olevia tietoja syötetään ajoittain ulos selväkielisten tietojen sisäänsyötön yhteydessä pidentämällä rekisteriä siirtorekisterillä 40. Dekoodauslaitteella, jota ei ole esitetty, on vastaavasti siirtorekisteri ja EXOR-veräjä, jotka on kytketty samalla tavalla.

Kuviossa 5 esitetään vaihtoehto kuviossa 4 esitetystä laitteesta, EXOR-veräjä 41 on korvattu luku- ja kirjoitusmuistilla 42, jota osoitetaan siirtorekisterin 40 muistilla ja jonka lähtö on yhdistetty toisen koodiyksikön 4' siirtorekisteriin 9'. Muistissa 42 olevat tiedot voidaan vaihtaa ohjelmoimalla sisään uusi koodi näppäimistöllä 43. Muistin 42 tarkoituksena on että, siirretyjä, koodattuja tietoja ei voida jälkikäteen dekoodata, jos joku, joka on kuunnellut siirretyt tiedot, myöhemmin hankkii itselleen dekoodauslaitteen. Sanoman dekoodaamiseksi on nimittäin päästävä käsiksi siihen koodiin, joka on muistissa 42 koodauksen yhteydessä, ja jos tätä koodia muutetaan tasaisin väliajoin, jälkeenpäin tapahtuva dekoodaus tulee mahdottomaksi. Ainoa asia, joka on varmistettava, on että muistin on sisällettävä riittävän paljon koodeja siten, että jälkeenpäin tapahtuva koodaus ei voi tapahtua kokeilemalla kaikkia mahdollisia koodeja, jotka muisti voisi sisältää. Samoin kuin muissa suoritusmuotoesimerkeissä ei-esitetty dekoodauslaite on rakennettu vastaavalla tavalla.

Kuviossa 6 esitetään kuviossa 5 esitetyn koodauslaitteen muunnos, joka eliminoi ne käytännön ongelmat, jotka liittyvät niiden koodien käsittelyyn ja siirtoon dekoodauslaitteeseen, jotka syötetään muistiin 42, sekä siihen työpanokseen, joka sisältyy koodien syöttämiseen tasaisin väliajoin. Kuviossa 6 esitettyyn koodauslaitteen muunnokseen sisältyy siirtorekisterin 40 ja muistin 42 lisäksi tietokone 43, jolla on tulo, joka on kytketty johtimen 51 kautta sekoitusyksikön 3 lähtöön, osoitelähdöt, jotka on osoiteväylän 44 kautta yhdistetty muistiin 42, tulo/lähtö, joka on yhdistetty tietojohtimen 45 kautta muistiin 42, ja ohjaussignaalilähtö luku/kirjoitussignaalin siirtämiseksi johtimella

46 muistiin 42. Laite käsittää edelleen siirtorekisteriin 40 yhdistetyn puskurin 47, johon siirtorekisterin sisältö välitallennetaan ja jolla on kolmitilalähdöt, jotka on kytkettävissä osoiteväylään 44. Laite käsittää vielä kellon 48, joka on ohjelmoitavissa tietokoneesta 43, joka voi olla nopealla ja haihtuvalla muistilla varustettu yhden piipalan tietokone. Tietokoneen muistissa on ohjelman muotoon tallennettuna algiritmi, jonka avulla tietokone luo uuden koodin muistille 42. Koodi luodaan eri aikavälein, jolloin varsinaisen ajanjakson pituus määrittyy edellisen ajanjakson aikana luodulla koodilla ja jolloin kelloa 48 käytetään ajanjakson loppumisen määrittämiseen. Kun ajanjakson aikana tuotettu koodi on luotu valmiiksi, se välitallennetaan odottamaan siirtoa muistiin 42. Tietokone 43 määrittää sopivat ajankohdat siirtoa varten analysoimalla signaalit sekoitusyksikön 3 lähdöstä. Kun ennaltamääritetty tapahtuma, esimerkiksi että lähdössä ei ole yhtään signaalia, tapahtuu, tapahtuu välitallennetun koodin siirtäminen muistiin. Tietokone kytkee tällöin puskurin 47 lähdöt pois osoiteväylältä johtimella 50 olevan ohjaussignaalin avulla, antaa kirjoitussignaalin johtimelle 46 ja osoittaa muistia osoiteväylän 44 kautta siten, että tuotettu koodi voidaan siirtää muistiin 42 tietojohtimen 45 kautta.

Tätä koodauslaitteen suoritusmuotoa vastaava ei-esitetty dekoodauslaite on rakennettu vastaavalla tavalla varustettuna siirtorekisterillä, puskurilla, tietokoneella, muistilla, jne. Dekoodauslaitteen tietokone tuottaa uuden koodin muistiinsa saman algoritmin avulla, jota koodauslaitteen 43 tietokone käyttää. Dekoodauslaitteen tietokone käyttää edelleen samoja kriteereitä kuin tietokone 32 päättäessään milloin uuden koodin syöttäminen muistiin tapahtuu. Molempien muistien sisältö on näin aina sama.

Huomautettakoon myös, että koodi, joka estää aikaisemmin kuunnellun tiedon dekoodaamisen, on tuotettava siten, että sitä ei voida jäljittää matemaattisesti taaksepäin ajassa. Tämän alan asiantuntijat tuntevat tämäntyyppiset algoritmit, joten niitä ei kuvata tässä yhteydessä lähemmin.

