(19) Octrooiraad Nederland

(11) Publikatienummer: **9202284**

(12) **A TERINZAGELEGGING**

(21) Aanvraagnummer: **9202284**

(22) Indieningsdatum: **29.12.92**

(51) Int.Cl.[5]: **G09C 1/00**, H04L 9/28

(43) Ter inzage gelegd: **18.07.94 I.E. 94/14**

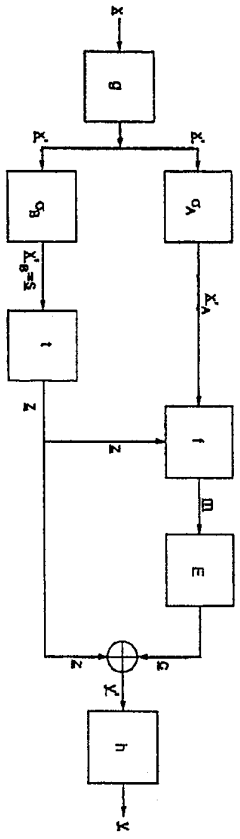
(71) Aanvrager(s): **Koninklijke PTT Nederland N.V. te Groningen**

(72) Uitvinder(s): **De uitvinder heeft van tenaamstelling afgezien**

(74) Gemachtigde: **Ir. Th.A.H.J. Smulders c.s.**
Vereenigde Octrooibureaux
Nieuwe Parklaan 97
2587 BN 's-Gravenhage

(54) **Bloksgewijze vercijfering op basis van algebraïsche coderingsmethoden**

(57) Werkwijze voor bloksgewijze vercijfering, ontcijfering in een cryptosysteem. Een berichtblok (x) van n berichtsymbolen wordt vercijferd in een cryptogram (Y) van lengte n. Een eerste deelblok (x_A'), een selectie (σA) van k<n berichtsymbolen uit het te vercijferen berichtblok, wordt omgezet in een codewoord (c) van lengte n met behulp van een kxn-vercijfermatrix (E) van rang k, welke een willekeurig gekozen fouten corrigerende, (n, k) lineaire code C genereert. Met een tweede deelblok (x_B') gevormd door de n-k resterende berichtsymbolen (σ_B), wordt een syndroomvector (s) van lengte n-k bepaald, waarmee uit een gegeven syndroom/foutvector-verzameling (t) een unieke foutvector (z) van lengte n wordt bepaald, welke vervolgens bij het codewoord wordt opgeteld om het cryptogram (y) te vormen. Dankzij de werkwijze is de informatiedichtheid R=1 tussen zender en ontvanger, en is bloksgewijs en herhaald vercijferen mogelijk.



NL A 9202284

Titel: Bloksgewijze vercijfering op basis van algebraïsche coderingsmethoden

A. Achtergrond van de uitvinding

1. Gebied van de uitvinding

De uitvinding ligt op het gebied van cryptosystemen. Meer in het bijzonder heeft zij betrekking op een werkwijze voor het bloksgewijze vercijferen en ontcijferen van berichten gebaseerd op algebraïsche coderingsmethoden onder gebruikmaking van geheime sleutel-elementen.

2. Stand van de techniek

Voor de beveiliging van informatieuitwisseling over communicatiekanalen in communicatie-netwerken zijn cryptosystemen, waarin vercijferen en ontcijferen geschiedt op basis van algebraïsche coderingsmethoden, op zich bekend. Zo beschrijven referentie [1] en referenties [2] en [3] respectievelijk een 'openbare sleutel'-cryptosysteem en een 'geheime sleutel'-cryptosysteem, welke gebruik maken van fouten corrigerende codes. Daarbij wordt een vercijferschema toegepast, waarin een te verzenden bericht van lengte k wordt omgezet in een cryptogram door met behulp van een codegenerator eerst de k berichtsymbolen om te zetten in een codewoord of codevector van lengte $n>k$ volgens een dergelijke fouten corrigerende code, en vervolgens in de verkregen codevector door optelling met een foutvector als het ware kunstmatig een naderhand te corrigeren foutpatroon aan te brengen. De foutvector wordt daarbij willekeurig gekozen uit een verza-

meling van foutvectoren, welke foutpatronen representeren, die corrigeerbaar zijn met behulp van de gegeven code. Het uit referentie [1] bekende cryptosysteem maakt gebruik van een fouten corrigerende code, i.c. de Goppa code, die willekeurig gekozen foutvectoren van Hamming-gewicht $\leq t$ kan corrigeren. Het uit referenties [2] en [3] bekende cryptosysteem past fouten corrigerende codes, i.c. BCH-codes, toe met lengte van $n \leq 250$ bits en een minimum afstand $d \leq 6$, waarbij de foutvectoren willekeurig worden gekozen uit een van tevoren vastgelegde (geheime) verzameling van foutvectoren met een Hamming-gewicht van ca. n/2. Aan de ontvangstzijde worden de cryptogrammen gedecodeerd, waarbij uit het cryptogram eerst het toegevoegde foutpatroon uniek wordt bepaald, waarna het codewoord kan worden gedecodeerd in het oorspronkelijke bericht. In een 'openbare-sleutel'-cryptosysteem is de codegenerator in 'scrambled' vorm openbaar, in een 'geheime-sleutel'-cryptosysteem niet. Aangezien voor dergelijke fouten corrigerende codes snelle decodeeralgoritmen bestaan zijn hoge vercijfersnelheden ($\geq$ 1Mbits/s) realiseerbaar. Uit referentie [4] is een dergelijk 'openbare-sleutel'-cryptosysteem bekend, waarin het feit, dat aan de ontvangstzijde het kunstmatig toegevoegde foutpatroon uniek kan worden teruggevonden, wordt gebruikt om of extra ('secundaire' bericht-)informatie over tezenden zoals een authenticatie code, of een deel van het foutpatroon daadwerkelijk voor fouten correctie op de communicatieverbinding toe te passen.

Een op dergelijke vercijferschema's gebaseerd cryptosysteem heeft de volgende belangrijke nadelen:

- de (primaire) informatie-dichtheid R (eng.: information rate) tussen zender en ontvanger bedraagt k/n, is derhalve steeds kleiner dan 1;

- omdat k=n, zijn gangbare methoden voor bloksgewijze vercijfering

niet zonder meer toepasbaar, en is herhaald vercijferen niet mogelijk. Bovendien is het vercijferschema door een inherente lineariteit als zodanig onveilig. Weliswaar geeft referentie [3], meer in het bijzonder sectie III. B., een suggestie om aan dit nadeel te ontkomen, t.w. door het gebruik van niet-lineaire codes. Dit heeft echter het nadeel, dat de eenvoud van het gebruik van lineaire codes verloren gaat.

B. Samenvatting van de uitvinding

Met de uitvinding wordt beoogd te voorzien in een werkwijze voor bloksgewijze vercijfering en ontcijfering gebaseerd op algebraïsche coderingsmethoden onder gebruikmaking van 'geheime sleutel'-elementen, welke werkwijze bovengenoemde nadelen niet bezit.

