FI000108690B

(12) **PATENTTIJULKAISU**
PATENTSKRIFT

(10) **FI 108690 B**

(45) Patentti myönnetty - Patent beviljats **28.02.2002**

(51) Kv.lk.7 - Int.kl.7

H04K 1/06, H04L 9/08

(21) Patenttihakemus - Patentansökning **924092**

(22) Hakemispäivä - Ansökningsdag **11.09.1992**

(24) Alkupäivä - Löpdag **11.09.1992**

(41) Tullut julkiseksi - Blivit offentlig **14.03.1993**

(32) (33) (31) Etuoikeus - Prioritet

13.09.1991 US 759312 P

SUOMI – FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN

(73) Haltija - Innehavare

1 •**American Telephone & Telegraph Company,** 32 Avenue of the Americas, New York, NY 10013-2412, AMERIKAN YHDYSVALLAT, (US)

(72) Keksijä - Uppfinnare

1 •**Reeds, III,James Alexander,** 127 Southgate Road, New Providence, NJ 07974, AMERIKAN YHDYSVALLAT, (US)
2 •**Treventi,Philip Andrew,** 15 Candlewood Drive, Murray Hill, NJ 07974, AMERIKAN YHDYSVALLAT, (US)

(74) Asiamies - Ombud: Berggren Oy Ab
Jaakonkatu 3 A, 00100 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning

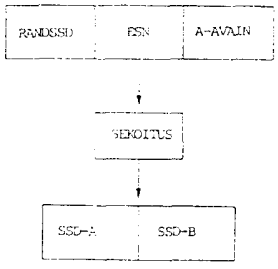
Puheen ja ohjaussanomien salakirjoittaminen solukkojärjestelmässä
Lönnskrift av tal och av styrningsmeddelanden i cellsystem

(56) Viitejulkaisut - Anförda publikationer

EP A 354770 (H04L 9/08)

(57) Tiivistelmä - Sammandrag

Protokolla, joka todentaa asiakkaan matkaviestimen oikeaperäisyyden palvelun tuottajalle ja jossa signalointisanomat on salakirjoitettu ja jossa puheviestit voidaan salakirjoittaa. Palvelun tuottaja antaa jokaisen asiakkaan matkaviestimelle yksikäsitteisen "salaisuuden" sekä muuta informaatiota, kuten puhelinnumeron. Palvelun tuottajan niin halutessa asiakkaan matkaviestimelle lähetetään määräys, jonka mukaan se kehittää yhteisen salaisen tiedon tämän salaisuuden perusteella. Yhteinen salattu tieto kehitetään bittijonon avulla, jonka palvelun tuottaja tätä tarkoitusta varten lähettää. Osaa kehitetystä yhteisestä salaisesta tiedosta käytetään puheen salakirjoittamiseksi ja samaa tai muuta osaa kehitetystä yhteisestä salaisesta tiedosta käytetään syötteenä prosessille, joka kehittää toisen salakirjoitusavaimen. Tätä avainta käytetään asiakkaan matkaviestimessä niiden asiakkaan matkaviestimen kehittämien ohjaussignaalien koodaamiseksi, jotka vaikuttavat kulloinkin yhdistettynä olevan puhelun luonteeseen.



Protokoll som fastslår autenticiteten för en kunds mobila kommunikationsanläggning för servicetillställaren, och där signaleringsmeddelandena enkrypterats och där ljudkommunikationen kan enkrypteras. Servicetillställaren ger den mobila kommunikationsanläggningen för varje kund en entydig "hemlighet" samt övrig information, såsom ett telefonnummer. Om servicetillställaren så önskar sändes till kundens mobila kommunikationsanläggning en order enligt vilken den bildar en gemensam hemlig uppgift på basen av denna hemlighet. Den gemensamma hemliga uppgiften bildas medelst en bitlängd som servicetillställaren sänder för detta ändamål. En del av de bildade gemensamma hemliga uppgifterna användes för enkryptering av tal och samma del eller en annan del av de bildade gemensamma hemliga uppgifterna används för inmatning till en process som utvecklar en andra enkrypteringsnyckel. Denna nyckel används i kundens mobila kommunikationsanläggning för kodning av de styrsignaler som kundens mobila kommunikationsanläggning bildat vilka inverkar på naturen för samtalet som tillkopplats vid denna tidpunkt.

Puheen ja ohjaussanomien salakirjoittaminen solukkojärjestelmässä

Tämä keksintö liittyy oikeaperäisyyden todentaviin protokolliin ja erityisesti protokolliin, jotka varmistavat viestintää suorittavien radiopuhelimien ja muiden sellaisten luvallisuuden.

Tavanomaisessa puhelinliikenteessä kukin puhelinkoje (telekopiointilaite, modeemi jne.) on fysikaalisesti liitetty valitsinporttiin paikalliskeskuksessa. Liitäntä tapahtuu kiinteällä johdolla tai osoitetun kanavan välityksellä kiinteällä johdolla. Langallisen yhteyden asentaa palvelun tuottaja (joka tyypillisesti on puhelinlaitos) ja siksi palvelun tuottaja voi olla kohtalaisen varma siitä, että kanavalla tapahtuva lähetys saapuu tietyltä asiakkaalta. Toisaalta tilaajan oikeaperäisyyden todentaminen langattomassa viestinnässä on vähemmän varmaa.

Yhdysvalloissa nykyisin käytettävässä solukkopuhelinsovitelmassa, kun solukkopuhelintilaaja ottaa puhelun, hänen solukkopuhelimensa ilmaisee palvelun tuottajalle kutsujan identiteetin laskutustarkoituksia varten. Tätä informaatiota ei ole salakirjoitettu. Jos luvaton tunkeutuja salakuuntelee oikeaan aikaan, hän pystyy saamaan tilaajan tunnisteinformaation. Tämä käsittää tilaajan puhelinnumeron ja tilaajalaitteen elektronisen sarjanumeron (ESN, electronic serial number). Tämän jälkeen tunkeilija voi ohjelmoida solukkopuhelimensa tekeytymään täksi *bona fide* -tilaajaksi saadakseen petoksellisesti palveluja. Vaihtoehtoisesti tunkeutuja voi liittyä olemassaolevalle yhteydelle, käyttää tilaajan solukkopuhelinta suuremmalla teholla lähettämällä enemmän tehoa sekä ohjaamaan puhelun omiin tarkoituksiinsa lähettämällä tiettyjä ohjauskoodeja palvelun tuottajalle. Pohjimmiltaan tällainen rosvoaminen

onnistuu, koska palvelun tuottajalla ei ole mitään mekanismia kutsujan identiteetin todentamiseksi yksilöllisesti yhteyden muodostamisajankohtana ja/tai yhteyden ollessa aktiivinen.

On käytettävissä tekniikkaa, joka sallii salakuuntelijan automaattisesti käydä läpi kaikki solukkotaajuudet tietyssä solussa tällaisen tunnisteinformaation saamiseksi. Näin ollen solukkopuhelinpalveluiden rosvous rehottaa. Myös puhesignaalien salakirjoituksen puute asettaa keskustelujen sisällön alttiiksi salakuuntelijoille. Lyhyesti sanoen on olemassa selvä tarve tehokkaista varmuustoimenpiteistä solukkoviestinnän alalla, ja tämä johdattaa käyttämään salakirjoitusta oikeaperäisyyden varmistamiseksi ja yksityisyyden suojaamiseksi.

On olemassa useita standardoituja salakirjoitusmenetelmiä solukkoviestinnässä olemassaolevan, yleistä lajia olevan oikeaperäisyyden todentamisongelman ratkaisemiseksi, mutta jokaisessa osoittautuu olevan käytännön ongelmia. Ensiksikin voidaan käyttää klassillista haaste/vastaus -protokollaa, joka perustuu yksityistä avainta käyttävään salakirjoitusalgoritmiin. Tässä lähestymistavassa tilaajan matkaviestimelle annetaan salainen avain, joka on myös kotijärjestelmän tiedossa. Kun palveleva järjestelmä haluaa todentaa tilaajan oikeaperäisyyden, se antaa kotijärjestelmältä haasteen ja vaatii vastauksen, joita tietyn tilaajan yhteydessä käytetään. Haaste ja vastaus syötetään palvelevaan järjestelmään, joka välittää haasteen matkaviestimelle. Matkaviestin vuorostaan reagoi antamalla vastauksen, jonka se laskee haasteesta ja tallennetusta salaisesta avaimestaan. Palveleva järjestelmä vertaa kotijärjestelmän ja matkaviestimen antamia vastauksia, ja jos ne ovat yhtäpitävät, matkaviestin todetaan oikeaperäiseksi.

Tähän ratkaisutapaan liittyy se ongelma, että palveleva järjestelmä ei useinkaan pysty saamaan yhteyttä kotijärjestelmään riittävän nopeasti, jotta se mahdollistaisi oikeaperäisyyden todentamisen yhteyttä perustettaessa, tai että kotijärjestelmän tietokantaohjelmisto ei pysty hakemaan tilaajan salaista avainta ja muodostamaan haaste/vastaus -paria riittävän nopeasti. Sekunnin tai kahden sekunnin luokkaa olevat verkon tai ohjelmiston viiveet suurentaisivat samalla määrällä toimintaviivettä, joka kuluu, kunnes tilaaja kuulee valintaäänen nostettuaan kuulokkeen ottaessaan puhelun, ja pitemmät viiveet (joita solukkopalvelujen tuottajien nykyisin käyttämät ohjauspiirit ja keskuslaitteet aiheuttavat) ovat yleisiä. Nykyisessä ympäristössä tällaisia viiveitä ei voida hyväksyä.

Yleistä avainta käyttävä salakirjoitus muodostaa toisen standardiluokan oikeaperäisyysongelmien ratkaisemiseksi. Yleisesti sanoen kullekin matkaviestimelle annetaan yksilöllinen "yleinen avaintodistus", joka osoittaa, että matkaviestin on palvelun tuottajan luvallinen asiakas. Lisäksi kullekin matkaviestimelle annetaan myös salaisia tietoja (yksityisiä avaimia), joita se voi käyttää, yhdessä todistuksen kanssa, osoittaakseen kolmansille osapuolille (kuten palvelevalle järjestelmälle) olevansa luvallinen asiakas.

Palvelun tuottajalla voi esimerkiksi olla RSA-avainpari (F,G), jossa F on yksityinen ja G yleinen avain. Palvelun tuottaja voi antaa kullekin matkaviestimelle sen oman RSA-avainparin (D,E) yhdessä $F(E)$:n (matkaviestimen julkinen avain E salakirjoitettuna käyttäen palvelun tuottajan yksityistä avainta F). Tämän jälkeen matkaviestin vahvistaa identiteettinsä lähettämällä $(E,F(E))$:n palvelevalle järjestelmälle. Palveleva järjestelmä soveltaa G:tä $F(E)$:hen E:n saamiseksi. Palveleva järjestelmä kehittää haasteen X,

salakirjoittaa sen matkaviestimen julkista avainta *E* käyttäen *E(X)*:n saamiseksi, jonka se lähettää matkaviestimelle. Matkaviestin soveltaa yksityistä avaintaan *D* *E(X)*:ään *X*:n saamiseksi, jonka se lähettää selväkielisenä vastauksena takaisin palvelimelle.