Kuten on mainittu, tämän koodintuottamismenetelmän etuna on se, että

tiedot voidaan pitää salaisina myös siirtämisen jälkeen ja edelleen että laitteiden välille ei tarvitse siirtää mitään koodia sekä että koodin tuottaminen ei ole riippuvainen koodauslaitteen ja dekoodauslaitteen välisen siirtojohtimen tiedoista, vaikka tämä tapahtuu kuitenkin synkronisesti molemmissa laitteissa.

Sen ilmoittamiseksi, milloin uusi koodi on valmis, kelloa 48 käytetään lisäksi synkronisointitarkoituksiin. Synkronisointi tapahtuu siten, että tiettyjä ennaltamääritettyjä tapahtumia, esimerkiksi tiettyjä bittimalleja tai tiedonsiirron keskeytystä, käytetään aikaviitteinä molempien laitteiden kelloille. Kun tällainen ennaltamääritetty tapahtuma tapahtuu, kello asettuu tiettyyn tilaan. Tämän synkronisointitavan etuna on se, että tietoja, jotka ovat yhteisiä molemmille laitteille, käytetään hyväksi, jonka ansiosta synkronisointi tapahtuu hyvin tarkasti.

Monia muunnelmia ja muutoksia voidaan luonnollisesti toteuttaa tämän keksinnön yhteydessä poikkeamatta silti jäljempänä esitettävistä patenttivaatimuksista, ja tämän vuoksi ylläoleva kuvaus tulee käsittää ainoastaan esimerkkinä, joka ei ole millään tavoin rajoittava. Voidaan kytkeä esimerkiksi sarjassa enemmän kuin kaksi koodiyksikköä ja järjestää komponentteja kuvioiden 4-6 mukaisesti rajoittavien koodiyksiköiden jokaisen parin välille.

L5

Patenttivaatimukset

1. Sarjamaisesti siirrettyjä tietoja varten tarkoitettu koodauslaite, joka käsittää tulon (1) koodattavaa bittijonoa varten, lähdön (2) koodattua bittijonoa varten, sekoitusyksikön (3), jossa on ensimmäinen tulo koodattavaa bittijonoa varten, toinen tulo koodibittejä varten mainitun bittijonon koodaamista varten ja lähtö koodattua bittijonoa varten, koodiyksikön (4), joka käsittää siirtorekisterin (9) ja muistin (5), jota osoitetaan biteillä siirtorekisteristä (9), t u n n e t t u siitä, että siirtorekisterillä (9) on tulo koodattua bittijonoa varten ja siitä, että koodauslaite edelleen käsittää toisen koodiyksikön (4'), joka on kytketty ensimmäiseen koodiyksikköön (4) ja käsittää siirtorekisterin (9') ja muistin (5'), jota osoitetaan toisessa koodiyksikössä olevasta siirtorekisteristä (9') tulevilla biteillä ja jonka lähtö on kytketty toiseen tuloon sekoitusyksikköön (3).

2. Patenttivaatimuksen 1 mukainen koodauslaite, t u n n e t t u kolmannesta siirtorekisteristä (40), joka on järjestetty molempien koodiyksiköiden (4,4') väliin ja jonka tulo on kytketty ensimmäiseen koodiyksikköön (4), ja EXOR-veräjästä (41), joka vastaanottaa tuloillaan bittejä siirtorekisteristä (40) ja jonka lähtö on kytketty toisen koodiyksikön (4') siirtorekisteriin (9').

3. Patenttivaatimuksen 1 mukainen koodauslaite, t u n n e t t u molempien koodiyksiköiden (4,4') väliin järjestetystä siirtorekisteristä (40), jonka tulo on kytketty ensimmäiseen koodiyksikköön (4), ja luku- ja kirjoitusmuistista (42), jota osoitetaan biteillä siirtorekisteristä (40) ja jonka lähtö on kytketty toisen koodiyksikön (4') siirtorekisteriin (9').

4. Patenttivaatimuksen 3 mukainen koodauslaite, t u n n e t t u tietokoneesta (43), joka on järjestetty tuottamaan koodibittejä ennaltamääritetyn algoritmin mukaisesti sekä kirjoittamaan tuotetut koodibitit muistiin (42).

5. Sarjamaisesti siirrettyjä tietoja varten tarkoitettu dekoodaus-

laite, joka käsittää tulon (11) dekoodattavaa bittijonoa varten, lähdön (12) dekoodattua bittijonoa varten, sekoitusyksikön (13), jossa on ensimmäinen tulo dekoodattavaa bittijonoa varten, toinen tulo koodibittejä varten mainitun bittijonon dekoodaamista varten ja lähtö dekoodattua bittijonoa varten, koodiyksikön (14), joka käsittää siirtorekisterin (19) ja muistin (15), jota osoitetaan biteillä siirtorekisteristä (19), t u n n e t t u siitä, että siirtorekisterillä (19) on tulo dekoodattavaa bittijonoa varten ja että dekoodauslaite edelleen käsittää toisen koodiyksikön, joka on kytketty ensimmäiseen koodiyksikköön (14) ja käsittää siirtorekisterin ja muistin, jota osoitetaan toisessa koodiyksikössä olevasta siirtorekisteristä tulevilla biteillä ja jonka lähtö on kytketty toiseen tuloon sekoitusyksikköön (13).