De uitvinding berust op het volgende inzicht. Bij een corrigerende code wordt tevens een pariteits-controle matrix gekozen, waarmee aan de ontvangstzijde kan worden vastgesteld of een verzonden codevector al dan niet foutloos is overgekomen. Vermenigvuldiging van de pariteitscontrolematrix met een correct ontvangen codevector (van lengte n) resulteert in de nulvector van lengte n-k, met een foutief ontvangen codevector echter in een restvector $\neq \underline{0}$ van lengte n-k, syndroomvector geheten. In een 'geheime-sleutel'-cryptosysteem is de verzameling van foutvectoren, waaruit aan de zendzijde willekeurig wordt gekozen, geheim en zo samengesteld, dat er bij iedere mogelijke syndroomvector, waarin de pariteitscontrole aan de ontvangstzijde kan resulteren, slechts één foutvector bestaat, en dat alle foutvectoren verschillend zijn. Hierop berust het feit, dat aan de ontvangstzijde de aan de zendzijde toegepaste foutvector uniek kan worden teruggevonden. Door n-k extra berichtsymbolen, rechtsstreeks of via een inverteerbare

transformatie, op te vatten als een syndroomvector, en daarmee, op soort gelijke wijze als aan de ontvangstzijde, ook aan de zendzijde de toe te passen foutvector te bepalen, wordt bereikt, dat steeds blokken worden vercijferd in cryptogrammen van dezelfde lengte. Een willekeurige keuze van een foutvector aan de zendzijde blijft daarbij in zoverre gehandhaafd, naarmate de n-k extra berichtsymbolen in verschillende blokken ten opzichte van elkaar willekeurig zijn.

Een werkwijze voor het vercijferen en ontcijferen van te verzenden berichten in een cryptosysteem voor beveiliging van communicatieverbindingen, welke werkwijze omvat een eerste deelwerkwijze voor het vercijferen van berichtdata, waarbij de berichtdata bloksgewijze worden omgezet in cryptogrammen, geschikt voor verzending over een te beveiligen communicatieverbinding, en een tweede deelwerkwijze voor het ontcijferen van ontvangen cryptogrammen, waarbij de berichtdata worden herkregen, omvat daartoe volgens de uitvinding de stappen volgens conclusie 1.

In een eerste voorkeursuitvoering omvat de werkwijze bovendien de stap volgens conclusie 2, en in een tweede voorkeursuitvoering de stap volgens conclusie 3. Daardoor wordt het nadeel van de lineariteit van het vercijferschema opgeheven, terwijl toch lineaire codes kunnen worden toegepast.

Uit referentie [6] is bekend, dat het Rao-Nam-schema een zekere kwetsbaarheid heeft onder bepaalde zogenoemde 'chosen-plaintext' aanvallen, en dat de mate van kwetsbaarheid daarvoor kan worden verminderd door aan de zendzijde de vercijferstap met de matrix E vooraf te laten gaan door een transformatie van de berichtvector met een geheime inverteerbare, niet-lineaire functie, welke bovendien afhankelijk kan worden gekozen van de geselecteerde foutvector. In een voorkeursuitvoering omvat de werkwijze

volgens de uitvinding verder de stap volgens conclusie 4.

Als extra voordelen van vercijfer- en ontcijferschema's volgens de uitvinding kunnen nog worden genoemd, dat er geen restrictie is aan het Hamming-gewicht van de te gebruiken foutvectoren, en dat vercijfering van een nul-boodschap (i.e. de berichtvector met uitsluitend nul-symbolen) en van een eenheidsboodschap (i.e. een berichtvector met slechts een berichtsymbool en overigens nul-symbolen) een op deze vercijferschema's gebaseerd cryptosysteem niet onveilig maakt, althans de veiligheid niet aantoonbaar vermindert.

C. Referenties

[1] R.J. McEliece: "A public-key cryptosystem based on algebraic coding theory", DSN Progress Report 42-44, Jet Propulsion Laboratory, Pasadena, pp. 114-116, January 1978;

[2] T.R.M. Rao and K.-H. Nam: "Private-key algebraic cryptosystems", in: Advances in Cryptology - CRYPTO '86. New York: Springer-Verlag, 1986, pp. 35-48;

[3] T.R.N. Rao and K.H. Nam: "Private-key algebraic-code encryptions", IEEE Trans. Inform. Theory, vol. IT-35, no. 4, pp. 829-833, July 1989;

[4] USA-A-5,054,066;

[5] J. Meijers and J. van Tilburg: "Extended majority voting and private-key algebraic-code encryptions", ASIACRYPT'91, Fujiyoshida, Japan, November 1991;

[6] R. Struik and J. van Tilburg: "The Rao-Nam scheme is insecure against a chosen-plaintext attack", in: Advances in Cryptology - CRYPTO '87. New York: Springer-Verlag, 1987, pp. 445-457.

D. Korte beschrijving van de tekening

Hierna zal de uitvinding worden toegelicht in een beschrijving van enkele uitvoeringsvoorbeelden. Daarbij zal worden verwezen naar een tekening met de volgende figuren:

FIG. 1 toont in een blokschema een overzicht van een gangbaar cryptosysteem op basis van een geheime sleutel;

FIG. 2(a) toont voor het in FIG. 1 getoonde cryptosysteem een bekend vercijferschema gebaseerd op een algebraïsche coderingsmethode;

FIG. 2(b) toont een met het in FIG. 2(a) getoonde vercijferschema corresponderend, bekend ontcijferschema;

FIG. 3(a) toont voor het in FIG. 1 getoonde cryptosysteem een vercijferschema gebaseerd op een algebraïsche coderingsmethode volgens de uitvinding;

FIG. 3(b) toont een met het in FIG. 3(a) getoonde vercijferschema corresponderend ontcijferschema volgens de uitvinding;

FIG. 4(a) toont schematisch een specifieke uitvoering van het vercijferschema volgens FIG. 3(a);

FIG. 4(b) toont schematisch een specifieke uitvoering van het ontcijferschema volgens FIG. 4(b).

E. Beschrijving van een uitvoeringsvoorbeeld

Cryptografische systemen, of korter cryptosystemen, worden toegepast voor de beveiliging van communicatieverbindingen zoals bijvoorbeeld in telecommunicatienetwerken. Er zijn 'openbare-sleutel'-cryptosystemen en 'geheime-sleutel'-cryptosystemen. De uitvinding is gericht op een 'geheime-

sleutel'-cryptosysteem, waarin algebraïsche coderingsmethoden worden toegepast voor het vercijferen en ontcijferen van te verzenden berichten. In een 'geheime-sleutel'-cryptosysteem worden over een communicatieverbinding te verzenden berichten vercijferd en ontcijferd op basis van een geheime sleutel of een aantal geheime sleutelelementen. In FIG. 1 zijn de essentiële componenten van een dergelijk cryptosysteem weergegeven. Een aan de zendzijde door een berichtzender 1 gegenereerd bericht $\underline{m}$ wordt in een vercijfereenheid 2 vercijferd middels een vercijferalgoritme ENC tot een cryptogram $\underline{y}$, dat vervolgens over een communicatieverbinding 3 wordt verzonden. Aan de ontvangstzijde van de communicatieverbinding 3 wordt in een ontcijfereenheid 4 het cryptogram $\underline{y}$ weer ontcijferd middels een ontcijferalgoritme DEC in het oorspronkelijke bericht $\underline{m}$, dat vervolgens wordt aangeboden aan de ontvanger 5.

Symbolisch kan dit worden uitgedrukt door:

$$ENC(\underline{m},k) = \underline{y} \quad \text{en} \quad DEC(\underline{y},k) = \underline{m} \qquad \{1\}$$

Daarbij zijn de vercijfer- en ontcijferalgoritmen afhankelijk van eenzelfde geheime sleutel k, welke vooraf door een sleutelbeherende instantie 6 is gegenereerd en via een veilige weg 7 toegevoerd aan de vercijfer- en ontcijfereenheden 2 en 4.