Vaikka tietyt muunnelmat tästä teemasta sisältävät vähemmän laskutoimituksia tai tiedonsiirtoa kuin muut, niin toistaiseksi ei ole ollut olemassa mitään julkista avainta käyttävää oikeaperäisyyden todentamismenetelmää, joka olisi tehokkaasti suoritettavissa sekuntia lyhyemmässä ajassa sellaisessa laitteistossa, jota nykyisin solukkopuhelimissa käytetään. Vaikka verkkoyhteyttä palvelevan järjestelmän ja kotijärjestelmän välillä ei oikeaperäisyyden todentamishetkellä tarvita, kuten asia on klassillisessa lähestymistavassa, niin samat aikarajoitukset, jotka poissulkevat klassillisen ratkaisun, poissulkevat myös julkista avainta käyttävän ratkaisun.

R. M. Needham ja M. D. Schroeder ovat ehdottaneet erästä toista tekniikkaa kirjoituksessa Using Encryption for Authentication in Large Computer Networks, Comm. of the ACM, Vol. 21, n:o 12, 993-999 (joulukuu 1989). Lyhyesti sanoen Needham-Schroederin tekniikka edellyttää, että kolmas, luotettu, osapuoli (AS) palvelee *oikeaperäisyyden todentavana palvelimena*, joka jakaa istuntoavaimet mahdollisille osapuolille (A ja B), joka yrittävät perustaa suojatun viestiyhteyden. Protokolla on seuraava: kun osapuoli A haluaa saada yhteyden osapuoleen B, se lähettää oikeaperäisyyden todentavalle palvelimelle AS oman nimensä, osapuolen B nimen, istuntoavaimen, tapahtumatunnisteen sekä B:n avainta käyttäen salakirjoitetun sanoman. Kaikki nämä tiedot salakirjoitetaan A:n avainta käyttäen. Osapuoli A vastaanottaa nämä tiedot, avaa ne, valitsee sen osan, joka on salakirjoitettu B:n avaimella ja toimittaa tämän

osan osapuolelle B. Osapuoli B avaa vastaanotetut sanomat ja löytää siitä osapuolen A nimen ja istuntoavaimen. Osapuoli B suorittaa viimeisen tarkistuksen ("toistojen" estämiseksi) antamalle haasteen osapuolelle A, ja osapuoli A vastaa istuntoavainta käyttäen. Osapuolen B havaitsema yhtäpitävyys todentaa osapuolen A identiteetin.

Solukkopuhelinliikenteen suojaustarpeet on täytetty sovitelmalla, joka riippuu yhteisestä salaisesta tietokentästä. Matkaviestin ylläpitää salaisuutta, jonka palvelun tuottaja on sille antanut, ja kehittää yhteisen salaisen tietokentän tämän salaisuuden perusteella. Palvelun tuottaja kehittää myös yhteisen salaisen tietokentän. Kun matkaviestin saapuu tukiaseman soluun, se antaa tunnisteensa tukiasemalle ja syöttää tukiasemalle hajakoodatun oikeaperäisyyden todistavan merkkijonon. Tukiasema konsultoi palvelun tuottajan kanssa, ja jos todetaan, että matkaviestin on *bona fide* -laite, niin palvelun tuottaja syöttää tukiasemalle yhteisen salaisen tietokentän. Tämän jälkeen matkaviestin on yhteydessä tukiaseman kanssa oikeaperäisyyden todentavien prosessien avulla, jotka suoritetaan matkaviestimen ja tukiaseman välillä yhteistä salaista tietokenttää käyttäen.

Eräs tämän sovitelman piirre on, että eri tukiasemien ei tarvitse päästä käsiksi palvelun tuottajan matkaviestimiin asentamaan salaisuuteen. Lisäksi vain niillä tukiasemilla, jotka ovat onnistuneet olemaan vuorovaikutuksessa matkaviestimen kanssa, on yhteinen salainen tietokenttä.

Toisaalta, enemmän aikaa vievä salaisuutta hyväksikäyttävä oikeaperäisyyden todentamisprosessi, joka tapahtuu vain palvelun tuottajan välityksellä, tapahtuu vain aika ajoittain, kun matkaviestin alussa saapuu soluun (tai kun on

epäiltävissä, että yhteinen salainen tietokenttä on mennyt sekaisin).

Tämän keksinnön periaatteiden mukaan sekä matkaviestin että tukiasema käyttävät osaa yhteisestä salaisesta tietokentästä salakirjoitusavainparin luomiseksi. Matkaviestin käyttää parin ensimmäistä salakirjoitusavainta puheen salakirjoittamiseksi, ja tukiasema käyttää sitä puheen avaamiseksi. Tukiasema käyttää parin toista salakirjoitusavainta puheen salakirjoittamiseksi, ja matkaviestin käyttää sitä puheen avaamiseksi.

Salakirjoitusavainparin luomiseksi käytetään samaa hajakoodausfunktiota, jota käytetään yhteisen salaisen tietokentän luomiseksi.

Salakirjoitettavat ohjaussanomat salakirjoitetaan kolmella perättäisellä muunnoksella, jotka tuottavat itsensä suhteen käänteisen salakirjoitusprosessin. Ensimmäisessä muunnoksessa lisätään satunnainen vakio salakirjoitettavan sanoman jokaiseen sanaan. Vakio liittyy hajakoodattuun merkkijonoon, joka käsittää osan yhteisestä salaisesta tietokentästä ja joka hajakoodataan hajakoodausfunktiolla, jota käytetään johdettaessa yhteinen salainen tietokenttä. Toisessa muunnoksessa se sanojen joukko, joka muodostaa (ensimmäisellä muunnoksella muunnetun) ohjaussanoman, jaetaan ensimmäiseen puoliskoon ja toiseen puoliskoon, ja ensimmäinen puolisko muunnetaan osittain toisen puoliskon perusteella. Kolmannessa muunnoksessa vähennetään satunnainen vakio (toisen muunnoksen muuntaman) salakirjoitettavan sanoman jokaisesta sanasta. Tässäkin vakio liittyy hajakoodattuun merkkijonoon, joka käsittää osan yhteisestä salaisesta tietokentästä ja joka hajakoodataan hajakoodausfunktiolla, jota käytetään johdettaessa yhteinen salainen tietokenttä.

Kuvio 1 esittää verkkopalvelujen tuottajien ja solukkopalveluiden tuottajien sovitelmaa, jotka tuottajat on yhdistetty toisiinsa sekä paikallaan pysyvien puhelimien että matkapuhelimien ja muiden sellaisten palvelemiseksi;

kuvio 2 esittää prosessia, joka ohjaa yhteisen salaisen tietokentän luomista ja sen verifiointia;

kuvio 3 esittää rekisteröintiprosessia vierailukohteena olevalla tukiasemalla esimerkiksi, kun matkaviestin aluksi saapuu tukiaseman palvelemaan soluun;

kuvio 4 esittää elementtejä, jotka yhdistetään ja hajakoodataan yhteisten salaisten tietojen luomiseksi;

kuvio 5 esittää elementtejä, jotka yhdistetään ja hajakoodataan verifiointisekvenssin luomiseksi;

kuvio 6 esittää elementtejä, jotka yhdistetään ja hajakoodataan rekisteröintisekvenssin luomiseksi, kun matkaviestin tulee radioyhteydelle;

kuvio 7 esittää elementtejä, jotka yhdistetään ja hajakoodataan puhelun aloitussekvenssin luomiseksi;

kuvio 8 esittää salakirjoitus- ja avausprosessia matkaviestimessä;

kuvio 9 esittää elementtejä, jotka yhdistetään ja hajakoodataan uudelleentodentamissekvenssin luomiseksi;

kuvio 10 esittää kolmivaiheista prosessia valittujen ohjaus- ja datasanomien salakirjoittamiseksi ja avaamiseksi; ja

kuvio 11 esittää matkaviestimen laitteiston lohkokaaviota.

Solukkomatkapuhelinsovitelmassa on monia matkapuhelimia, paljon pienempi määrä solukkopalveluiden tuottajia (missä kullakin tuottajalla on yksi tai useampia tukiasemia) sekä yksi tai useampia kytkentäisten verkkopalvelujen tuottajia (puhelinlaitoksia). Solukkopalvelujen tuottajat ja puhelinlaitokset toimivat yhdessä, jotta solukkopuhelintilaaja voi viestiä sekä solukko- että ei-solukkopuhelintilaajien kanssa. Tämä sovitelma on esitetty kaaviollisesti kuviossa

1, jossa puhelinlaitos I ja puhelinlaitos II toimivat yhdessä muodostaen keskukset 10-14 käsittävän kytkentäisen verkon. Paikallaan pysyvät yksiköt 20 ja 21 on liitetty keskukseen 10, matkaviestimet 22 ja 23 voivat liikkua vapaasti, ja tukiasemat 30-40 on liitetty keskuksiin 10-14. Tukiasemat 30-34 kuuluvat tuottajalle 1, tukiasemat 35 ja 36 kuuluvat tuottajalle 2, tukiasema 37 kuuluu tuottajalle 4, ja tukiasemat 38-40 kuuluvat tuottajalle 3. Tämän selityksen tarkoituksia varten tukiasema on synonyymi solulle, jossa on yksi tai useampia lähettimiä. Solujen yhdistelmä muodostaa solukkomaisen maantieteellisen palvelualueen (CGSA, cellular geographic service area), kuten esimerkiksi tukiasemat 30, 31 ja 32 kuviossa 1.

Jokaisella matkaviestimellä on elektroninen sarjanumero (ESN, electronic serial number), joka on yksinomaan tälle laitteelle kuuluva. Valmistaja installoi ESN:n silloin, kun laite valmistetaan (esimerkiksi lukumuistiin), ja sitä ei voi muuttaa. Se on kuitenkin luettavissa.

Kun asiakas haluaa tehdä palvelusopimuksen matkaviestimelle, jonka asiakas omistaa tai on vuokrannut, niin palvelun tuottaja antaa asiakkaalle puhelinnumeron (MIN1 tunnuksen), aluekooditunnuksen (MIN2 tunnuksen) sekä "salaisuuden" (A-avain). MIN1 ja MIN2 tunnukset liittyvät tuottajan tiettyyn CGSA:han, ja kaikki tukiasemat kuvion 1 sovitelmassa voivat tunnistaa sen CGSA:n, johon tietty MIN2- ja MIN1-pari kuuluu. A-avain on vain asiakkaan laitteiston ja tuottajan CGSA-suorittimen (ei eksplisiittisesti esitetty kuviossa 1) tiedossa. CGSA-suoritin ylläpitää laitteen ESN-, A-avain-, MIN1- ja MIN2-tunnuksia ja mitä tahansa muita tietoja, joita palvelun tuottaja saattaa haluta.

MIN1- ja MIN2-tunnusten sekä A-avaimen ollessa asennettu asiakaslaite alustetaan palvelua varten, kun CGSA-suoritin

lähettää matkaviestimelle erityisen satunnaissekvenssin (RANDSSD) ja määräyksen luoda "yhteisten salaisten tietojen" kenttä (SSD, "shared secret data" field). CGSA lähettää RANDSSD:n ja SSD-kentän kehittämismääräyksen solun tukiaseman kautta, kun matkaviestin sijaitsee solussa. SSD-kentän luonti noudattaa kuviossa 2 esitettyä protokollaa.

Lisäksi kuvion 1 sovitelmassa kukin tukiasema lähettää informaation kaikille solussaan oleville laitteille jollakin ennalta varatulla taajuuskaistalla (yleislähetyskaista). Lisäksi se ylläpitää kaksisuuntaista yhteyttä kunkin matkaviestimen kanssa keskinäisesti sovitulla, (väliaikaisesti) varatulla kanavalla. Tapa, jolla tukiasema ja matkaviestin sopivat viestintäkanavasta, on merkityksetön tämän keksinnön kannalta, joten tätä tapaa ei ole tässä yksityiskohtaisesti selitetty. Eräs ratkaisu voi olla esimerkiksi, että matkaviestin käy läpi kaikki kanavat ja valitsee tyhjän kanavan. Se lähettää sitten tukiasemalle MIN2- ja MIN1-tunnuksensa (joko selväkielisessä muodossa tai julkista avainta käyttäen salakirjoitettuna). Sen jälkeen kun oikeaperäiseksi todettu yhteys on perustettu, tukiasema voi tarvittaessa ohjata matkaviestimen vaihtamaan toiselle kanavalle.