6. Patenttivaatimuksen 5 mukainen dekoodauslaite, t u n n e t t u molempien koodiyksiköiden (14) väliin järjestetystä siirtorekisteristä, jonka tulo on kytketty ensimmäiseen koodiyksikköön (14), ja EXOR-veräjästä, joka vastaanottaa tuloillaan bittejä siirtorekisteristä ja jonka lähtö on kytketty toisen koodiyksikön siirtorekisteriin.

7. Patenttivaatimuksen 5 mukainen dekoodauslaite, t u n n e t t u molempien koodiyksiköiden (14) väliin järjestetystä siirtorekisteristä, jonka tulo on kytketty ensimmäiseen koodiyksikköön (14), ja luku- ja kirjoitusmuistista, jota osoitetaan biteillä siirtorekisteristä ja jonka lähtö on kytketty toisen koodiyksikön siirtorekisteriin.

8. Patenttivaatimuksen 7 mukainen dekoodauslaite, t u n n e t t u tietokoneesta, joka on järjestetty tuottamaan koodibittejä ennaltamääritetyn algoritmin mukaisesti sekä kirjoittamaan tuotetut koodibitit luku- ja kirjoitusmuistiin.

L6

Patentkrav

1. Krypteringsanordning för seriellt överförd information innefattande en ingång (1) för en följd av bitar, som skall krypteras, en utgång (2) för den krypterade bitföljden, en blandningsenhet (3) med en första ingång för följden av bitar som skall krypteras, en andra ingång för kodbitar för kryptering av nämnda bitföljd och en utgång för den krypterade bitföljden, en första kodenhet (4), som innefattar ett skiftregister (9) och ett minne (5), som adresseras med bitar från skiftregistret (9), k ä n n e t e c k n a d av att skiftregistret (9) har en ingång för den krypterade bitföljden och av att krypteringsanordningen vidare innefattar en andra kodenhet (4'), som är ansluten till den första kodenheten och innefattar ett skiftregister (9') och ett minne (5'), vilket adresseras med bitar från skiftregistret (9') i den andra kodenheten, och vars utgång är ansluten till den andra ingånden till blandningsenheten (3).

2. Krypteringsanordning enligt patentkrav 1, k ä n n e t e c k n a d av ett tredje skiftregister (40), vilket är anordnat mellan de båda kodenheterna (4,4') och vars ingång är ansluten till den första kodenheten (4), och en EXOR-grind (41), vilken på sina ingångar mottar bitar från skiftregistret (40) och vars utgång är ansluten till den andra kodenhetens (4') skiftregister (9').

3. Krypteringsanordning enligt patentkrav 1, k ä n n e t e c k n a d av ett mellan de båda kodenheterna (4,4') anordnat skiftregister (40), vars ingång är ansluten till den första kodenheten (4), och ett läs- och skrivminne (42), vilket adresseras med bitar från skiftregistret (40) och vars utgång är ansluten till den andra kodenhetens (4') skiftregister (9').

4. Krypteringsanordning enligt patentkrav 3, k ä n n e t e c k n a d av en dator (43), vilken är anordnad att alstra kodbitar enligt en förutbestämd algoritm och att skriva in de alstrade kodbitarna i minnet (42).

5. Dekrypteringsanordning för seriellt överförd information, innefat-

tande en ingång (11) för en följd av bitar, som skall dekrypteras, en utgång (12) för den dekrypterade bitföljden, en blandningsenhet (13) med en första ingång för följden av bitar som skall dekrypteras, en andra ingång för kodbitar för dekryptering av nämnda bitföljd och en utgång för den dekrypterade bitföljden, en första kodenhet (14), som innefattar ett skiftregister (19) och ett minne (15), som adresseras med bitar från skiftregistret, k ä n n e t e c k n a d av att skiftregistret (19) har en ingång för bitföljden som skall dekrypteras och av att dekrypteringsanordningen vidare innefattar en andra kodenhet, som är ansluten till den första kodenheten (14) och innefattar ett skiftregister och ett minne, vilket adresseras med bitar från skiftregistret i den andra kodenheten och vars utgång är ansluten till den andra ingången till blandningsenheten (13).

6. Dekrypteringsanordning enligt patentkrav 5, k ä n n e t e c k n a d av ett mellan de båda kodenheterna (14) anordnat skiftregister, vars ingång är ansluten till den första kodenheten (14), och en EXOR-grind, vilken på sina ingångar mottar bitar från skiftregistret och vars utgång är ansluten till den andra kodenhetens skiftregister.

7. Dekrypteringsanordning enligt patentkrav 5, k ä n n e t e c k n a d av ett mellan de båda kodenheterna (14) anordnat skiftregister, vars ingång är ansluten till den första kodenheten (14), och ett läs- och skrivminne, vilket adresseras med bitar från skiftregistret och vars utgång är ansluten till den andra kodenhetens skiftregister.

8. Dekrypteringsanordning enligt patentkrav 7, k ä n n e t e c k n a d av en dator, vilken är anordnad att alstra kodbitar enligt en förutbestämd algoritm och att skriva in de alstrade kodbitarna i läs- och skrivminnet.