Uit referentie [3], meer in het bijzonder op pagina 831 in secties II.B. en II.C., zijn een vercijferschema op basis van een algebraïsche coderingsmethode en een daarmee corresponderend ontcijferschema bekend. Hiervan is uit referentie [5], meer in het bijzonder sectie 3, een equivalente formulering bekend. In de beschrijving van de uitvoeringsvoorbeelden wordt van deze equivalente formulering uitgegaan. Hoewel deze formulering ook meer algemeen geldt over eindige lichamen $\mathcal{F}_q$ met $q>2$, wordt voor de eenvoud van de verdere beschrijving, evenals daar, de formulering beperkt over het eindi-

ge lichaam $\mathcal{F}_2$, het binaire geval derhalve.

Gegeven zijn als geheime sleutel-elementen:

- een kxn-vercijfermatrix E van rang k met zijn rechter inverse E^{-R}, waarvoor geldt $EE^{-R} = I_k$, waarin I_k de kxk-eenheidsmatrix is;

- een (n-k)xn-matrix D van rang n-k, welke een met de matrix E corresponderende pariteits-controlematrix is, zodanig dat geldt $ED^T = O$, waarin D^T de getransponeerde van de matrix D en O de kx(n-k)-nulmatrix voorstellen;

- een zogeheten syndroom/foutvector-tabel $T = \{(\underline{s},\underline{z}) \mid \underline{s}=\underline{z}D^T, \underline{z}\epsilon W\}$, waarin W een verzameling is van foutvectoren $\underline{z}$ van lengte n, en welke tabel zodanig is samengesteld, dat met elke verschillende syndroomvector $\underline{s}$ van lengte n-k slechts één verschillende foutvector $\underline{z}$ correspondeert. In plaats van de syndroom/foutvector-tabel T kan zoals bekend (zie referentie [3], meer in het bijzonder sectie III. B. on page 833) ook een geheime functie t worden toegepast met onafhankelijke variabelen gekozen op basis van de unieke syndroom/foutvector-combinaties, welke anders voor de samenstelling van de tabel T zouden worden geselecteerd; dus $t(\underline{s})=\underline{z}$ voor alle $(\underline{s},\underline{z})\epsilon T$.

Uit referentie [6] is bekend, dat het Rao-Nam-schema een zekere kwetsbaarheid heeft onder bepaalde zogenoemde 'chosen-plaintext' aanvallen, en dat de mate van kwetsbaarheid daarvoor kan worden verminderd door aan de zendzijde de vercijferstap met de matrix E vooraf te laten gaan door een transformatie van de berichtvector met een geheime inverteerbare, niet-lineaire functie, welke bovendien afhankelijk kan worden gekozen van de geselecteerde foutvector. Symbolisch geschreven is dit een functie $f(\underline{m},\underline{z})$, welke de berichtvector $\underline{m}$ omzet in een getransformeerde berichtvector $\underline{m}'$ van dezelfde lengte.

Uitgaande van de genoemde sleutel-elementen wordt een bericht $\underline{m}$ van lengte k, berichtvector $\underline{m}$ genoemd, vercijferd in een cryptogram $\underline{y}$ van lengte n volgens het schema:

$$\underline{y} = f(\underline{m},\underline{z})E + \underline{z} = \underline{m}'E + \underline{z} = \underline{c} + \underline{z} \qquad \{2\}$$

waarbij $\underline{z}$ willekeurig wordt gekozen uit de verzameling W; en het cryptogram $\underline{y}$ wordt ontcijferd volgens het schema:

(i) bereken de syndroomvector: $\underline{y}D^T = \underline{z}D^T = \underline{s}$;

(ii) bepaal in de tabel T bij de berekende $\underline{s}$ de unieke foutvector $\underline{z}$;

(iii) bereken de getransformeerde berichtvector: $(\underline{y}+\underline{z})E^{-R} = \underline{c}E^{-R} = \underline{m}'$; N.B. in het binaire geval is coördinaatsgewijs 'aftrekken' gelijk aan coördinaatsgewijs 'optellen';

(iv) bereken de oorspronkelijke berichtvector: $f^{-1}(\underline{m}',\underline{z}) = \underline{m}$.

Van deze bekende vercijfer- en ontcijferschema's tonen FIG. 2(a) en FIG. 2(b) de respectievelijke blokschema's.

Aangezien in dergelijke op een fouten corrigerende code gebaseerde schema's steeds een aantal van k berichtsymbolen wordt omgezet in een codewoord van n symbolen, geschiedt de vercijfering en ontcijfering steeds bloksgewijs (eng.: blockstream)

Deze bekende schema's hebben echter de beperking, dat de lengte (k) van de te vercijferen berichtvector $\underline{m}$ kleiner is dan de lengte (n) van het cryptogram. Daardoor is de informatie-dichtheid $R=k/n$ tussen zender en ontvanger steeds kleiner dan 1, zijn gangbare methoden voor bloksgewijze vercijfering niet zonder meer toepasbaar, en is herhaald vercijferen niet mogelijk. Als dezelfde syndroom/foutvector-tabel $T(\underline{s},\underline{z})$ of een daarmee equivalente tabelfunctie t met functiewaarden $\{t(\underline{s})=\underline{z} \ (\underline{s},\underline{z})\epsilon T\}$ eveneens aan de zendzijde aanwezig is, dan kan het kiezen van een willekeurige foutvector $\underline{z}$ geschieden door bijvoorbeeld met een 'random'-generator een syn-

droomvector $\underline{s}$ te bepalen, waarbij vervolgens met de tabel of de functie de corresponderende foutvector $\underline{z}$ wordt bepaald. Nu is de lengte van de syndroomvector $\underline{s}$ juist n-k. Als nu n-k extra berichtsymbolen bij de vercijfering worden betrokken, dus in totaal n berichtsymbolen, waarvan k symbolen, althans in hoofdzaak, volgens het bekende vercijferschema worden behandeld en de resterende n-k symbolen voor de bepaling van de syndroomvector $\underline{s}$ worden gebruikt om zijn corresponderende foutvector $\underline{z}$ te vinden, wordt genoemde beperking opgeheven. Van op deze gedachte gebaseerde vercijfer- en ontcijferschema's zijn in FIG. 3(a) en FIG. 3(b) blokschema's weergegeven.

Gegeven zijn als vercijfer- en ontcijferelementen:

- een eerste inverteerbare niet-lineaire functie $g(\underline{x}) = \underline{x}'$ en een tweede inverteerbare niet-lineaire functie $h(y) = y'$, welke resp. vectoren $\underline{x}$ en $\underline{y}$ van lengte n omzetten in een getransformeerde vectoren $\underline{x}'$ en $\underline{y}'$ eveneens van lengte n;

- een eerste selectiefunctie $\sigma_A(\underline{x}) = \underline{x}_A$, welke een vector $\underline{x}$ van lengte n omzet naar een eerste deelvector $\underline{x}_A$ van lengte $k<n$ als volgt: als $\underline{x} = (x_1,x_2,---,x_n)$, dan is $\underline{x}_A = (x_{a1},x_{a2},---,x_{ak})$, waarin $A=\{a1, a2,----,ak\}$ een deelverzameling is van de verzameling van coördinaatindices $\{1,2,---,n\}$. Anders gezegd, σ_A vormt uit een aangeboden vector de eerste deelvector door volgens een gegeven selectiepatroon daaruit vectorcoördinaten te selecteren;

- een tweede selectiefunctie $\sigma_B(\underline{x}) = \underline{x}_B$, welke een vector $\underline{x}$ van lengte n omzet naar een tweede deelvector $\underline{x}_B$ van lengte n-k als volgt: als $\underline{x} = (x_1,x_2,---,x_n)$, dan is $\underline{x}_B = (x_{b1},x_{b2},---,x_{b(n-k)})$, waarin de verzameling $B=\{b1,b2,----,b(n-k)\}$ eveneens een deelverzameling is van de verzameling van coördinaatindices $\{1,2,---,n\}$, maar complementair met de verzameling