Kuten seuraavassa on yksityiskohtaisemmin selitetty, puhelua tämän keksinnön matkapuhelinjärjestelmässä perustettaessa ja ylläpidettäessä oikeaperäisyyden todentamisprosessi voidaan suorittaa useita kertoja keskustelun kuluessa. Siksi käytettävän oikeaperäisyyden todentamisprosessin tulee olla suhteellisen varma ja yksinkertainen toteuttaa. Rakenteen yksinkertaistamiseksi ja toteutuskustannusten alentamiseksi sekä matkaviestimen että tukiaseman tulee käyttää samaa prosessia.

Monet oikeaperäisyyden todentamisprosessit käyttävät hajakoodausfunktiota eli yksisuuntaista funktiota tämän prosessin toteuttamiseksi. Hajakoodausfunktio suorittaa monta-yhteen -kuvauksen, joka muuntaa "salaisuuden" allekirjoitukseksi. Seuraavassa on selitetty yksi hajakoodausfunktio, joka on yksinkertainen, nopea, tehokas ja joustava. Se on erittäin sopiva tämän keksinnön oikeaperäisyyden todentamisprosesseihin, mutta muita hajakoodausfunktioita voidaan tietenkin käyttää.

Sekoitusprosessi

Sekoitusprosessi luo "allekirjoituksen", joka käsittää d "salaista" datasanaa sisältävän lohkon $b(i)$, k sanaa sisältävän avaimen $x(j)$ avulla, missä d, i, j ja k ovat kokonaislukuja. "Allekirjoituksen" luontiprosessi suoritetaan yksi datasana kerrallaan. Tämän selityksen tarkoituksia varten sanat, joilla sekoitusprosessi operoi, ovat 8 bitin pituisia (jotka antavat suljetun välin 0...255), mutta voidaan käyttää mitä tahansa sananpituutta. "Salaisen" datalohkon pituus sisältyy saha-aaltofunktioon

$s_d(t) = t$ kun $0 \leq t \leq d - 1$
$s_d(t) = 2d - 2 - t$ kun $d \leq t \leq 2d - 3$, ja
$s_d(t) = s_d(t + 2d - 2)$ kaikilla t:n arvoilla.

Tätä funktiota käytetään seuraavassa prosessissa, jossa alkaen arvoista z=0 ja i=0 perättäisesti kasvavilla i:n kokonaislukuarvoilla alueella $0 \leq 6d$-5

a) $b(s_d(i))$ päivitetään:
$b(s_d(i)) = b(s_d(i)) + x(i_k) + SBOX(z)$ mod 256
jossa
* i_k on i modulo k, $SBOX(z) = y+[y/2048]$ mod 256,
* $y = (z \oplus 16)(z + 111)(z)$,

* [$y/2048$] osamäärän y jaettuna 2048:lla kokonaislukuosa ja $\oplus$ edustaa biteittäin laskettua pelkkä-TAI -funktiota, ja

b) z päivitetään: $z = z+b(s_d(i)) \bmod 256$.

Havaitaan, että edellä esitetyssä prosessissa ei ole mitään todellista eroa datan ja avaimen välillä. Siksi missä tahansa merkkijonossa, jota käytetään oikeaperäisyyden todentamisessa, osaa siitä voidaan käyttää avaimena edellä esitetyssä prosessissa. Kääntäen datasanojen yhdistettynä avaimen kanssa voidaan katsoa olevan "oikeaperäisyyden todistava merkkijono". Huomataan myös, että jokainen sana $b(i)$, jossa $0 \leq i \leq d$, hajakoodataan yksilöllisesti, yksi kerrallaan, mikä suorittaa hajakoodauksen "paikallaan". Hajakoodausfunktiolle sinänsä ei tarvita mitään lisäpuskureita.

Edellä esitetty prosessi voidaan helposti suorittaa aivan tavanomaisella perussuorittimella, koska ainoat tarvittavat operaatiot ovat: siirto (2048:lla jakamisen suorittamiseksi), katkaisu ([ ] -funktion ja mod 256 -funktion suorittamiseksi), yhteenlasku-, kertolasku- ja biteittäin laskettava pelkkä-TAI -funktio.

Palataan tarkastelemaan kuvion 2 SSD-kentän initialisointiprosessia. Kun matkaviestin vastaanottaa RANDSSD-sekvenssin ja määräyksen luoda uusi SSD-kenttä (nuoli 100 kuviossa 2), niin uusi SSD-kenttä kehitetään kuvion 4 mukaisesti. Matkaviestin yhdistää ESN-tunnuksen, A-avaimen ja RANDSSD-sekvenssin oikeaperäisyyden todistavan merkkijonon muodostamiseksi. Oikeaperäisyyden todistava merkkijono syötetään sekoitus-lohkoon 101 (selitetty edellä), joka antaa SSD-kentän. SSD-kenttä käsittää kaksi osakenttää: SSD-A -osakentän, jota käytetään oikeaperäisyyden todentamisproseduurien tukena, sekä SSD-B -osakenttä, jota

käytetään puheen sekoitusproseduurien tukena ja joidenkin signalointisanomien (selitetty jäljempänä) salakirjoittamiseksi. Huomattakoon että voidaan luoda suuri määrä SSD-osakenttiä joko jakamalla edellä selitetyllä tavalla muodostettu SSD-kenttä osiin tai suurentamalla ensin SSD-kenttää. SSD-kentän bittien lukumäärän suurentamiseksi tarvitsee vain aloittaa suuremmalla databittien määrällä. Kuten jäljempänä esitetystä selityksestä ilmenee, tämä ei ole kovin haasteellinen vaatimus.

Kotijärjestelmän CGSA-suorittimella on tiedossaan sen matkaviestimen ESN ja A-avain, jolle vastaanotetut MIN2- ja MIN1-tunnukset oli osoitettu. Sen tiedossa on myös lähettämänsä RANDSSD-sekvenssi. Siksi kotijärjestelmän CGSA-suoritin pystyy toisintamaan matkaviestimen SSD-kentän luontiprosessin. Yhdistämällä RANDSSD-signaalin ESN-tunnuksen ja A-avaimen kanssa, ja edellä selitetyn sekoitusprosessin avulla, CGSA-suoritin luo uuden SSD-kentän ja jakaa sen SSD-A- ja SSD-B -osakenttiin. Kotijärjestelmän CGSA-suorittimessa luotu SSD-kenttä täytyy kuitenkin tarkistaa.

Kuvion 2 mukaan matkaviestin panee alulle luodun SSD-kentän tarkistamisen. Matkaviestin kehittää satunnaisen haastesekvenssin (RANDBS-sekvenssin) lohkossa 102 ja lähettää sen kotijärjestelmän CGSA-suorittimelle palvelevan tukiaseman (sen tukiaseman, joka palvelee matkaviestimen sijaintialuetta) välityksellä. Kuvion 5 mukaan kotijärjestelmän CGSA-suoritin yhdistää haasteen RANDBS-sekvenssin, matkaviestimen ESN:n, matkaviestimen MIN1-tunnuksen ja juuri luodun SSD-A:n oikeaperäisyyden todistavan merkkijonon muodostamiseksi, joka syötetään sekoitusprosessiin. Tässä tapauksessa sekoitusprosessi luo hajakoodatun oikeaperäisyyden todistavan signaalin AUTHBS, joka lähetetään matkaviestimelle. Matkaviestin myös yhdistää RANDBS-

sekvenssin, ESN-tunnuksensa, MIN1-tunnuksensa ja juuri luodun SSD-A:n oikeaperäisyyden todistavan merkkijonon muodostamiseksi, joka syötetään sekoitusprosessiin. Matkaviestin vertaa sekoitusprosessinsa tulosta kotijärjestelmän CGSA-suorittimelta vastaanotettuun hajakoodattuun oikeaperäisyyden todistavaan signaaliin (AUTHBS). Jos vertailuvaihe (lohko 104) ilmaisee yhtäpitävyyden, niin matkaviestin lähettää kotijärjestelmän CGSA-suorittimelle kuittaussanoman, joka ilmoittaa päivityksen onnistumisesta SSD-kentässä. Muussa tapauksessa matkaviestin ilmoittaa yhtäpitävyysvertailun epäonnistuneen.

Matkaviestimen tultua initialisoiduksi SSD-kenttä pysyy voimassa, kunnes kotijärjestelmän CGSA-suoritin määrää luotavaksi uuden SSD-kentän. Tämä voi tapahtua esimerkiksi, jos on syytä uskoa, että SSD-kenttä on mennyt sekaisin. Tällaisena ajankohtana kotijärjestelmän CGSA-suoritin lähettää matkaviestimelle uuden RANDSSD-sekvenssin sekä määräyksen uuden SSD-kentän luomiseksi.

Kuten edellä on mainittu, solukkopuhelinliikenteessä kukin tukiasema lähettää eri informaatiosignaaleja kaikkien solussaan olevien matkaviestimien hyväksikäytettäväksi. Kuvion 1 sovitelman mukaan yksi tukiaseman lähettämistä signaaleista on satunnais- tai valesatunnaissekvenssi (RAND-sekvenssi). Eri oikeaperäisyyden todentamisprosessit käyttävät RAND-sekvenssiä matkaviestimien luomien ja lähettämien signaalien satunnaistamiseksi. RAND-sekvenssiä täytyy tietenkin ajoittain vaihtaa, jotta estettäisiin tallennus-/toistoyritykset. Eräs ratkaisu RAND-signaalin piiloajan valitsemiseksi on tehdä se lyhyemmäksi kuin keskimääräisen puhelun odotettu kestoaika. Näin ollen matkaviestin saadaan yleensä käyttämään eri RAND-signaaleja perättäisissä puheluissa.

Tämän keksinnön erään näkökohdan mukaan niin pian kun matkaviestin havaitsee tulleensa soluun, se rekisteröityy tukiasemalle, jotta se voidaan todentaa oikeaperäiseksi. Vasta kun matkaviestin on todettu oikeaperäiseksi, se voi ottaa puheluja tai vastaanottaa sille tulevia tukiaseman suoria puheluja.

Kun matkaviestin aloittaa rekisteröitymisprosessin, se hyväksyy tukiaseman lähettämän RAND-sekvenssin ja vuorostaan lähettää palvelevalle tukiasemalle MIN1- ja MIN2-tunnuksensa ja ESN-sekvenssinsä (selväkielisenä) samoinkuin hajakoodatun oikeaperäisyyden todistavan merkkijonon. Kuvion 6 mukaan hajakoodattu oikeaperäisyyden todistava merkkijono johdetaan yhdistämällä RAND-sekvenssi, ESN-sekvenssi, MIN1-tunnus ja SSD-A -osakenttä oikeaperäisyyden todistavan merkkijonon muodostamiseksi ja syöttämällä tämä oikeaperäisyyden todistava merkkijono sekoitusprosessiin. Hajakoodattu oikeaperäisyyden todistava merkkijono sekoitusprosessin ulostulossa lähetetään palvelevalle tukiasemalle yhdessä ESN-sekvenssin kanssa.