Fig.1

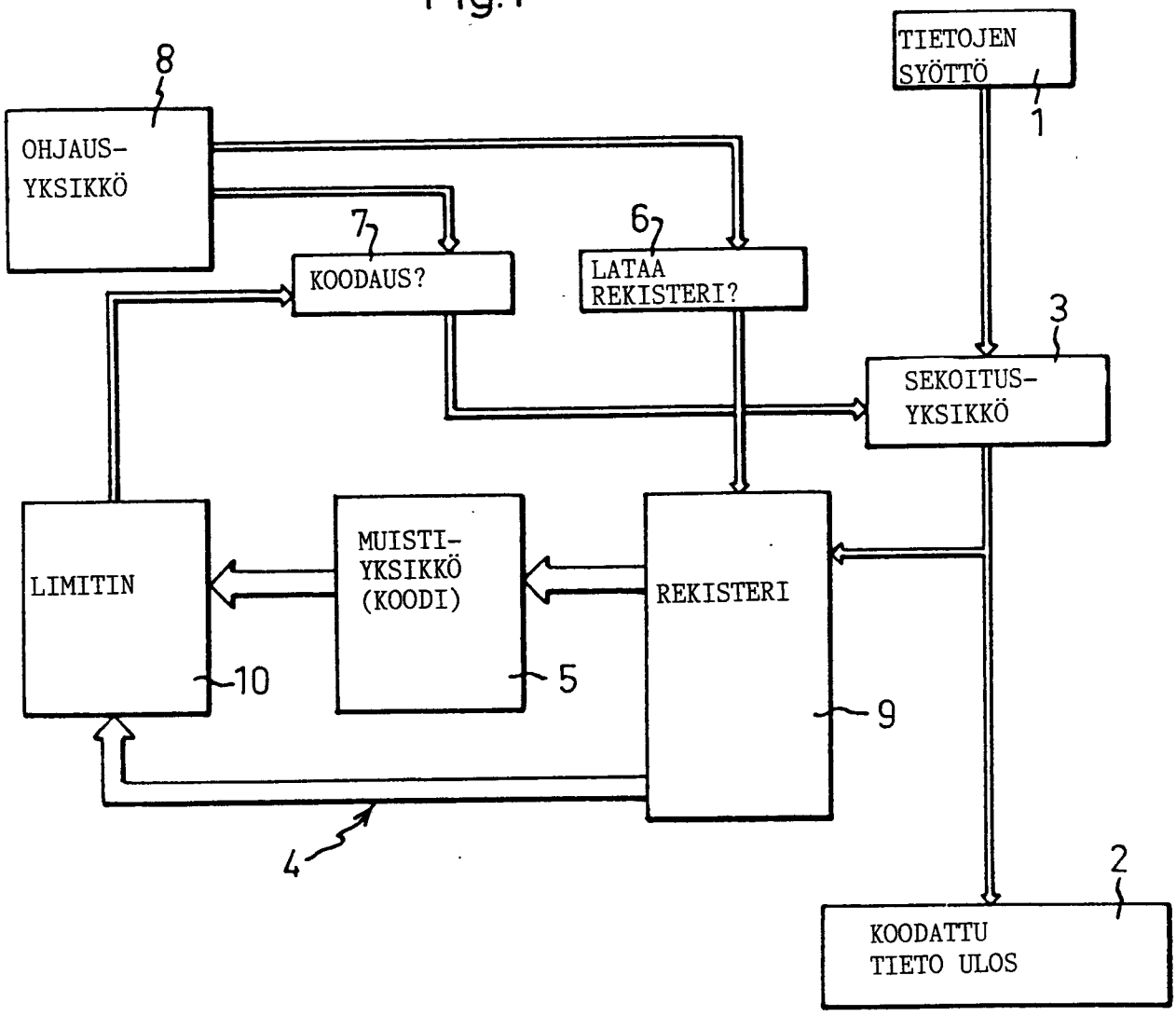

TIETOJEN SYÖTTÖ
1
8
OHJAUS-YKSIKKÖ
7
KOODAUS?
6
LATAA REKISTERI?
3
SEKOITUS-YKSIKKÖ
LIMITIN
10
MUISTI-YKSIKKÖ (KOODI)
5
REKISTERI
9
4
2
KOODATTU TIETO ULOS