A. Derhalve doet σ_B in feite hetzelfde als σ_A, maar vormt de tweede deelvector uit de 'resterende' vectorcoördinaten van de aangeboden vector;

- een reconstructie-functie $\sigma_{AB}^{-1}(\underline{x}_A,\underline{x}_B) = \underline{x}$, welke uit twee aangeboden deelvectoren $\underline{x}_A$ en $\underline{x}_B$, respectievelijk van lengte k en n-k, de vector $\underline{x}$ reconstrueert, waarvoor geldt, dat $\sigma_A(\underline{x}) = \underline{x}_A$ en $\sigma_B(\underline{x}) = \underline{x}_B$; welke functie derhalve in feite de inverse vormt van de in combinatie toegepaste functies σ_A en σ_B;

- een kxn-vercijfermatrix E van rang k, met zijn rechter inverse E^{-R};

- een (n-k)xn-matrix D van rang n-k, welke een met de matrix E corresponderende pariteits-controlematrix is, zodanig dat geldt $ED^T = O$, i.e. de kx(n-k)-nulmatrix, waarbij D^T de getransponeerde van de matrix D voorstelt;

- een syndroom/foutvector-functie $t(\underline{s})=\underline{z}$, welke een aangeboden syndroomvector $\underline{s}$ van lengte n-k wordt omgezet in een foutvector $\underline{z}\epsilon W$, waarin $W \subset \mathcal{F}_2^n$ met de eigenschap: als $\underline{z}_1,\underline{z}_2 \epsilon W$, dan geldt $(\underline{z}_1+\underline{z}_2)D^T \neq 0$; daarbij is de functie t zodanig geconstrueerd, dat met elke verschillende syndroomvector $\underline{s}$ van lengte n-k een verschillende foutvector $\underline{z}$ correspondeert;

- een derde inverteerbare niet-lineaire functie $f(\underline{x}_A,\underline{z}) = \underline{m}$, welke een vector $\underline{x}_A$ van lengte k in afhankelijkheid van een gegeven vector $\underline{z}$ van lengte n omzet in een vector $\underline{m}$ van lengte k.

Het vercijferschema voor de vercijfering van een berichtvector $\underline{x}$ van lengte n in een cryptogram $\underline{y}$ van dezelfde lengte omvat de volgende stappen:

e(i) bereken de vector $\underline{x}' = g(\underline{x})$ van lengte n;

e(ii) bepaal de eerste deelvector $\underline{x}_A' = \sigma_A(\underline{x}')$ van lengte k, en de tweede deelvector $\underline{x}_B' = \sigma_B(\underline{x}')$ van lengte n-k;

e(iii) kies de tweede deelvector als syndroomvector: $\underline{s} = \underline{x}_B'$, en bepaal de foutvector $\underline{z} = t(\underline{s})$ van lengte n;

e(iv) bereken de vector $\underline{m} = f(\underline{x}_A', \underline{z})$ van lengte k;

e(v) bereken de vector $\underline{y}' = \underline{m}E + \underline{z}$ van lengte n;

e(vi) bereken de vector $\underline{y} = h(\underline{y}')$.

Van dit vercijferschema toont FIG. 3(a) een blokschema.

Een met dit vercijferschema corresponderend ontcijferschema voor het ontcijferen van het cryptogram $\underline{y}$ in de oorspronkelijke berichtvector $\underline{x}$ van lengte n omvat de volgende stappen:

d(i) bereken de vector $\underline{y}' = h^{-1}(\underline{y})$ van lengte n;

d(ii) bereken de syndroomvector $\underline{s} = \underline{y}'D^T$ van lengte n-k;

d(iii) bepaal de foutvector $\underline{z} = t(\underline{s})$ van lengte n;

d(iv) bereken de vector $\underline{m} = (\underline{y}' - \underline{z})E^{-R}$ van lengte k;

d(v) bereken de vector $\underline{x}_A' = f^{-1}(\underline{m}, \underline{z})$ van lengte k;

d(vi) bepaal de vector $\underline{x}' = \sigma_{AB}^{-1}(\underline{x}_A', \underline{x}_B')$ van lengte n, waarin vector $\underline{x}_B' = \underline{s}$, de in stap d(ii) berekende syndroomvector, wordt gekozen;

d(vii) bereken de vector $\underline{x} = g^{-1}(\underline{x}')$ van lengte n, de oorspronkelijke berichtvector.

Van dit ontcijferschema toont FIG. 3(b) een blokschema.

De inverteerbare niet-lineaire functies f, g en h kunnen zoals gebruikelijk afhankelijk gekozen worden van geheime sleutels ka, kb en kc respectievelijk, symbolisch aangeduid door f_{ka}, g_{kb}, en h_{kc}. In de meest algemene uitvoeringsvorm van deze vercijfer/ontcijferschema's vormen de sleutels ka, kb en kc, de selectieverzamelingen A en B, de matrix E (met impliciet de matrix D) en de syndroom/foutvector-functie $t(\underline{s})$ de geheime sleutel-elementen. De functies g en h worden bijvoorkeur als elkaars inverse, en de selec-

tieverzamelingen A en B vast gekozen.

Een syndroomvector $\underline{s}$ van lengte n-k kan als volgt worden geschreven:

$$\underline{s} = (s_1, s_2, \text{--}, s_{n-k}) = \Sigma_{1 \leq i \leq n-k}\, s_i \underline{u}^{(i)} \qquad \{3\},$$

voor i = 1,--,n-k, en waarin $\underline{u}^{(i)}$ de i-de de eenheidsvector is van de lengte n-k (i.e. de vector met op de i-de coördinaatpositie een 1 en op de overige n-k-1 coördinaatposities nullen). De n-k eenheidsvectoren $\underline{u}_{(i)}$ zijn in feite de eenheidssyndroomvectoren, welke de syndroomvectorruimte opspannen. Bij gegeven matrices E en D, waarvoor geldt, dat $ED^T = O$, is bij iedere eenheidssyndroomvector $\underline{u}^{(i)}$ van de door de matrix E gegenereerde code C een foutvector $\underline{z}^{(i)}$ te bepalen, waarvoor moet gelden:

$$\underline{z}^{(i)} D^T = \underline{u}^{(i)} \qquad \text{met } 1 \leq i \leq n-k \qquad \{4\},$$

waarbij $\underline{z}^{(i)} \neq \underline{z}^{(j)}$ voor $i \neq j$. De vergelijking {4} houdt voor elke $1 \leq i \leq n-k$ een stelsel in van n-k vergelijkingen met n onbekenden, zodat iedere foutvector $\underline{z}^{(i)}$ binnen de door de n-k vergelijkingen gestelde grenzen vrij kan worden gekozen. Combinatie van de vergelijkingen {3} en {4} levert:

$$\underline{s} = \Sigma_{1 \leq i \leq n-k}\, s_i \underline{u}^{(i)} = \Sigma_{1 \leq i \leq n-k}\, s_i \underline{z}^{(i)} D^T = \underline{z} D^T \qquad \{5\},$$

waaruit volgt, dat

$$\underline{z} = \Sigma_{1 \leq i \leq n-k}\, s_i \underline{z}^{(i)},$$

hetgeen te schrijven is als

$$\underline{z} = \underline{s} Z \qquad \{6\},$$

waarin Z een (n-k)xn-matrix is, waarvan de n-k rijen worden gevormd door de vectorcoördinaten van de n-k gekozen foutvectoren $\underline{z}^{(i)}$. De matrix Z is daarmee een eenvoudige realisatie van de tabelfunctie t (met $t(\underline{s}) = \underline{z}$).