Joissakin suoritusmuodoissa matkaviestimen käyttämä koko RAND-sekvenssi tai osa siitä lähetetään myös palvelevalle tukiasemalle (yhdessä ESN-sekvenssin ja MIN1- ja MIN2 -tunnusten kanssa), koska on olemassa se mahdollisuus, että RAND-arvo on muuttunut siihen mennessä, kunnes hajakoodattu oikeaperäisyyden todistava merkkijono on saavuttanut tukiaseman.

Tukiaseman puolella palvelevan tukiaseman tiedossa on RAND-sekvenssi (koska tämä tukiasema on luonut sen) ja sillä on myös tiedossa ESN ja MIN2- ja MIN1-tunnukset, joiden avulla matkaviestin on antanut tunnistaa itsensä. Matkaviestimen SSD-kenttä *ei* kuitenkaan ole tukiaseman tiedossa. Sen tiedossa on matkaviestimen kotijärjestelmän

CGSA-suorittimen tunniste (MIN1- ja MIN2-tunnuksista). Näin ollen se jatkaa oikeaperäisyyden todentamisprosessia lähettämällä matkaviestimen kotijärjestelmän CGSA-suorittimelle MIN1-tunnuksen, ESN-sekvenssin, matkaviestimen luoman ja lähettämän hajakoodatun oikeaperäisyyden todistavan merkkijonon sekä RAND-sekvenssin, jonka palveleva tukiasema on lähettänyt (ja jonka matkaviestin on sisällyttänyt luomaansa hajakoodattuun oikeaperäisyyden todistavaan merkkijonoon). Matkaviestimen MIN1-tunnuksesta ja ESN-sekvenssistä kotijärjestelmän CGSA-suoritin saa tietoonsa matkaviestimen tunnisteen ja siten matkaviestimen SSD-A -osakentän. Siksi se voi jatkaa ja kehittää oikeaperäisyyden todistavan merkkijonon aivan kuten matkaviestin on tehnyt ja syöttää sen sekoitusprosessiin (kuvio 6). Jos matkaviestimen kotijärjestelmän CGSA-suorittimen luoma hajakoodattu oikeaperäisyyden todistava merkkijono on yhtäpitävä matkaviestimessä luodun ja palvelevan tukiaseman syöttämän hajakoodatun oikeaperäisyyden todistavan merkkijonon kanssa, niin todentaminen katsotaan onnistuneeksi. Tällaisessa tapauksessa kotijärjestelmän CGSA-suoritin syöttää palvelevalle tukiasemalle yksikön SSD-kentän. Toisaalta ESN-tunnuksen ja SSD-kentän pitämiseksi salaisina tukiasemien ja CGSA-suorittimen välinen viestiliikenne suoritetaan salakirjoitetussa muodossa.

Edellä selitetyssä protokollassa matkaviestimen CGSA-suoritin yrittää todentaa hajakoodatun oikeaperäisyyden todistavan merkkijonon pätevyyden. Kun todentaminen on epäonnistunut, niin CGSA-suoritin ilmoittaa palvelevalle tukiasemalle, että matkaviestintä ei todettu oikeaperäiseksi ja voi ehdottaa, että joko yhteys matkaviestimeen katkaistaan tai että matkaviestin määrätään yrittämään rekisteröintiprosessia uudelleen. Rekisteröitymisprosessin yrittämiseksi uudelleen CGSA-suoritin voi joko jatkaa mukanaoloa oikeaperäisyyden todentamisprosessissa tai se voi

siirtää tämän palvelevan tukiaseman tehtäväksi. Viimeksi mainitussa vaihtoehdossa palveleva tukiasema ilmoittaa kotijärjestelmän CGSA-suorittimelle matkaviestimen ESN-sekvenssin ja MIN1-tunnuksen, ja CGSA-suoritin vastaa matkaviestimen SSD-kentällä ja sillä RANDSSD:llä, jonka avulla SSD-kenttä on luotu. Palveleva tukiasema suorittaa sitten oikeaperäisyyden todentamisen siinä merkityksessä, että luodaan hajakoodattu oikeaperäisyyden todistava merkkijono ja verrataan sitä matkaviestimen lähettämään hajakoodattuun oikeaperäisyyden todistavaan merkkijonoon. Uudelleenyrittämistä koskeva määräys voidaan silloin suorittaa ilman kotijärjestelmän CGSA-prosessia siten, että palveleva tukiasema lähettää RANDSSD:n matkaviestimelle. Tämä "rekisteröintiprotokolla" on esitetty kuviossa 3.

Sen jälkeen kun matkaviestin on "rekisteröity" palvelevalla tukiasemalla (edellä selitetyn prosessin avulla), palvelevalla tukiasemalla on tiedossaan matkaviestimen ESN ja SSD-kenttä, ja seuraavat oikeaperäisyyden todentamisprosessit tässä solussa voivat tapahtua palvelevassa tukiasemassa tarvitsematta ottaa yhteyttä kotijärjestelmän CGSA-suorittimeen – yhtä lukuunottamatta. Kun mistä tahansa syystä halutaan muuttaa SSD-kenttää, viestiliikenne tapahtuu itse asiassa kotijärjestelmän CGSA-suorittimen ja matkaviestimen välillä, ja palveleva tukiasema toimii vain tämän viestiliikenteen välittäjänä. Tämä johtuu siitä, että uuden SSD-kentän luonti vaatii salaisen A-avaimen saamista, eikä A-avaimen saantia ole sallittu millekään muulle kuin CGSA-suorittimelle. Näin ollen kun uusi SSD-kenttä on määrä kehittää ja kun matkaviestin ei ole kotijärjestelmän CGSA:n alueella, tapahtuu seuraavaa:

- kotijärjestelmän CGSA-suoritin luo RANDSSD-sekvenssin ja muuttaa SSD-kenttää tämän RANDSSD-sekvenssin perusteella,

- kotijärjestelmän CGSA-suoritin syöttää palvelevalle tukiasemalle RANDSSD-sekvenssin ja juuri luodun SSD-kentän,

- palveleva tukiasema määrää matkaviestimen muuttamaan sen SSD-kenttää ja antaa matkaviestimelle RANDSSD-sekvenssin,

- matkaviestin muuttaa SSD-kenttää ja lähettää haasteen palvelevalle tukiasemalle,

- palveleva tukiasema luo AUTHBS-merkkijonon (selitetty edellä) ja lähettää sen matkaviestimelle, ja

- matkaviestin todentaa AUTHBS-merkkijonon ja ilmoittaa palvelevalle tukiasemalle, että sekä matkaviestimellä että palvelevalla tukiasemalla on sama SSD-kenttä.

Kun tukiasema on rekisteröinyt matkaviestimen, tämä voi ottaa puheluja oikeaperäisyyden todentamisprosessin avulla, joka on esitetty kuviossa 7. Puhelun aloitussekvenssi yhdistää signaalit RAND, ESN, SSD-A ja ainakin jonkin osan kutsutun osapuolen tunnusnumerosta (puhelinnumerosta) (MIN3 kuviossa 7). Yhdistetyt signaalit syötetään sekoitusprosessiin hajakoodatun oikeaperäiseksi todentamissekvenssin kehittämiseksi, jonka palveleva tukiasema voi todentaa. Todentamisen sallimiseksi palvelevalla tukiasemalla myös kutsutun osapuolen tunnusnumero täytyy tietenkin lähettää sellaisella tavalla, jonka tukiasema voi vastaanottaa (ja, kuten edellä, ehkä osa RAND-signaalista), esim. selväkielisenä. Sen jälkeen kun oikeaperäisyyden todistava sekvenssi on todennettu, tukiasema voi käsitellä puhelun ja muodostaa yhteyden kutsuttuun osapuoleen.

Protokolla matkaviestimen yhdistämiseksi, kun sen on "kutsuttu osapuoli", noudattaa kuvion 6 rekisteröintiprotokollaa. Toisin sanoen palveleva tukiasema pyytää kutsuttua matkaviestintä lähettämään RAND-sekvenssistä luodun oikeaperäisyyden todistavan sekvenssin, ESN-tunnuksen, MIN1-tunnuksen ja SSD-A -osakentän. Kun oikeaperäisyyden todentaminen on tapahtunut, tukiaseman ja kutsutun osapuolen välille perustetaan yhteys, jotta viimeksi mainittu voi vastaanottaa tietoja, jotka ovat lähtöisin puhelun ottaneelta matkaviestimeltä (tai paikallaan pysyvältä laitteelta), ja lähettää tälle tietoja.

Huomattakoon että kaikki edellä selitetyt oikeaperäisyyden todentamiset ovat (todentamismielessä) tehokkaita vain suhteessa itse oikeaperäisiksi todettuihin paketteihin tai jonoihin. Suojauksen tehostamiseksi voidaan muina aikoina lisäksi käyttää kolmea erilaista suojaustoimenpidettä. Ne ovat puheen salakirjoittaminen, satunnainen uudelleen suoritettava oikeaperäiseksi todentaminen ja ohjaussanomien salakirjoittaminen.

Puheen salakirjoittaminen

Puhesignaali salakirjoitetaan muuntamalla se ensin digitaaliseen muotoon. Tämä voidaan suorittaa millä tahansa useista tavanomaisista menetelmistä käyttämällä tai käyttämättä tiivistystä (compression) ja käyttämällä tai käyttämättä virheenkorjauskoodeja. Digitaalisten signaalien bitit jaetaan perättäisiin K bitin ryhmiin ja kukin ryhmistä salakirjoitetaan. Tarkemmin sanoen sekä matkaviestimessä että tukiasemalla RAND-sekvenssi, ESN- ja MIN1-tunnukset ja SSD-B -osakenttä yhdistetään ja syötetään sekoitusprosessiin. Sekoitusprosessi tuottaa 2K bittiä ja nämä bitit jaetaan ryhmiin A ja B, joissa kummassakin on K bittiä. Matkaviestimessä ryhmää A käytetään lähtevän puheen salakirjoittamiseksi ja ryhmää B käytetään tulevan

puheen salakirjoittamiseksi. Kääntäen: tukiasemalla ryhmää A käytetään tulevan puheen salakirjoittamiseksi ja ryhmää B käytetään lähtevän puheen salakirjoittamiseksi. Kuvio 8 esittää puheen salakirjoitus- ja avausprosessia.

Oikeaperäisyyden uudelleen todentaminen

Tukiaseman niin halutessa käynnistetään oikeaperäisyyden uudelleentodentamisprosessi sen varmistamiseksi, että matkaviestin, jonka tukiasema uskoo olevan aktiivisena, todella on se matkaviestin, jolle on annettu lupa olla aktiivisena. Tämä suoritetaan siten, että tukiasema pyytää matkaviestintä lähettämään hajakoodatun oikeaperäisyyden todistavan sekvenssin kuvion 9 mukaisesti. Jokaisen tällaisen pyynnön mukana tukiasema lähettää erityisen sekvenssin (RANDU). Matkaviestin luo hajakoodatun oikeaperäisyyden todistavan sekvenssin yhdistämällä RANDU-sekvenssin, matkaviestimen aluekoodin MIN2-tunnuksen, ESN-tunnuksen, MIN1-tunnuksen ja SSD-A -tunnuksen. Yhdistetty merkkijono syötetään sekoitusprosessiin ja tulokseksi saatava hajakoodattu oikeaperäisyyden todistava sekvenssi lähetetään tukiasemalle. Tässä kohdassa tukiasema pystyy todentamaan, että hajakoodattu oikeaperäisyyden todistava merkkijono on pätevä.