Fig.2

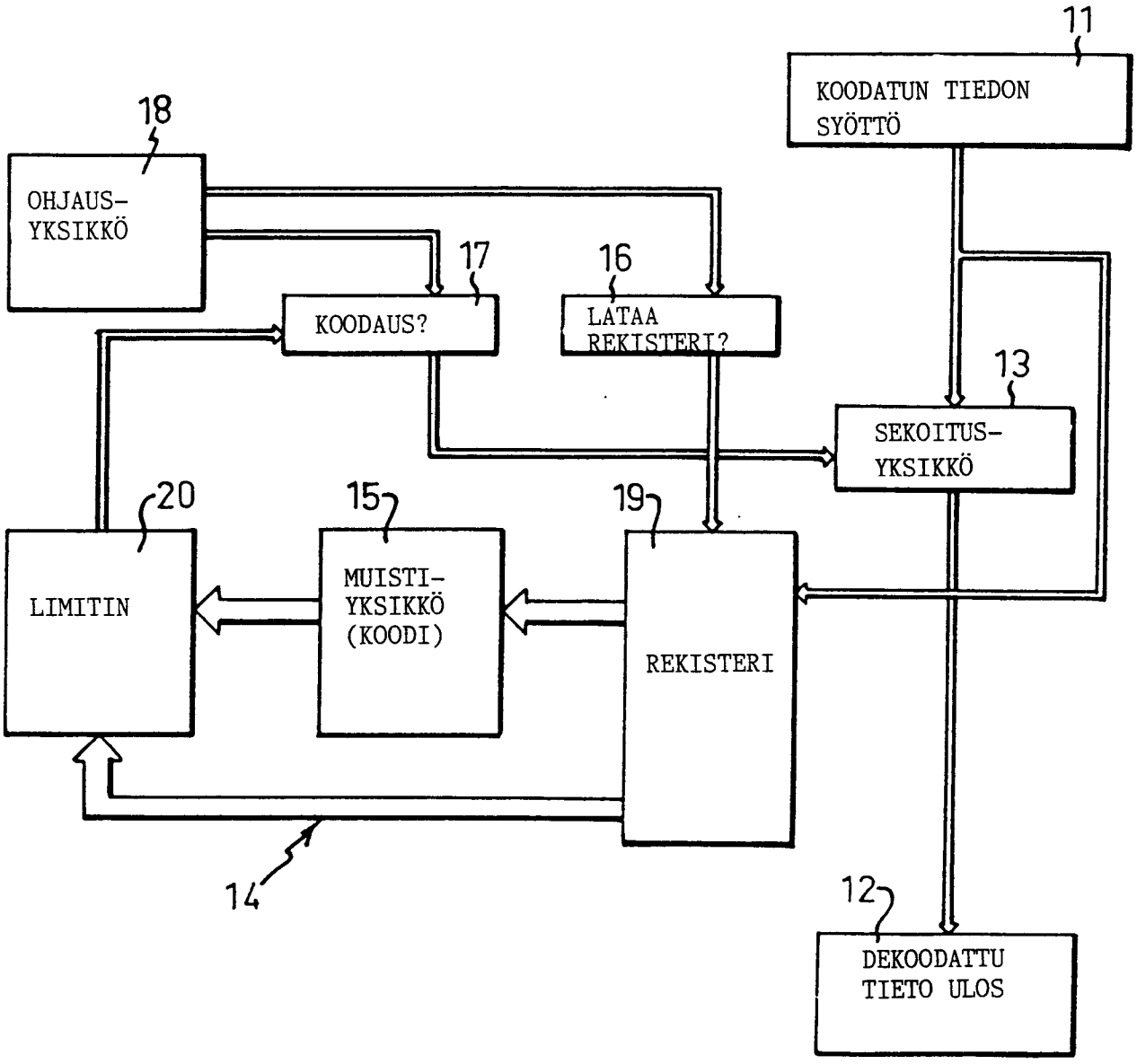

11
KOODATUN TIEDON SYÖTTÖ
18
OHJAUS-YKSIKKÖ
17
KOODAUS?
16
LATAA REKISTERI?
13
SEKOITUS-YKSIKKÖ
20
LIMITIN
15
MUISTI-YKSIKKÖ (KOODI)
19
REKISTERI
14
12
DEKOODATTU TIETO ULOS