De vercijfer- en ontcijferschema's volgens de uitvinding kunnen zowel in hardware als in software worden gerealiseerd met op zich bekende middelen. Hardware realisatie verdient de voorkeur bij hoge vercijfersnelheden,

terwijl een software realisatie een grotere mate van flexibiliteit toelaat.

Voorbeeld 1.

Het voorbeeld behelst een vercijfering van binaire blokken van lengte 32, waarbij ieder blok weer onder verdeeld in subblokken van lengte 8, dit is byte-gewijs, wordt verwerkt. Daartoe wordt een te vercijferen 32-bits vector $\underline{x}$ genoteerd als $\underline{x}=(\underline{x}_1,\underline{x}_2,\underline{x}_3,\underline{x}_4)$, dus opgedeeld in subvectoren van 8-bits, waarbij iedere subvector $\underline{x}_i=(x_{8i-7},x_{8i-6},\text{---},x_{8i})$ voor $i=1,\text{--},4$, een 8-bitsvector voorstelt. Deze notatie wordt hierna toegepast.

De vercijfermatrix E is een 8x32-matrix van volle rang (i.c. rang 8). De pariteitscontrole-matrix D is een 24x32-matrix, waarvoor geldt $ED^T = O$, de 8x24-nulmatrix. De tabelfunctie wordt gerealiseerd door een 24x32-matrix Z, welke op de hierboven aangegeven wijze is verkregen.

Voor de selectiefunctie σ_A is de verzameling $A=\{25,\text{--},32\}$, en voor de selectiefunctie σ_B is de verzameling $B=\{1,\text{--},24\}$.

De van sleutels ka, kb en kc afhankelijke inverteerbare niet-lineaire functies f_{ka}, g_{kb} en h_{kc} laten zich, zoals bekend en gebruikelijk, goed realiseren met behulp van substitutiefuncties. Een substitutiefunctie S, ook wel S-box genoemd, bestaat voor een 8-bits subblok verwerking uit een rij van alle 256 verschillende 8-bits elementen. Dus voor iedere 8-bits subvector $\underline{w}$ is er een unieke 8-bits subvector $\underline{v}$, zodat geldt $\underline{w}=S(\underline{v})$ en $\underline{v}=S^{-1}(\underline{w})$.

De sleutels ka, kb en kc zijn binaire bitreeksen en worden daarom ook genoteerd als vectoren $\underline{ka}$, $\underline{kb}$ en $\underline{kc}$, opgedeeld in 8-bits subvectoren. Zij zijn in dit voorbeeld als volgt gekozen: $\underline{ka}$ is een 8-bits vector, en $\underline{kb} = \underline{kc}$ zijn 32-bitsvectoren.

De functie f_{ka} zet met behulp van een reeds bepaalde foutvector $\underline{z}$ de deelvector $\underline{x}_A'$ om volgens:

$$f_{ka}(\underline{x}_A', \underline{z}) = (S(\underline{x}_{A1}' + \underline{z}_1 + \underline{ka}_1)) = (\underline{m}_1) = \underline{m},$$

terwijl voor de inverse geldt:

$$f_{ka}^{-1}(\underline{m}, \underline{z}) = (S^{-1}(\underline{m}_1) + \underline{z}_1 + \underline{ka}_1) = (\underline{x}_{A1}') = \underline{x}_A.$$

De functie g_{kb} zet de berichtvector $\underline{x}$ om volgens:

$$g_{kb}(\underline{x}) = (S(\underline{x}_1 + \underline{kb}_1), ---, S(\underline{x}_4 + \underline{kb}_4)) = (\underline{x}_1', ---, \underline{x}_4') = \underline{x}'.$$

De functie h_{kb} wordt gelijk gekozen aan de inverse van de functie g_{kb}, i.e. de functie h_{kb} zet de vector $\underline{y}'$ om in het cryptogram $\underline{y}$ volgens:

$$h_{kb}(\underline{y}') = (S^{-1}(\underline{y}_1') + \underline{kb}_1, ---, S^{-1}(\underline{y}_4') + \underline{kb}_4) = (\underline{y}_1, ---, \underline{y}_4) = \underline{y}.$$

De geheime sleutelelementen zijn de sleutelvectoren $\underline{ka}$ en $\underline{kb}$, en de matrices E (met impliciet matrix D) en Z.

Het vercijferschema volgens dit voorbeeld is weergegeven in FIG. 4(a).

De te vercijferen berichtvector $\underline{x}$ wordt in een eerste geheugenblok 41 geplaatst met vier byte-posities, een voor elke van vier subvectoren $\underline{x}_i$ van $\underline{x}$. Van uit het geheugenblok 41 worden de vier subvectoren ieder afzonderlijk aangeboden aan een eerste substitutie-blok 42, waarin de aangeboden subvectoren $\underline{x}_i$ worden omgezet in subvectoren $\underline{x}_i'$ volgens de functie g_{kb}. Om deze omzetoperatie byte-gewijs uit te voeren bestaat het substitutie-blok 42 uit vier S-boxen SG1 t/m SG4. Deze S-boxen zijn overeenkomstig de gekozen functie g_{kb} onderling gelijk gekozen, maar wel wordt er bij een aangeboden subvector $\underline{x}_i$ eerst een overeenkomstige subvector $\underline{kb}_i$ van de toegevoerde sleutel $\underline{kb}$ opgeteld voordat er wordt gesubstitueerd. Dit is in de figuur aangegeven door de pijl KB. De substitutieresultaten worden geplaatst in een tweede geheugenblok 43 eveneens met vier byte-posities voor de subvectoren $\underline{x}_i'$. Overeenkomstig het door de gekozen verzamelingen A en B gedefinieerde selectieschema dienen de eerste drie subvectoren van de vector $\underline{x}'$ als syndroomvector $\underline{s}$ en worden daartoe geplaatst in een derde geheugenblok 44 met drie byte-posities, terwijl de vierde subvector $\underline{x}_4'$

wordt geplaatst in een vierde geheugenblok 45 met één byte-positie om de eerste deelvector $\underline{x}_A'$ te vormen. De syndroomvector $\underline{s}$ wordt in een matrixblok 46 in zijn geheel onderworpen aan een matrixvermenigvuldiging met de matrix Z, hetgeen resulteert in een foutvector $\underline{z}$ van lengte 32, waarvan de subvectoren $\underline{z}_i$ worden geplaatst in de vier byte-posities van een vijfde geheugenblok 47. In een opteller 48 worden vervolgens de deelvector in het vierde geheugenblok 45 en de deelvector in de eerste byte-positie van het vijfde geheugenblok 47 (binair en coördinaatsgewijs) opgeteld en onderworpen. Het resultaat van de optelling wordt aangeboden aan een tweede substitutie-blok 49 en omgezet in een subvector $\underline{m}_1$ volgens de functie f_{ka}. Het substitutie-blok 49 bestaat uit één S-box SF1. Deze S-box is overeenkomstig de gekozen functie f_{ka} gelijk gekozen aan de S-box uit het eerste substitutieblok 42, maar ook hier wordt er bij de door de opteller 48 aangeboden subvector eerst de enige subvector $\underline{ka}_1$ van de toegevoerde sleutel $\underline{ka}$ opgeteld voordat er wordt gesubstitueerd. Dit is in de figuur aangegeven door de pijl KA. Het substitutieresultaat, de subvector $\underline{m}_1$, wordt geplaatst in een zesde geheugenblok 50 met één byte-positie. De subvector $\underline{m}_1$ wordt in een tweede matrixblok 51 in zijn geheel onderworpen aan een matrixvermenigvuldiging met de matrix Ė, hetgeen resulteert in een code vector $\underline{c}$ van lengte 32, waarvan de subvectoren $\underline{c}_i$ worden geplaatst in de vier byte-posities van een zevende geheugenblok 52. In optellers 53, 54, 55 en 56 worden vervolgens de deelvectoren $\underline{c}_i$ van de codevector $\underline{c}$ uit het zevende geheugenblok 52 opgeteld bij de overeenkomstige deelvectoren $\underline{z}_i$ van de foutvector $\underline{z}$ uit het vijfde geheugenblok 47. Het resultaat van de optelling, de vector $\underline{y}'$ met de deelvectoren $\underline{y}_i'$, wordt geplaatst in een achtste geheugenblok 57 met vier byte-posities. Van uit het geheugenblok 57 worden de vier subvectoren $\underline{y}_i'$ ieder afzonderlijk aangeboden aan een derde substitutie-blok