Ohjaussanomien salakirjoitus

Kolmas suojaustoimenpide koskee ohjaussanomien yksityisyyden varmistamista. Perustetun puhelun kuluessa voi syntyä eri tilanteita, jotka vaativat ohjaussanomien lähettämistä. Joissakin tilanteissa ohjaussanomat voivat merkittävästi ja haitallisesti vaikuttaa joko puhelun ottaneeseen matkaviestimeen tai tukiasemaan. Tästä syystä on toivottavaa, että jotkin lähetetyt ohjaussanomatyypit salakirjoitetaan (kohtalaisen hyvin) keskustelun ollessa kesken. Vaihtoehtoisesti voidaan valittujen sanomatyyppien valitut kentät salakirjoittaa. Tämä käsittää "datan" ohjaussano-

mat, kuten luottokorttien numerot ja puhelun uudelleenmäärittelevät ohjaussanomat. Tämä suoritetaan ohjaussanomien salakirjoitusjärjestelmällä (Control Message Cryptosystem, CMC).

Ohjaussanomien salakirjoitusjärjestelmä (CMC) on symmetristä avainta käyttävä salakirjoitusjärjestelmä, jolla on seuraavat ominaisuudet:

1) se on suhteellisen varma,
2) se toimii tehokkaasti kahdeksanbittisessä tietokoneessa, ja
3) se on itsensä suhteen käänteinen (so. involutiivinen).

CMC:n salakirjoitusavain on 256 tavua sisältävä matriisi *TBOX*[*z*], joka johdetaan "salaisuudesta" (esim. SSD-B -osakentästä) seuraavasti:

1. jokaisella *z*:lla välillä $0 \leq z < 256$ asetetaan *TBOX*[*z*]=*z*, ja

2. sovelletaan matriisia *TBOX*[*z*] ja salaisuutta (SSD-B) sekoitusprosessiin.

Tämä on olennaisesti se, mitä on esitetty elementeissä 301, 302 ja 303 kuviossa 8 (lukuunottamatta sitä, että bittien lukumäärä kuviossa 8 on 2K eikä 256 tavua).

Sen jälkeen kun avain on johdettu, CMC:tä voidaan käyttää ohjaussanomien salakirjoittamiseksi ja avaamiseksi. Vaihtoehtoisesti avain voidaan johtaa "lennossa" joka kerta, kun avainta käytetään. CMC:llä on kyky salakirjoittaa vaihtelevan pituuden omaavia sanomia, joissa on kaksi tavua tai useampia tavuja. CMC:n toiminta on itsensä suhteen käänteinen, resiprookkinen, eli involutiivinen. Toi-

sin sanoen täsmälleen samoja operaatioita sovelletaan salakirjoitettuun tekstiin selväkielisen tekstin tuottamiseksi kuin selväkieliseenkin tekstiin salakirjoitetun tekstin tuottamiseksi. Involuutiofunktio on sellainen funktio, joka on itsensä käänteisfunktio (esim. $x = 1/x'$, $x = T(T(x'))$). Siten CMC-operaatioiden kaksinkertainen soveltaminen pitää tiedot muuttumattomina.

Seuraavassa selityksessä on oletettu, että salakirjoitusprosessilla (ja avausprosessilla) selväkielinen teksti (tai salakirjoitettu teksti) on datapuskurissa ja että CMC operoi tämän datapuskurin sisällöllä siten, että tämän datapuskurin lopullinen sisältö käsittää salakirjoitetun tekstin (tai selväkielisen tekstin). Tämä merkitsee sitä, että elementit 502 ja 504 kuviossa 10 voivat olla yksi ja sama rekisteri.

CMC käsittää kolme perättäistä vaihetta, joista kukin muuttaa jokaista tavujonoa datapuskurissa. Huomaa, että sekä CMC kokonaisuudessaan että toinen CMC:n käsittämä vaihe ovat involuutio. Kun datapuskuri on d tavun pituinen ja kutakin tavua merkitään $b(i)$:llä, jossa i on välillä $0 \leq i < d$, niin:

I. CMC:n ensimmäinen vaihe on seuraavanlainen:

1. Asetetaan muuttujan z alkuarvoksi nolla.

2. Perättäisillä i:n kokonaislukuarvoilla välillä $0 \leq i < d$

a. muodostetaan muuttuja q seuraavasti: q = z ⊕ i:n vähiten merkitsevä tavu, missä ⊕ on bittikohtainen Boolen pelkkä-TAI -operaattori,

b. muodostetaan muuttuja k seuraavasti:
$k = TBOX[q]$,

c. päivitetään $b(i)$ seuraavasti:
$b(i) = b(i) + k \bmod 256$, ja

d. päivitetään z seuraavasti:
$z = b(i) + z \bmod 256$.

II. CMC:n toinen vaihe on involutiivinen ja käsittää:

1. kaikilla i:n arvoilla välillä $0 \leq i < (d\text{-}1)/2$:

$b(i) = b(i) \oplus (b(d\text{-}1\text{-}i)$ TAI $1)$, jossa TAI on bittikohtainen Boolen TAI-operaattori.

III. CMC:n viimeinen vaihe on salakirjoituksen avaaminen, joka on ensimmäiselle vaiheelle käänteinen:

1. Asetetaan muuttujan z alkuarvoksi nolla.

2. Perättäisillä i:n kokonaislukuarvoilla välillä $0 \leq i < d$

a. muodostetaan muuttuja q seuraavasti:
q = z $\oplus$ i:n vähiten merkitsevä tavu,

b. muodostetaan muuttuja k seuraavasti:
$k = TBOX[q]$,

c. päivitetään z seuraavasti:
$z = b(i) + z \bmod 256$.

c. päivitetään $b(i)$ seuraavasti:
$b(i) = b(i) - k \bmod 256$.

Kolmivaiheinen valittujen ohjaus- ja datasanomien salakirjoittamiseksi ja avaamiseksi käytettävä prosessi on esitetty kuviossa 10. Eräässä parhaana pidetyssä suoritusmuodossa ensimmäinen vaihe ja kolmas vaihe ovat autoavainsalakirjoitus ja -avaus vastaavasti. Autoavainjärjestelmä on ajallisesti muuttuva järjestelmä, jossa järjestelmän ulostuloa käytetään vaikuttamaan järjestelmän seuraavaan ulostuloon. Salakirjoituksia ja autoavainjärjestelmiä koskevat lisätiedot, katso W. Diffie ja M. E. Hellman, Privacy and Authentication: An Introduction to Cryptography, Proc. I.E.E.E., Vol. 67, n:o 3, maaliskuu 1979.

Matkaviestinlaite

Kuvio 11 esittää matkaviestinlaitteiston lohkokaaviota. Se käsittää ohjauslohkon 200, joka sisältää (vaikka ei esitetty) solukkopuhelimen näppäimistön, kuulokkeen ja laitteen tehonohjauskytkimen. Ohjauslohko 200 on liitetty suorittimeen 210, joka ohjaa matkaviestimen toimintoja, kuten puhesignaalien muuntamista digitaaliseen esitysmuotoon, ja mukaanluettuna virheenkorjauskoodit, lähtevien digitaalisten puhesignaalien salakirjoittaminen, tulevien puhesignaalien avaaminen, eri ohjaussanomien muodostaminen ja salakirjoittaminen (sekä avaaminen) jne. Lohko 210 on kytketty lohkoon 220, joka käsittää pääosan signaalien lähettämiseen ja vastaanottamiseen liittyvistä piireistä. Lohkot 200-220 ovat pohjimmiltaan tavanomaisia lohkoja, jotka suorittavat toimintoja, joita kaupalliset matkapuhelinlaitteet nykyisin suorittavat (vaikka kaupalliset laitteet eivät suorita salakirjoittamista ja avaamista). Tässä paljastettujen oikeaperäisyyden todentamis- ja salakirjoitusprosessien mukaanottamiseksi kuvion 11 laite sisältää myös lohkon 240, joka käsittää joukon suorittimeen 210 liitettyjä rekistereitä ja "persoonallisuusmoduulin" 230, joka myös on liitetty suorittimeen 210. Moduuli 230 voi olla osa matkapuhelinlaitteen fysikaalista rakennetta tai

se voi olla irrotettava (ja pistokkeella liitettävä) moduuli, joka on liitetty matkapuhelinlaitteeseen pistoliitännän avulla. Se voidaan liittää suorittimeen 210 myös sähkömagneettisen tien tai yhteyden välityksellä. Lyhyesti sanoen, moduuli 230 voi olla esimerkiksi toimikortti eli "älykortti" ("smart card").

Moduuli 230 käsittää sekoitussuorittimen 231 ja joukon suorittimeen 210 liitettyjä rekistereitä. Vaihtoehtoisesti toisessa parhaana pidetyssä suoritusmuodossa vain A-avain on moduulissa 230. Joukko etuja aiheutuu A-avaimen ja MIN1- ja MIN2-tunnusten asentamisesta moduulin 230 rekistereihin (ja ylläpitämisestä näissä) lohkon 240 rekisterien sijasta. On myös edullista tallentaa kehitetty SSD-kenttä moduulin 230 rekistereihin. On myös edullista sisällyttää moduulin 230 rekisterien joukkoon kaikki suorittimen 231 prosessien suorittamiseksi tarvittavat työrekisterit. Sisällytettäessä nämä elementit moduuliin 230 käyttäjä voi kantaa moduulia mukanaan, jolloin hän voi käyttää sitä eri matkaviestimien (esim. matkaviestimien "laajennusyksiköiden") yhteydessä, eikä mitään salaista informaatiota ole tallennettuna moduulin ulkopuolella. Voidaan tietenkin valmistaa matkaviestimiä, joissa moduuli 230 on laitteen yhdysrakenteinen ja kiinteä osa. Tällaisissa suoritusmuodoissa sekoitussuoritin 231 voidaan yhdistää suorittimeen 230. Lohko 240 tallentaa laitteen ESN-tunnuksen ja vastaanotettavat eri RAND-sekvenssit.

Vaikka edellä esitetty patenttiselitys on laadittu siten, että se liittyy tilaajan oikeaperäisyyden todentamiseen solukkopuhelinympäristössä ja että se käsittää henkilökohtaiset viestintäverkot, jotka palvelevat kannettavia lompakon kokoisia käsipuhelimia, niin on selvää, että tämän keksinnön periaatteet ovat sovellettavissa mihin tahansa ympäristöön, jossa viestinnän on havaittu olevan riittä-

mättömästi salattua ja jossa jäljittely on mahdollinen ongelma. Tämä käsittää esimerkiksi tietokoneverkot.

Patenttivaatimukset

1. Menetelmä sanomasignaalien joukon salaamiseksi lähettämistä varten viestintäjärjestelmässä, **tunnettu** siitä, että

luodaan avainsignaalien joukko hajakoodaamalla ensimmäisten signaalien joukko ja toisten signaalien joukko;

salataan (505) mainittu sanomasignaalien joukko mainitun avainsignaalien joukon osajoukon perusteella ensimmäisten välisignaalien joukon muodostamiseksi;

muutetaan mainittua ensimmäisten välisignaalien joukkoa avaimettomalla evolventillä muunnoksella (507), joka muuntaa mainitun ensimmäisten välisignaalien joukon ensimmäistä osajoukkoa mainittujen ensimmäisten välisignaalien toisen osajoukon perusteella toisten välisignaalien joukon muodostamiseksi; ja

puretaan (511) mainitun toisten välisignaalien joukon salaus muunnoksella, joka on käänteinen mainitulle salausvaiheelle salattujen sanomasignaalien joukon (504) muodostamiseksi lähettämistä varten mainitussa viestintäjärjestelmässä.