Fig. 3

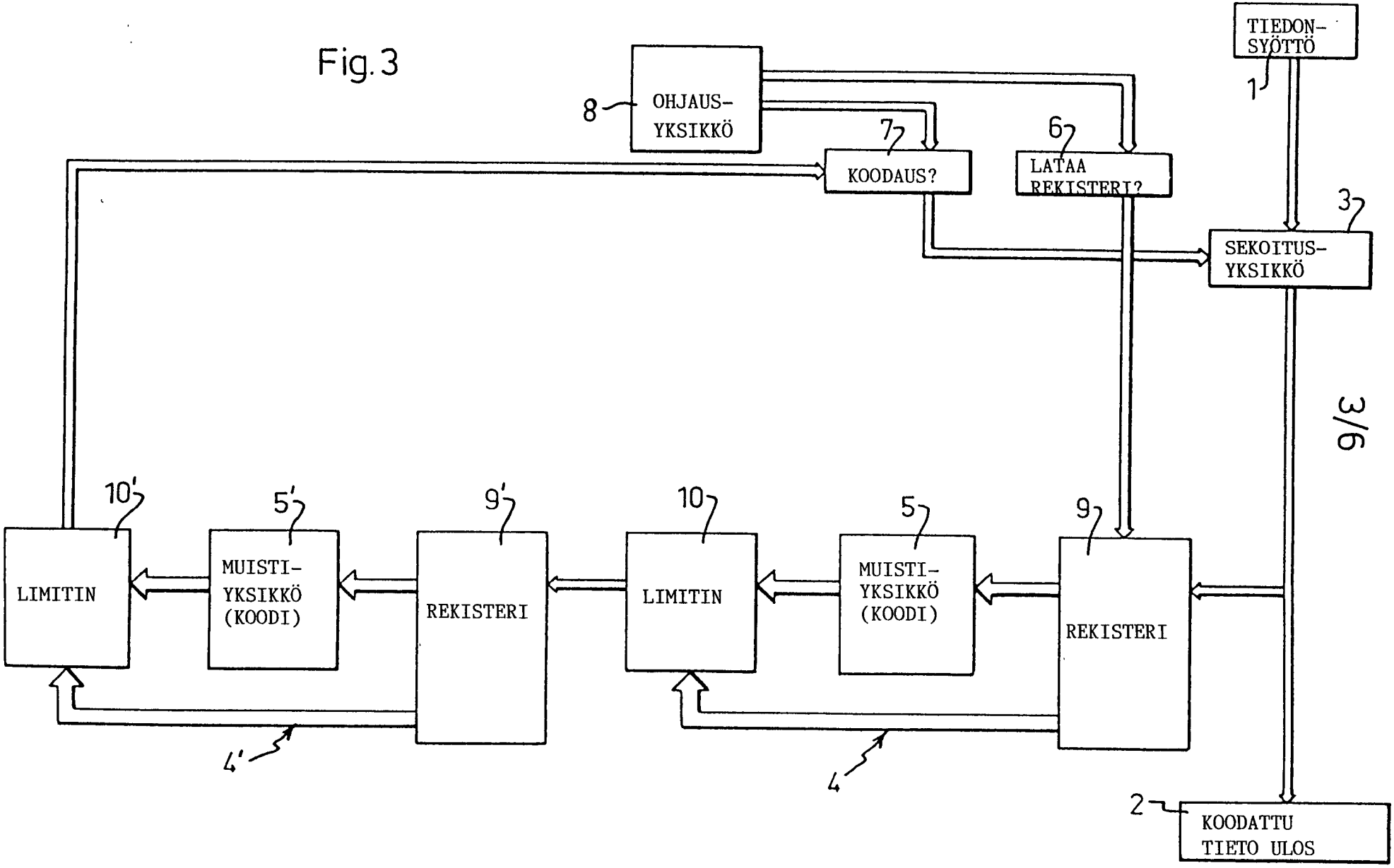

TIEDON-
SYÖTTÖ
1
8
OHJAUS-
YKSIKKÖ
7
KOODAUS?
6
LATAA
REKISTERI?
3
SEKOITUS-
YKSIKKÖ
10'
LIMITIN
5'
MUISTI-
YKSIKKÖ
(KOODI)
9'
REKISTERI
10
LIMITIN
5
MUISTI-
YKSIKKÖ
(KOODI)
9
REKISTERI
4'
4
2
KOODATTU
TIETO ULOS

Fig.4

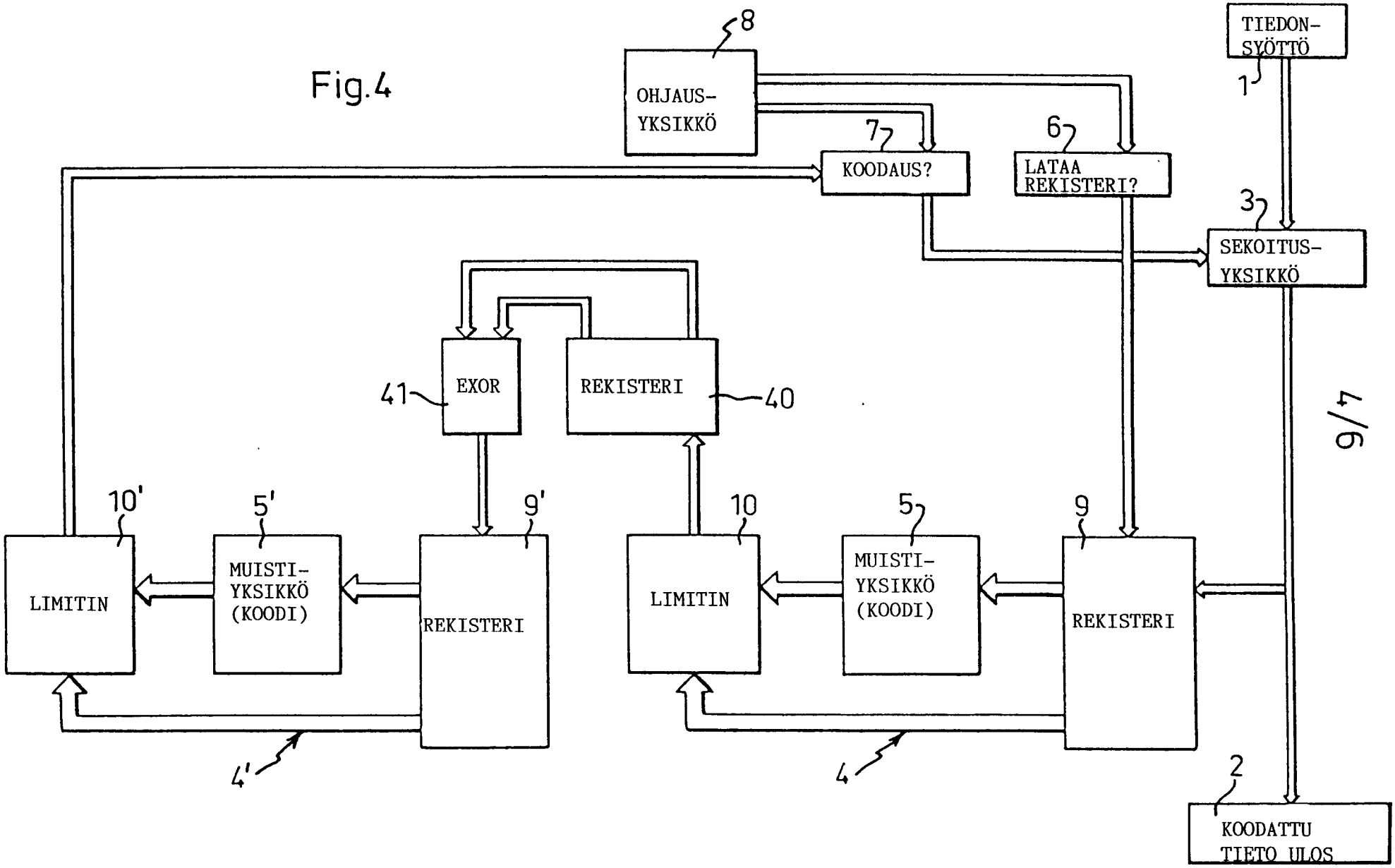

8
OHJAUS-
YKSIKKÖ
TIEDON-
SYÖTTÖ
1
7
KOODAUS?
6
LATAA
REKISTERI?
3
SEKOITUS-
YKSIKKÖ
41
EXOR
REKISTERI
40
10'
5'
9'
10
5
9
LIMITIN
MUISTI-
YKSIKKÖ
(KOODI)
REKISTERI
LIMITIN
MUISTI-
YKSIKKÖ
(KOODI)
REKISTERI
4'
4
2
KOODATTU
TIETO ULOS