58, waarin de aangeboden subvectoren $\underline{y}_i'$ worden omgezet in subvectoren $\underline{y}_i$ volgens de functie g_{kb}^{-1}. Voor een byte-gewijze uitvoering van deze omzetting bestaat het substitutie-blok 58 uit vier S-boxen $SG1^{-1}$ t/m $SG4^{-1}$. Deze S-boxen zijn overeenkomstig de gekozen functie g_{kb}^{-1} onderling gelijk gekozen en vormen de inverse van de in het eerste substitutieblok 42 toegepaste S-box. Bovendien wordt er bij het substitutieresultaat van een aangeboden subvector $\underline{y}_i'$ een overeenkomstige subvector $\underline{kb}_i$ van de toegevoerde sleutel $\underline{kb}$ opgeteld. Dit is in de figuur aangegeven door de pijl KB. De substitutieresultaten worden geplaatst in een negende geheugenblok 59 eveneens met vier byte-posities. Zij vormen de deelvectoren $\underline{y}_i$ van het cryptogram $\underline{y}$.

Het corresponderende ontcijferschema is weergegeven in FIG. 4(b). De aanduidingen hierin zijn volledig afgestemd op die in FIG. 4(a), zodat wordt volstaan met een opsomming van de genummerde onderdelen. In het schema zijn opgenomen:

- zes geheugenblokken 61, 63, 67, 72, 77 en 79 met elk vier byte-posities voor de subvectoren respectievelijk van de vectoren $\underline{y}$, $\underline{y}'$, $\underline{z}$, $\underline{c}$, $\underline{x}'$ en $\underline{x}$;
- een geheugenblok 65 met drie byte-posities voor de syndroomvector $\underline{s}$;
- een geheugenblok 74 met één byte-positie voor de vector $\underline{m}_1$;
- twee substitutieblokken 62 en 78, respectievelijk gelijk aan de substitutieblokken 42 en 58 in het vercijferschema van FIG. 4(a), voor het omzetten van de vectoren $\underline{y}$ in $\underline{y}'$ en $\underline{x}'$ in $\underline{x}$ respectievelijk;
- een substitutieblok 75 welke de inverse is van het substitutieblok 49 in het vercijferschema van FIG. 4(a), voor het omzetten van de subvector $\underline{m}_1$;

- vier optellers 68 t/m 71 voor het byte-gewijze optellen van de vector $\underline{y}'$ en de foutvector $\underline{z}$;
- een opteller 76 voor het optellen van de eerste subvector $\underline{z}_1$ van de foutvector $\underline{z}$ en de in het substitutieblok 75 omgezette subvector $\underline{m}_1$;
- drie matrixblokken 64, 66 en 73 voor het uitvoeren van matrixvermenigvuldigingen respectievelijk met de matrices D^T, Z en E^{-R} op de vectoren $\underline{y}'$, $\underline{s}$ en $\underline{c}$ volgens:

$\underline{y}'D^T = \underline{s}$, $\underline{s}Z = \underline{z}$, en $\underline{c}E^{-R} = \underline{m}_1$.

De specifieke keuze van de functie h_{kc} als de inverse van de functie g_{kb} heeft voordeel bij herhaald vercijferen, waarbij een van tevoren bepaald aantal malen de inhoud van het geheugenblok 57 weer wordt geplaatst in geheugenblok 43, voordat deze aan het substitutieblok 58 wordt aangeboden voor het verkrijgen van het eigenlijke, te verzenden cryptogram $\underline{y}$. Aan de ontcijferzijde moet vanzelfsprekend het zelfde aantal malen worden ontcijferd door de inhoud van geheugenblok 77 steeds weer terug te voeren naar het geheugenblok 63. Dit aantal malen is bijvoorbeeld volgens een van tevoren vastgestelde procedure af te leiden uit een van de sleutel-elementen.

Gegeven de generatormatrix G van een (n,k) lineaire code C in kanonieke vorm: $G = [I \mid Q]$, waarin I de kxk-eenheidsmatrix is en Q een kx(n-k)-matrix is. Voor de corresponderende pariteitscontrole-matrix H geldt dan: $H = [-Q^T \mid I]$, waaruit direct te zien is, dat: $GH^T = O_{k,n-k}$, de kx(n-k)-nulmatrix. Ook van de matrix Z, waarmee bij een gegeven syndroomvector een unieke foutvector uit een beperkte verzameling van foutvectoren kan worden berekend, is een soort kanonieke vorm te definiëren door:

$Z_0 = [O_{n-k,k} \mid I_{n-k}]$, waarin $O_{n-k,k}$ de (n-k)xk-nulmatrix is en I_{n-k} de (n-k)x(n-k)-eenheidsmatrix is, en waaruit onmiddellijk blijkt, dat:

$Z_0H^T = I_{n-k}$.

Uitgaande van een gegeven generatormatrix G in kanonieke vorm kan een willekeurige vercijfermatrix worden geconstrueerd voor de (n,k) lineaire code C door: E = SGP, waarin S een inverteerbare kxk-matrix en P een nxn-permutatiematrix zijn. Om lange sleutel-elementen zoals S en P tevermijden is het bekend om deze te gegeneren op basis van sleutels van beperkt lengte, zogeheten 'short seeds' (zie referentie [3], meer in het bijzonder de 'note' in sectie II. C., p. 831). Ook een S-box kan worden gegenereerd op basis van een dergelijke beperkte sleutel.

Voorbeeld 2

Toegepast op de hierboven beschreven uitvoeringsvorm van voorbeeld 1 betekent dit dat bij gegeven sleutelelementen ka, kb, kd, ke, kf en kg, en bij een gegeven generatormatrix G van de (32,8) lineaire code C eerst in een aantal voorbereidende stappen de matrices E, D en Z als volgt worden bepaald:

(1) bepaal op basis van het sleutelelement kd een eerste inverteerbare 8x8-matrix S_{kd} en op basis van het sleutelelement ke een tweede inverteerbare 8x8-matrix S_{ke};

(2) bepaal op basis van het sleutelelement kf een 32x32-permutatiematrix P_{kf};

(3) bereken de vercijfermatrix E volgens: $E = S_{kd}GP_{kf}$;

(4) bereken de pariteitscontrole-matrix D volgens: $D = HP_{kf}$;

(5) bereken de matrix Z volgens: $Z = Z_0P_{kf} + S_{ke}E$.