2. Menetelmä sanomasignaalien joukon salauksen purkamiseksi vastaanottamista varten viestintäjärjestelmässä, **tunnettu** siitä, että

luodaan avainsignaalien joukko hajakoodaamalla ensimmäisten signaalien joukko ja toisten signaalien joukko;

salataan (505) mainittu sanomasignaalien joukko mainitun avainsignaalien joukon osajoukon perusteella ensimmäisten välisignaalien joukon muodostamiseksi;

muutetaan mainittua ensimmäisten välisignaalien joukkoa avaimettomalla evolventillä muunnoksella (507), joka muuntaa mainitun ensimmäisten välisignaalien joukon ensimmäistä osajoukkoa mainittujen ensimmäisten välisignaalien toisen osajoukon perusteella toisten välisignaalien joukon muodostamiseksi; ja

puretaan (511) mainittu toisten välisignaalien joukko muunnoksella, joka on käänteinen mainitulle salausvaiheelle salaukseltaan purettujen sanomasignaalien (504) muodostamiseksi.

3. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että se käsittää vaiheet:

ensimmäisten signaalien joukon vastaanottamiseksi;

mainitun sanomasignaalien joukko luomiseksi; ja

mainitun salattujen sanomasignaalien joukon lähettämiseksi.

4. Patenttivaatimuksen 2 mukainen menetelmä, **tunnettu** siitä, että se käsittää vaiheet:

ensimmäisten signaalien joukon luomiseksi;

mainitun salaukseltaan purettujen sanomasignaalien joukon käyttämiseksi; ja

mainitun sanomasignaalien joukon vastaanottamiseksi.

5. Laite sanomasignaalien joukon salaamiseksi lähettämistä varten viestintäjärjestelmässä, **tunnettu** siitä, että se käsittää:

välineet avainsignaalien joukon luomiseksi hajakoodaamalla ensimmäisten signaalien joukon ja toisten signaalien joukon;

välineet (501) mainitun sanomasignaalien joukon salaamiseksi mainitun avainsignaalien joukon osajoukon perusteella ensimmäisten välisignaalien joukon muodostamiseksi;

välineet (509) mainitun ensimmäisten välisignaalien joukon muuttamiseksi avaimettomalla evolventillä muunnoksella, joka muuntaa mainitun ensimmäisten välisignaalien joukon ensimmäistä osajoukkoa mainittujen ensimmäisten välisignaalien toisen osajoukon perusteella toisten välisignaalien joukon muodostamiseksi; ja

välineet (513) mainitun toisten välisignaalien joukon salauksen purkamiseksi muunnoksella, joka on käänteinen mainitulle salausvaiheelle salattujen sanomasignaalien joukon muodostamiseksi lähettämistä varten mainitussa viestintäjärjestelmässä.

6. Laite sanomasignaalien joukon salauksen purkamiseksi vastaanottamista varten viestintäjärjestelmässä, **tunnettu** siitä, että se käsittää:

välineet avainsignaalien joukon luomiseksi hajakoodaamalla ensimmäisten signaalien joukon ja toisten signaalien joukon;

välineet (505) mainitun sanomasignaalien joukon salaamiseksi mainitun avainsignaalien joukon osajoukon perusteella ensimmäisten välisignaalien joukon muodostamiseksi;

välineet (509) mainitun ensimmäisten välisignaalien joukon muuttamiseksi avaimettomalla evolventillä muunnoksella, joka muuntaa mainitun ensimmäisten välisignaalien joukon ensimmäistä osajoukkoa mainittujen ensimmäisten välisig-

naalien toisen osajoukon perusteella toisten välisignaalien joukon muodostamiseksi; ja

välineet (513) mainitun toisten välisignaalien joukon salauksen purkamiseksi muunnoksella, joka on käänteinen mainitulle salausvaiheelle salaukseltaan purettujen sanomasignaalien joukon muodostamiseksi.

7. Patenttivaatimuksen 5 mukainen laite, **tunnettu** siitä, että laite lisäksi käsittää välineet:

ensimmäisten signaalien joukon vastaanottamiseksi;

mainitun sanomasignaalien joukon luomiseksi; ja

mainitun salattujen signaalien joukon lähettämiseksi.

8. Patenttivaatimuksen 6 mukainen laite, **tunnettu** siitä, että laite lisäksi käsittää välineet:

ensimmäisten signaalien joukon luomiseksi;

mainitun salaukseltaan purettujen sanomasignaalien joukon käyttämiseksi; ja

mainitun sanomasignaalien joukon vastaanottamiseksi.

Patentkrav

1. Förfarande för kryptering av en uppsättning meddelandesignaler för sändning i ett kommunikationssystem, **kännetecknat** av att:

skapa en uppsättning nyckelsignaler genom hashning av en uppsättning av första signaler och en uppsättning av andra signaler;

kryptera (505) nämnda uppsättning meddelandesignaler baserat på en delmängd av nämnda uppsättning nyckelsignaler

för att bilda en uppsättning av första mellanliggande signaler;

ändra nämnda uppsättning av första mellanliggande signaler i överensstämmelse med en okodad evolvent transformation (507) som modifierar en första delmängd av nämnda uppsättning av första mellanliggande signaler baserat på en andra delmängd av nämnda första mellanliggande signaler för att bilda en uppsättning av andra mellanliggande signaler; och

dekryptering (511) nämnda uppsättning av andra mellanliggande signaler i överensstämmelse med en transformation, som är inversen av nämnda krypteringssteg, för att bilda en uppsättning krypterade meddelandesignaler (504) vilka skall sändas i nämnda kommunikationssystem.

2. Förfarande för dekryptering av en uppsättning meddelandesignaler mottagna i ett kommunikationssystem, **kännetecknat** av att:

skapa en uppsättning nyckelsignaler genom hashning av en uppsättning av första signaler och en uppsättning av andra signaler;

kryptera (505) nämnda uppsättning meddelandesignaler baserat på en delmängd av nämnda uppsättning nyckelsignaler för att bilda en uppsättning av första mellanliggande signaler;

ändra nämnda uppsättning av första mellanliggande signaler med en okodad evolvent transformation (507) som modifierar en delmängd av nämnda uppsättning av första mellanliggande signaler baserat på en andra delmängd av nämnda första mellanliggande signaler för att bilda en uppsättning av andra mellanliggande signaler; och

dekryptera (511) nämnda uppsättning av andra mellanliggande signaler med en transformation, som är inversen av nämnda krypteringssteg, för att bilda en uppsättning dekrypterade meddelandesignaler (504).

3. Förfarande enligt patentkrav 1, **kännetecknat** av steget att:

motta uppsättningen första signaler,

generera nämnda uppsättning meddelandesignaler, och

sända nämnda uppsättning krypterade meddelandesignaler.

4. Förfarande enligt patentkrav 2, **kännetecknat** av steget att:

generera uppsättningen första signaler,

påverka nämnda uppsättning dekrypterade meddelandesignaler, och

motta mämnda uppsättning meddelandesignaler.

5. Anordning för kryptering av en uppsättning meddelandesignaler för sändning i ett kommunikationssystem, **kännetecknad** av:

organ för att skapa en uppsättning nyckelsignaler genom hashning av en uppsättning första signaler och en uppsättning andra signaler;

organ (501) för kryptering av nämnda uppsättning meddelandesignaler baserat på en delmängd av nämnda uppsättning nyckelsignaler för att bilda en uppsättning av första mellanliggande signaler;

organ (509) för att ändra nämnda uppsättning av första mellanliggande signaler i överensstämmelse med en okodad evolvent transformation som modifierar en första delmängd av nämnda uppsättning av första mellanliggande signaler baserat på en andra delmängd av nämnda första mellanliggande signaler för att bilda en uppsättning av andra mellanliggande signaler; och

organ (513) för att dekryptera nämnda uppsättning av andra mellanliggande signaler i överensstämmelse med en tranformation, som är inversen av nämnda krypteringssteg, för att bilda en uppsättning krypterade meddelandesignaler som skall sändas i nämnda kommunikationssystem.

6. Anordning för dekryptering av en uppsättning meddelandesignaler mottagna i ett kommunikationssystem, **kännetecknad** av:

organ för att skapa en uppsättning nyckelsignaler genom hashning av en uppsättning första signaler och en uppsättning andra signaler;

organ (501) för kryptering av nämnda uppsättning meddelandesignaler baserat på en delmängd av nämnda uppsättning nyckelsignaler för att bilda en uppsättning av första mellanliggande signaler;

organ (509) för att ändra nämnda uppsättning av första mellanliggande signaler med en okodad evolvent transformation som modifierar en första delmängd av nämnda uppsättning av första mellanliggande signaler baserat på en andra delmängd av nämnda första mellanliggande signaler för att bilda en uppsättning av andra mellanliggande signaler; och

organ (513) för att dekryptera nämnda uppsättning av andra mellanliggande signaler med en transformation, som är inversen av nämnda krypteringssteg, för att bilda en uppsättning dekrypterade meddelandesignaler.

7. Anordning enligt patentkrav 5, **kännetecknad** av:

organ för att motta uppsättningen första signaler,

organ för att generera nämnda uppsättning meddelandesignaler, och

organ för att sända nämnda uppsättning krypterade meddelandesignaler.

8. Anordning enligt patentkrav 6, **kännetecknad** av:

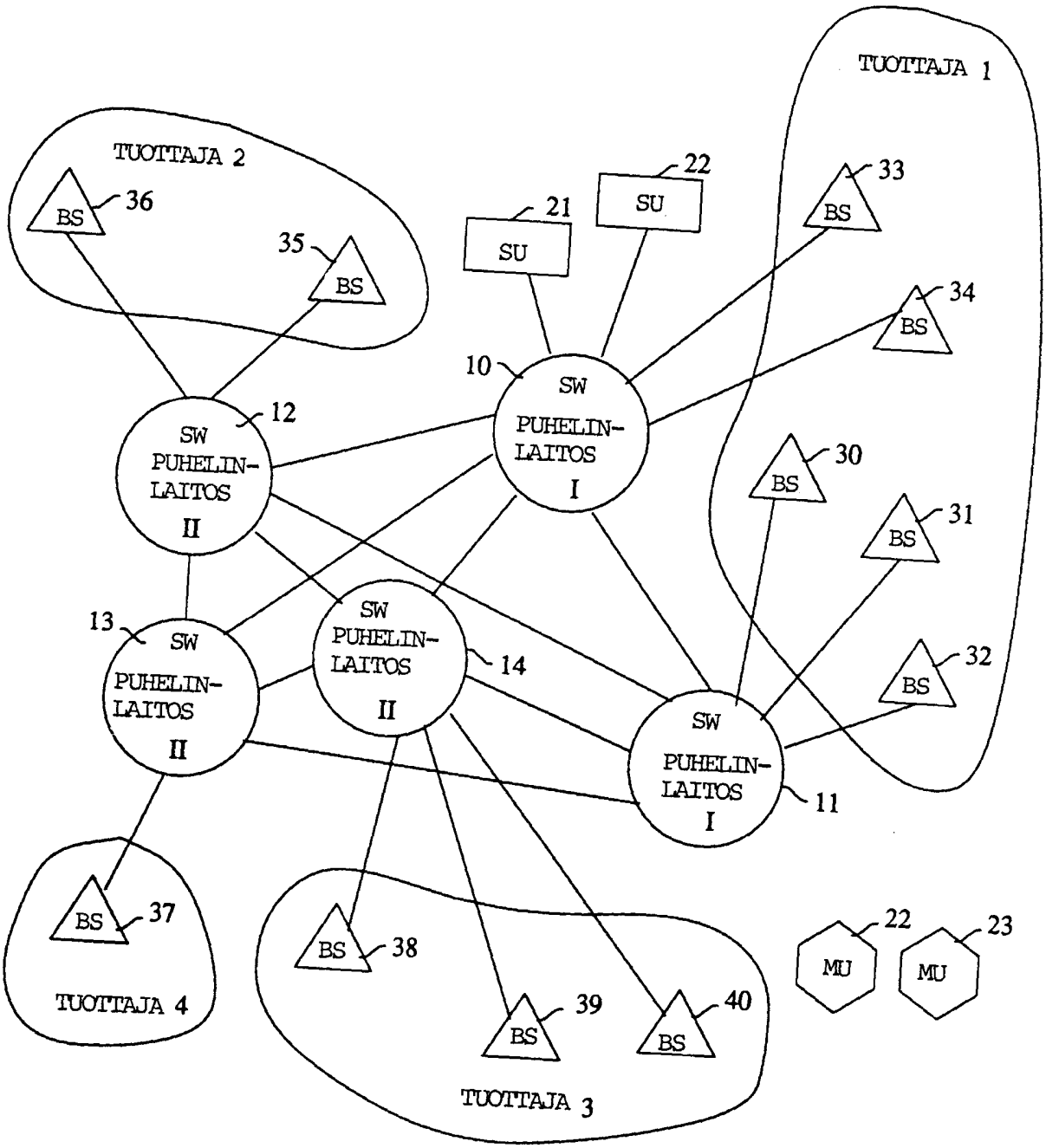
organ för att generera uppsättningen första signaler,