Fig.5

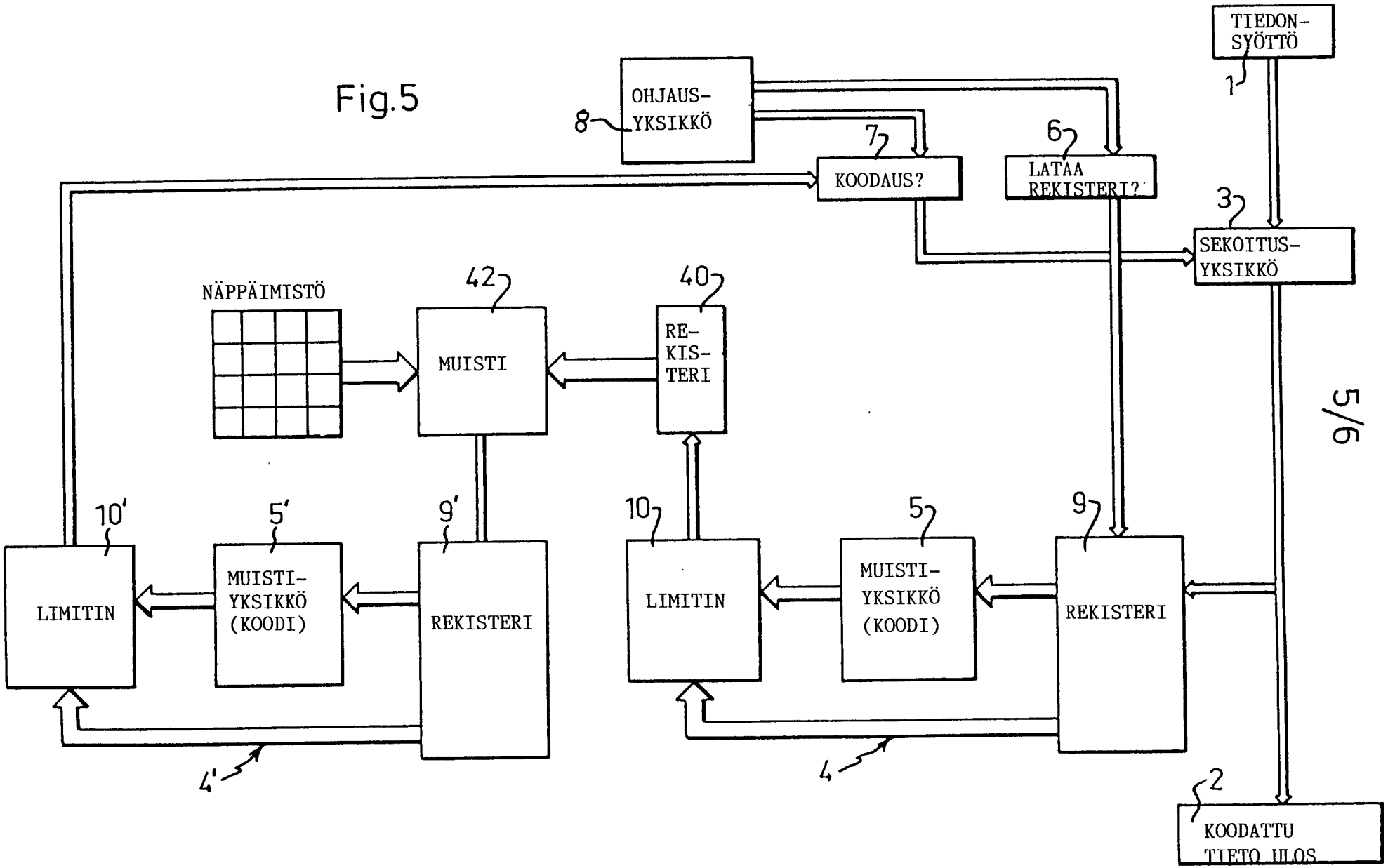
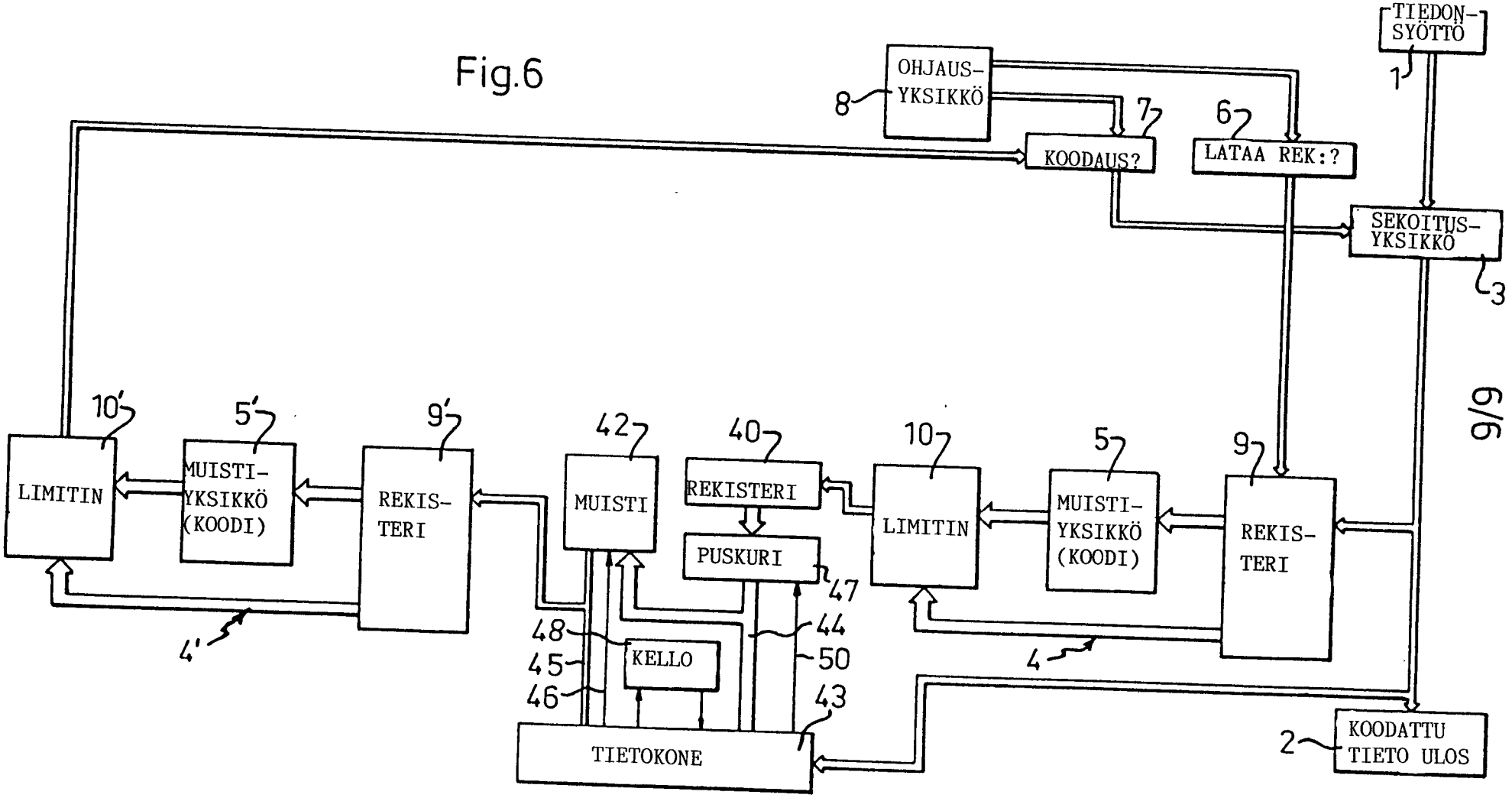