(6) genereer op basis van het sleutelelement kg een 8-bits S-box.

Ook hier geldt weer: $ED^T = O$ en $ZD^T = Z_0H^T$.

Uitdrukkelijk zij nog vermeld, dat de vercijfermatrix E een willekeurig geko-

zen lineaire (n,k) code C kan representeren, als maar steeds geldt, dat de matrix E er een is van volle rang. De minimum afstand tussen de codewoorden doet niet terzake. Ook als uitgegaan wordt van een kanonieke vorm van de generatormatrix G voor een lineaire code, kan de matrix Q willekeurig worden gekozen, bijvoorbeeld op basis van een extra sleutelelement kh.

F. Conclusies

1. Een werkwijze voor het vercijferen en ontcijferen van berichten in een cryptosysteem voor beveiliging van communicatieverbindingen, welke werkwijze omvat een eerste deelwerkwijze voor het vercijferen van berichtdata, waarbij de berichtdata bloksgewijze worden omgezet in cryptogrammen geschikt voor verzending over een te beveiligen communicatieverbinding, en een tweede deelwerkwijze voor het ontcijferen van ontvangen cryptogrammen, waarbij de berichtdata worden herkregen, welke eerste deelwerkwijze voor het vercijferen de volgende stappen omvat:

- het omzetten van te verzenden berichtdata in blokken van n berichtsymbolen, aldus berichtvectoren vormend met n vectorcoördinaten,

- het opsplitsen van elke berichtvector in een eerste deelvector van lengte k en een tweede deelvector van lengte n-k, waarbij uit de n vectorcoördinaten van de berichtvector voor de vectorcoördinaten van de eerste deelvector k vectorcoördinaten en voor de vectorcoördinaten van de tweede deelvector de resterende n-k vectorcoördinaten worden geselecteerd volgens een van tevoren vastgelegd selectieschema,

- het coderen van de eerste deelvector met behulp van een van tevoren gekozen kxn-matrix (E) van volle rang, welke een generatormatrix representeert voor een fouten corrigerende code (C), daarbij een codevector van lengte n vormend,

- het met behulp van de tweede deelvector uniek selecteren van een foutvector uit een verzameling van foutvectoren van lengte n, welke verzameling van tevoren met behulp van een (n-k)xn-matrix (D) is samengesteld uit foutvectoren, waarbij de matrix (D) een pariteitscontrole-matrix representeert voor de fouten corrigerende code (C) en de foutvectoren ieder een verschillend foutpatroon representeren, dat corrigeerbaar is met behulp van

de code (C),

- het door optellen van de geselecteerde foutvector en de codevector bepalen van een somvector van lengte n voor het verkrijgen van een cryptogram,

en welke tweede deelwerkwijze van ontcijferen de volgende stappen omvat:

- het reconstrueren van de tweede deelvector uit het cryptogram door matrixvermenigvuldiging met de getransponeerde van de pariteitscontrolematrix (D),

- het met behulp van de tweede deelvector uniek selecteren van de foutvector uit de verzameling van foutvectoren,

- het reconstrueren van de codevector door binaire optelling van het cryptogram en de geselecteerde foutvector,

- het reconstrueren van de eerste deelvector door decoderen van de codevector met behulp van een nxk-matrix, welke de rechts-inverse matrix is van de generatormatrix (E),

- het reconstrueren van de berichtvector door samenvoegen van de gedecodeerde eerste en tweede deelvectoren overeenkomstig een schema dat de inverse is van het genoemde selectieschema.

2. Werkwijze volgens conclusie 1, waarin in de eerste deelwerkwijze de berichtvector voorafgaande aan opsplitsing met behulp van een eerste inverteerbare niet-lineaire transformatie wordt omgezet in een getransformeerde berichtvector van dezelfde lengte, en in de tweede deelwerkwijze het reconstrueren van de berichtvector geschiedt door het samenvoegen van de gecodeerde eerste en tweede deelvectoren, waarbij de getransformeerde berichtvector wordt verkregen, gevolgd door een omzetting met behulp van een transformatie, welke de inverse is van genoemde eerste

inverteerbare niet-lineaire transformatie.

3. Werkwijze volgens conclusie 1 of 2, waarin in de eerste deelwerkwijze voor het verkrijgen van het cryptogram de somvector met behulp van een tweede inverteerbare niet-lineaire transformatie wordt omgezet in een getransformeerde somvector van dezelfde lengte, en in de tweede deelwerkwijze het cryptogram voorafgaande aan de reconstructie van de tweede deelvector wordt omgezet in de somvector met behulp van een transformatie, welke de inverse is van de tweede inverteerbare niet-lineaire transformatie.

4. Werkwijze volgens een der conclusies 1,--,3, waarin in de eerste deelwerkwijze voorafgaande aan de stap van het coderen de eerste deelvector met behulp van een derde inverteerbare niet-lineaire transformatie, welke afhankelijk is van de met behulp van de tweede deelvector geselecteerde foutvector, wordt omgezet in een getransformeerde eerste deelvector, en in de tweede deelwerkwijze de stap van de reconstructie van de eerste deelvector bestaat uit het decoderen, waarbij de getransformeerde eerste deelvector wordt verkregen, gevolgd door een omzetting met behulp van een transformatie, welke de inverse is van genoemde derde inverteerbare niet-lineaire transformatie.

5. Werkwijze volgens een der conclusies 1,---,4, waarin de kxn-matrix E van tevoren is geconstrueerd door matrixvermenigvuldiging van een niet-singuliere kxk-matrix (S), een kxn-generatormatrix (G) voor een fouten corrigerende code (C) en een nxn-permutatiematrix (P), en de stap van het reconstrueren van de tweede deelvector wordt uitgevoerd door matrixvermenig-

vuldiging met de getransponeerde van de pariteitscontrole-matrix (D), welke van tevoren is geconstrueerd door matrixvermenigvuldiging van een (n-k)xn-matrix (H), welke een met de generatormatrix (G) corresponderende pariteitscontrole-matrix is voor de fouten corrigerende code (C), en de inverse (nxn)-permutatiematrix (P^{-1}).

6. Werkwijze volgens conclusie 1, waarin de selectie van de foutvector geschiedt door matrixvermenigvuldiging met een (n-k)xn-matrix Z, waarvoor geldt dat matrixvermenigvuldiging met de getransponeerde van de pariteitscontrole-matrix (D) de (n-k)-eenheidsmatrix oplevert (i.e. $ZD^T = I_{n-k}$).

7. Werkwijze volgens conclusie 6, waarin de matrices E, D en Z van tevoren zijn gegenereerd op basis van een generatormatrix G voor de fouten corrigerende code (C) in kanonieke vorm en een aantal geheime sleutelelementen van beperkte lengte.

8. Werkwijze volgens een der conclusies 3, 4 of 5, waarin de inverteerbare niet-lineaire transformaties geschieden in afhankelijkheid van een geheime sleutel.

9. Deelwerkwijze voor het bloksgewijze vercijferen van berichtdata geschikt voor toepassing in de werkwijze volgens een der conclusies 1 t/m 8.

10. Deelwerkwijze voor het ontcijferen van cryptogrammen geschikt voor toepassing in de werkwijze volgens een der conclusies 1 t/m 8.