organ för påverkan på nämnda uppsättning dekrypterade meddelandesignaler, och

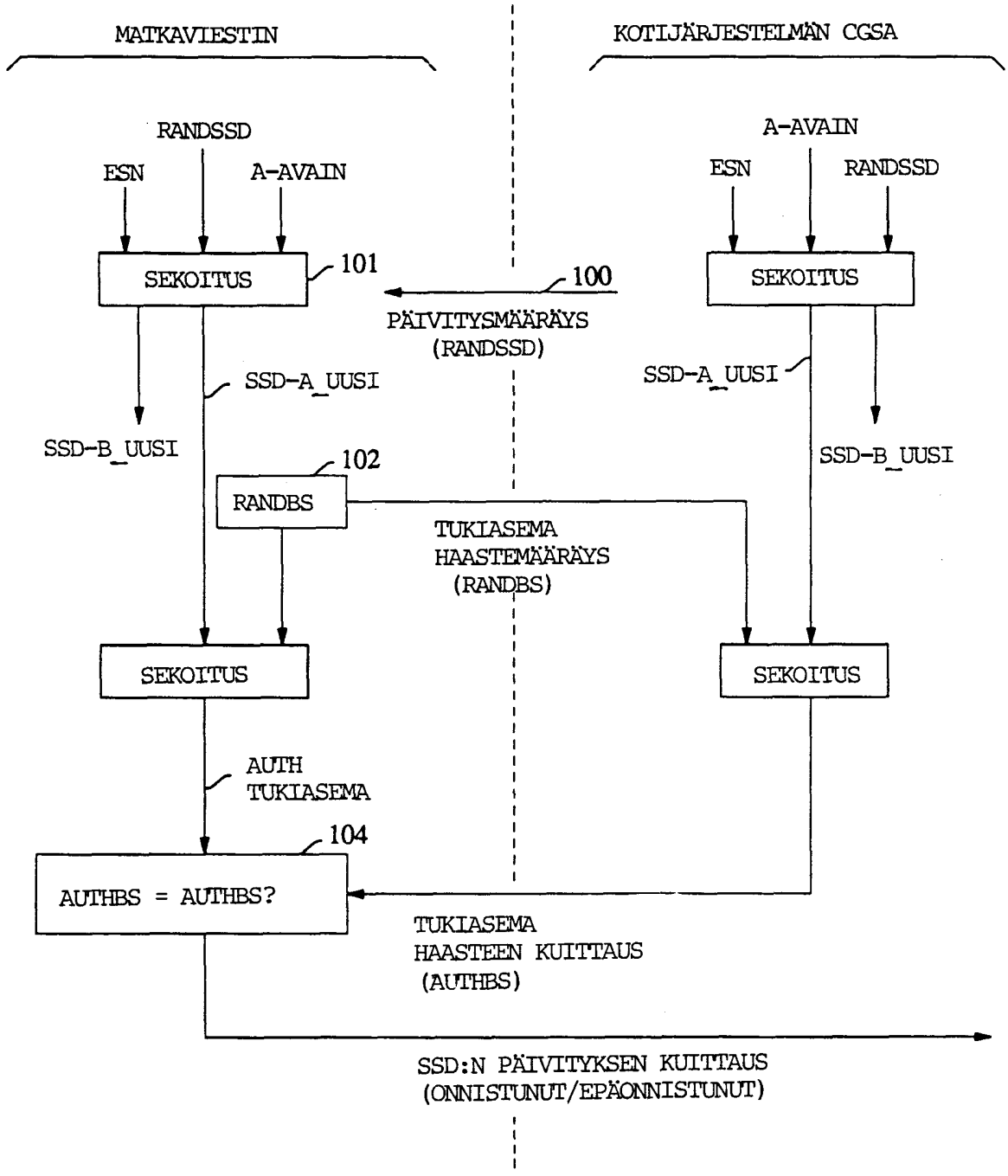
organ för att motta nämnda uppsättning meddelandesignaler.

108690

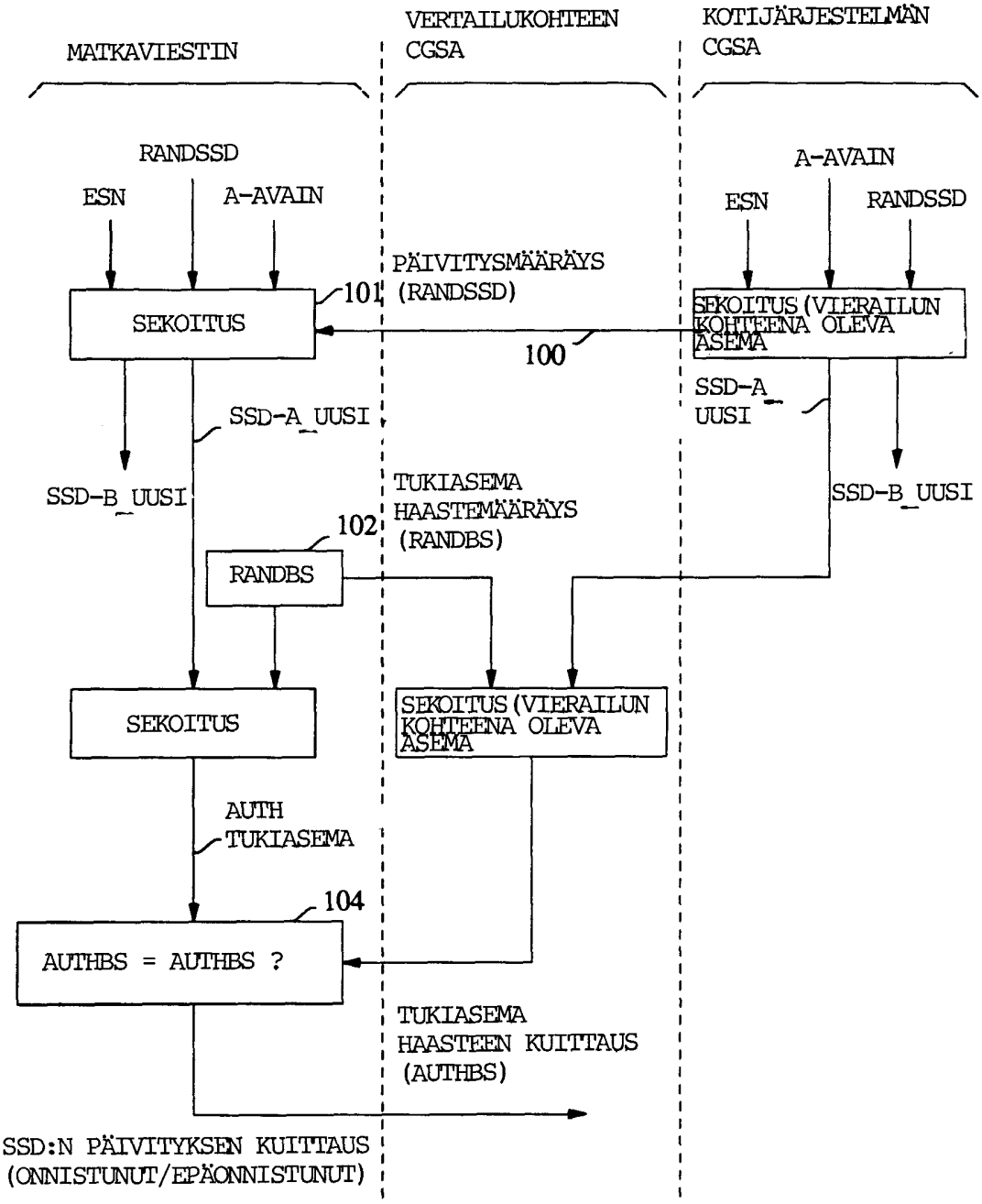
KUVIO 1



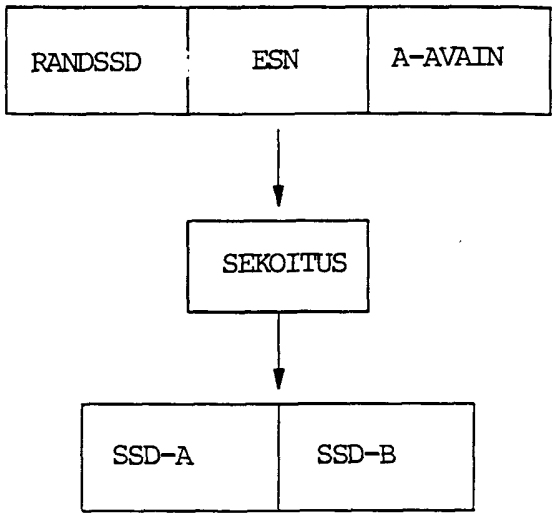
KUVIO 2


MATKAVIESTIN
KOTIJÄRJESTELMÄN CGSA
RANDSSD
ESN
A-AVAIN
A-AVAIN
ESN
RANDSSD
SEKOITUS
101
100
SEKOITUS
PÄIVITYSMÄÄRÄYS
(RANDSSD)
SSD-A_UUSI
SSD-A_UUSI
SSD-B_UUSI
SSD-B_UUSI
102
RANDBS
TUKIASEMA
HAASTEMÄÄRÄYS
(RANDBS)
SEKOITUS
SEKOITUS
AUTH
TUKIASEMA
104
AUTHBS = AUTHBS?
TUKIASEMA
HAASTEEN KUITTAUS
(AUTHBS)
SSD:N PÄIVITYKSEN KUITTAUS
(ONNISTUNUT/EPÄONNISTUNUT)