TIEDON-
SYÖTTÖ
1
OHJAUS-
YKSIKKÖ
8
7
KOODAUS?
6
LATAA
REKISTERI?
3
SEKOITUS-
YKSIKKÖ
NÄPPÄIMISTÖ
42
MUISTI
40
RE-
KIS-
TERI
10'
5'
9'
LIMITIN
MUISTI-
YKSIKKÖ
(KOODI)
REKISTERI
10
5
9
LIMITIN
MUISTI-
YKSIKKÖ
(KOODI)
REKISTERI
4'
4
2
KOODATTU
TIETO ULOS

Fig.6


TIEDON-
SYÖTTÖ
1
OHJAUS-
YKSIKKÖ
8
7
6
KOODAUS?
LATAA REK:?
SEKOITUS-
YKSIKKÖ
3
10'
5'
9'
42
40
10
5
9
LIMITIN
MUISTI-
YKSIKKÖ
(KOODI)
REKIS-
TERI
MUISTI
REKISTERI
PUSKURI
47
LIMITIN
MUISTI-
YKSIKKÖ
(KOODI)
REKIS-
TERI
4'
48
45
46
KELLO
44
50
43
4
TIETOKONE
2
KOODATTU
TIETO ULOS

PATENTTI-JA REKISTERIHALLITUS
PATENTTIOSASTO

TUTKIMUSRAPORTTI

PATENTTIHAK.NR	LUOKKA	TUTKIJA	TUTKIMUSTUL. SAATU
885698	H04L 9/00	HO	EP WO US x x

TUTKITUT LUOKAT	TUTKITUT MAAT FI SE NO DK CH DE WO EP GB US	TUTK. KESK. *)
H04L 9/00	x	
02	x	

PATENTTIVIRASTOJEN JULK.	LUOKKA	TYYPPI **)	HUOM!
1)			
2)			
3)			
4)			
5)			
6)			
7)			
8)			
9)			

*) TUTKIMUS KESKEYTETTY ESTEEN LÖYTYMISEN TAKIA
**) MERKITSE A, JOS TEKNIIKAN TASOA

KÄÄNNÄ!

PATENTTIVIRASTOJEN JULK.	LUOKKA	TYYPPI **)	HUOM!
10)			
11)			
12)			
13)			
14)			
15)			
16)			
17)			
18)			
19)			

MUITA JULKAISUJA / ON-LINE TUTKIMUS, JOS TEHTY (TIETOKANTA, HAKUSANAT YM.)

HELSINKI 8.6.1992
PÄIVÄYS

ALLEKIRJOITUS