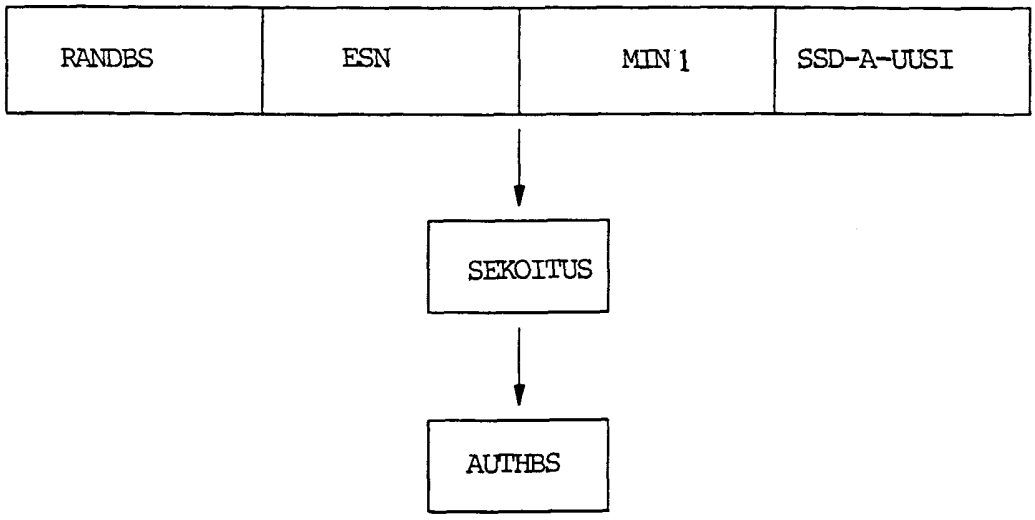
KUVIO 3


MATKAVIESTIN
VERTAILUKOHTEEN CGSA
KOTIJÄRJESTELMÄN CGSA
RANDSSD
ESN
A-AVAIN
PÄIVITYSMÄÄRÄYS (RANDSSD)
101
SEKOITUS
100
A-AVAIN
ESN
RANDSSD
SEKOITUS (VIERAILUN KOHTEENA OLEVA ASEMA
SSD-A_UUSI
SSD-A UUSI
SSD-B_UUSI
SSD-B_UUSI
TUKIASEMA HAASTEMÄÄRÄYS (RANDBS)
102
RANDBS
SEKOITUS
SEKOITUS (VIERAILUN KOHTEENA OLEVA ASEMA
AUTH TUKIASEMA
104
AUTHBS = AUTHBS ?
TUKIASEMA HAASTEEN KUITTAUS (AUTHBS)
SSD:N PÄIVITYKSEN KUITTAUS (ONNISTUNUT/EPÄONNISTUNUT)

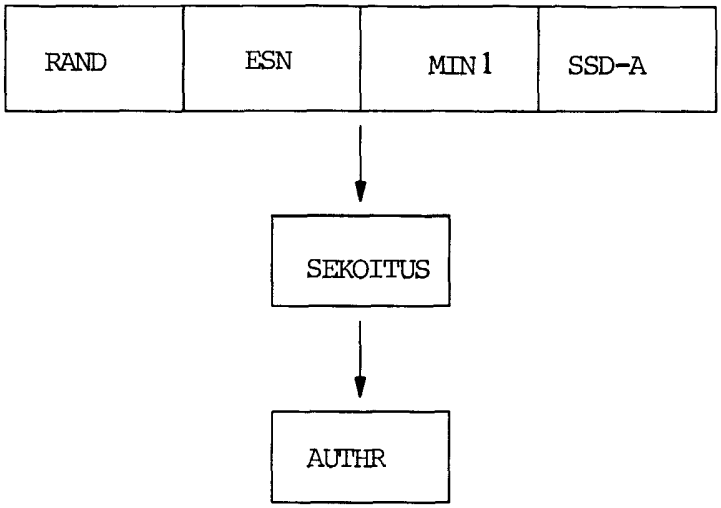
KUVIO 4



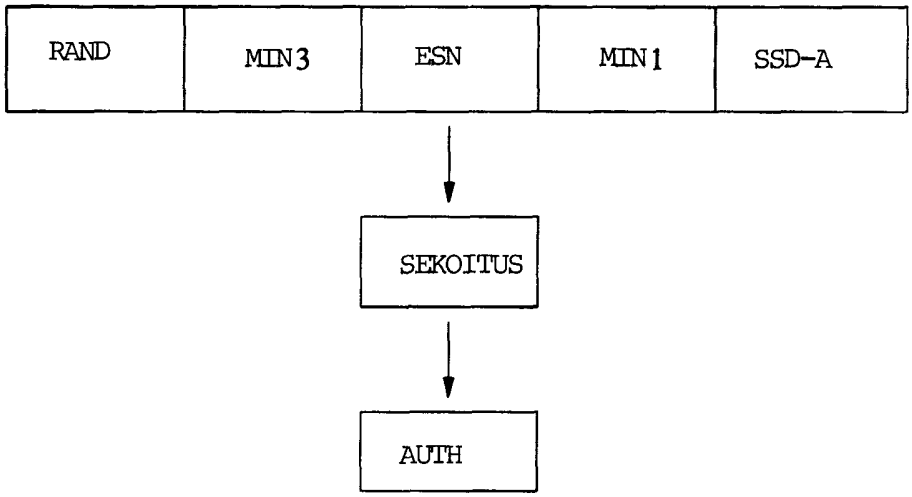
KUVIO 5



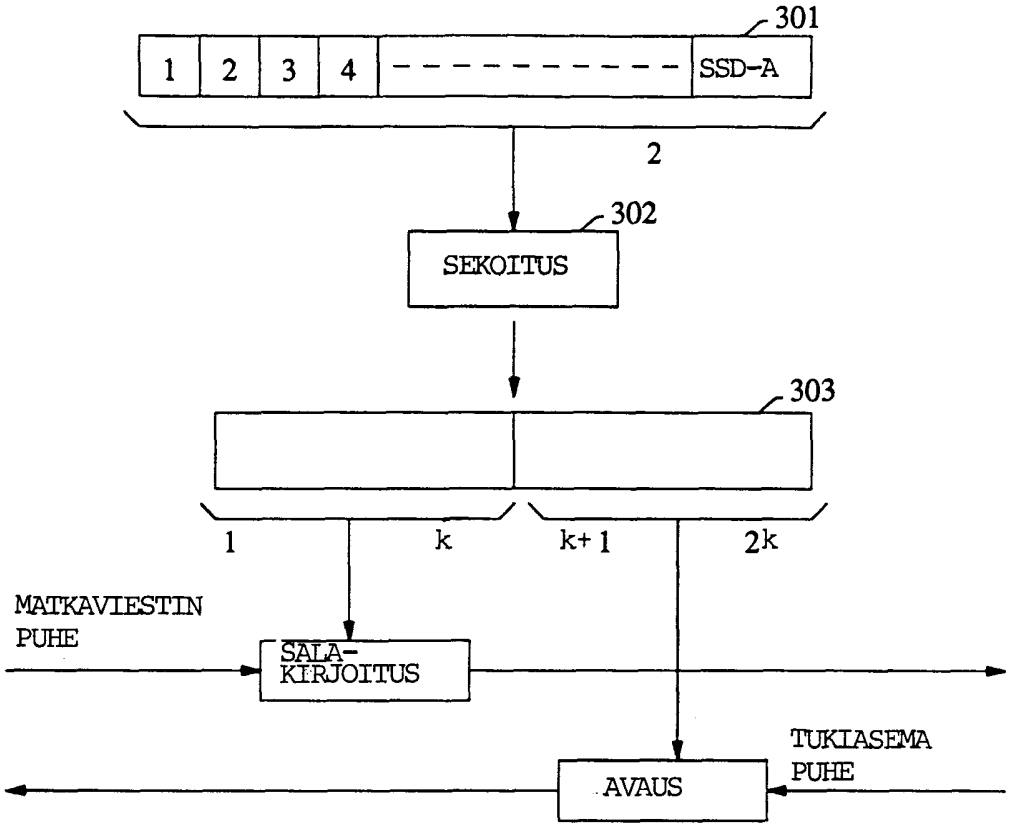
KUVIO 6



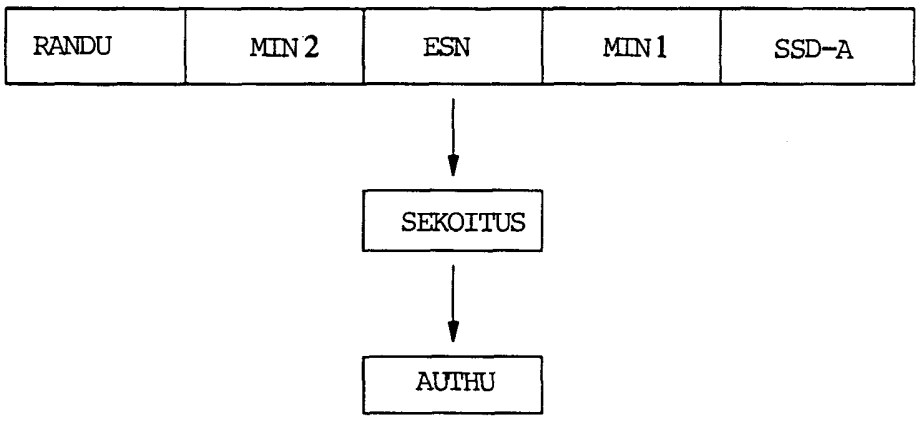
KUVIO 7



KUVIO 8

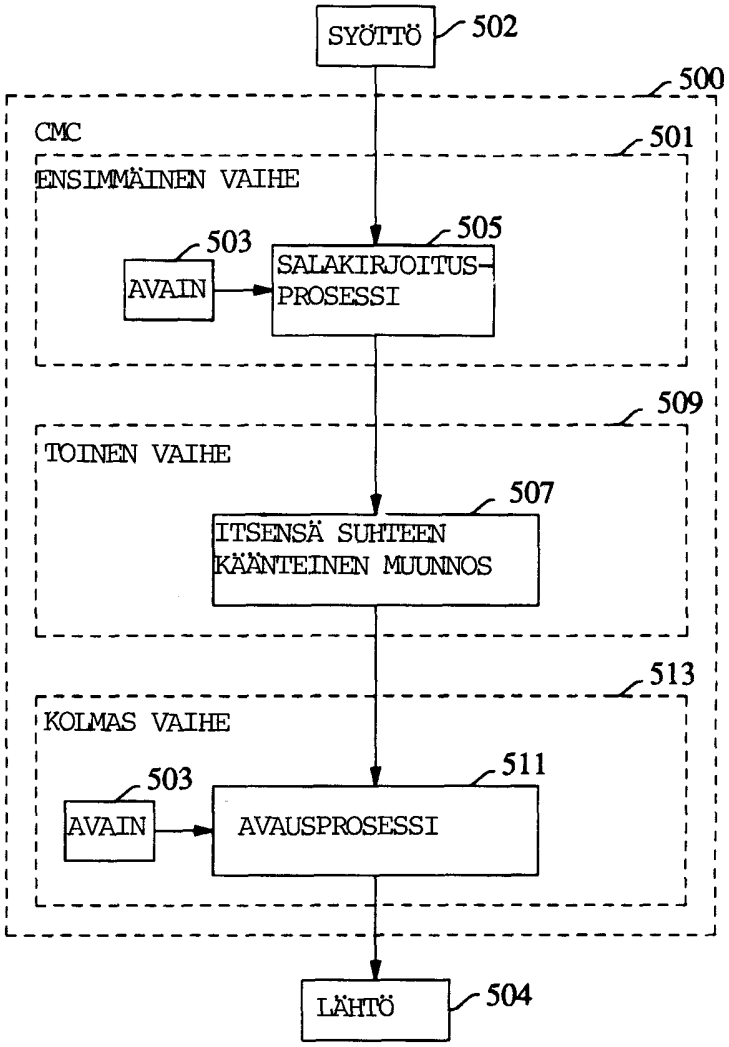


KUVIO 9



KUVIO 10

OHJAUSSANOMIEN SALAKIRJOITUSJÄRJESTELMÄ



KUVIO 11