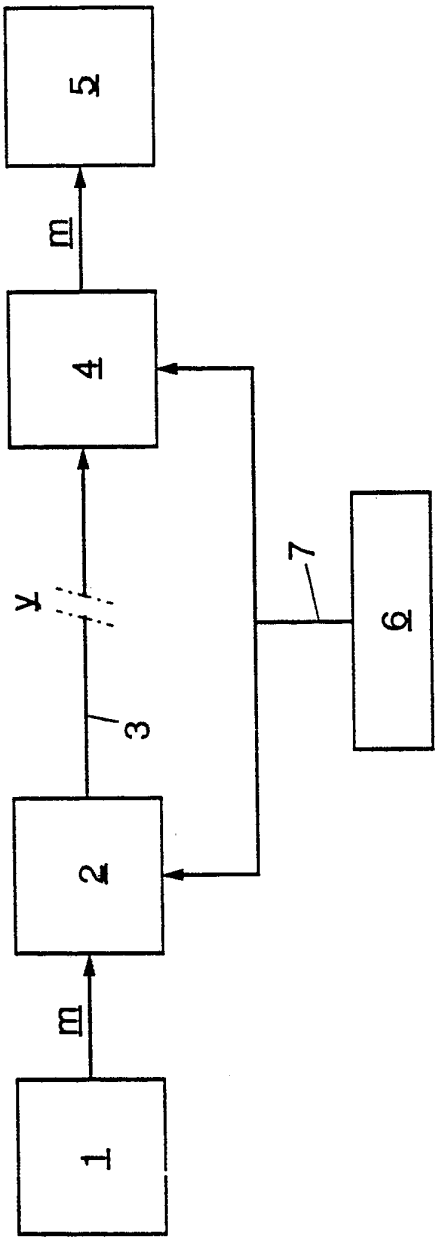


FIG. 1

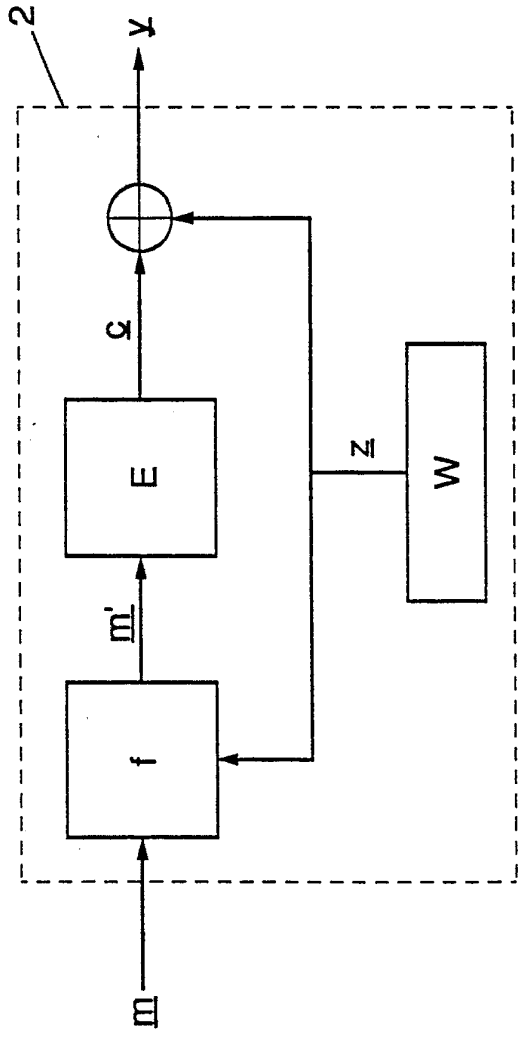


FIG. 2(a)

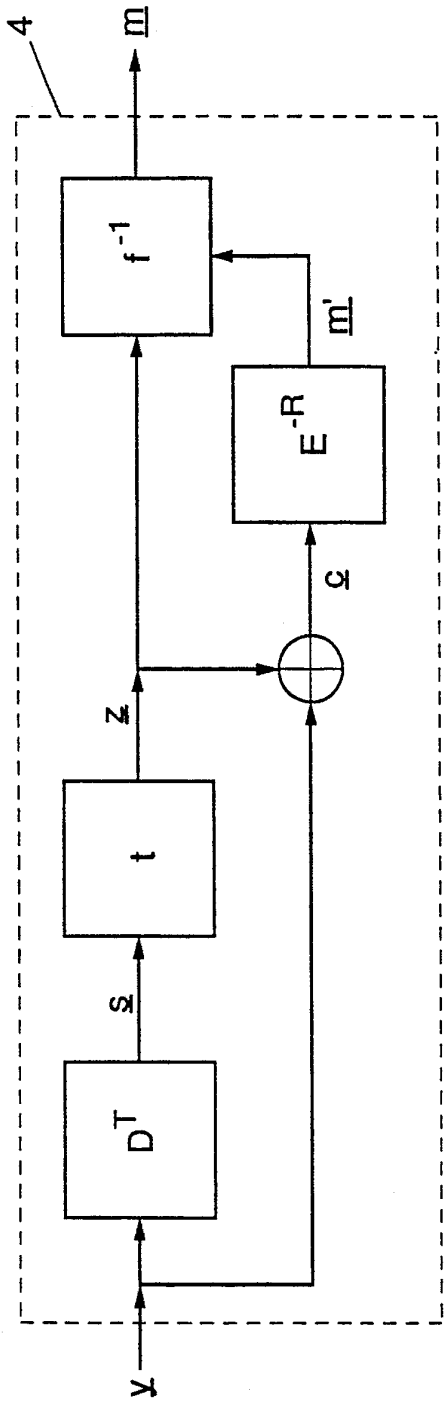


FIG. 2(b)

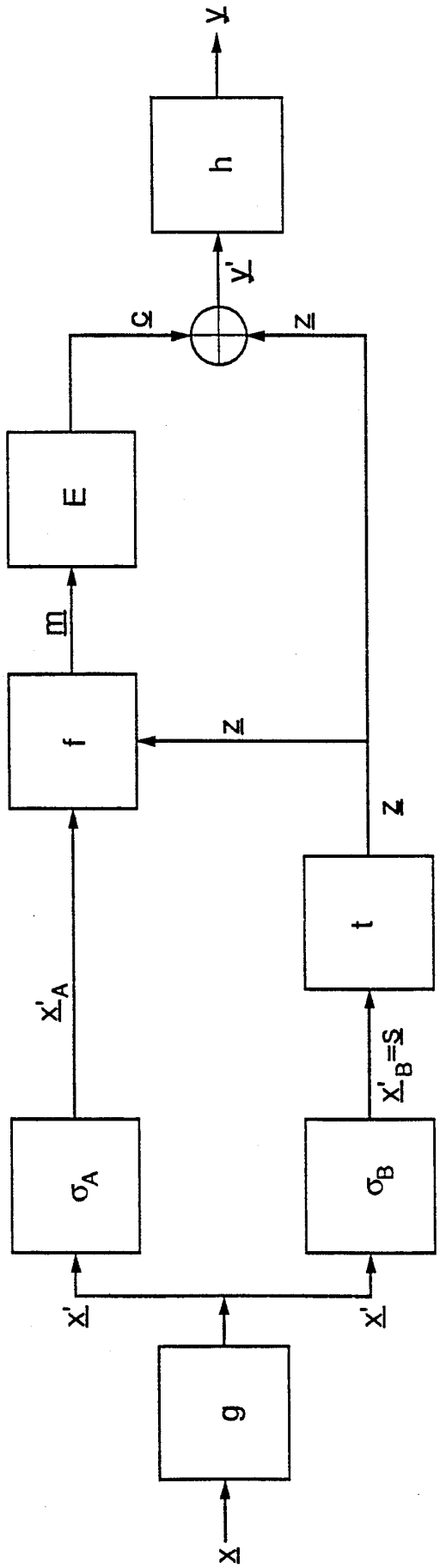


FIG. 3(a)

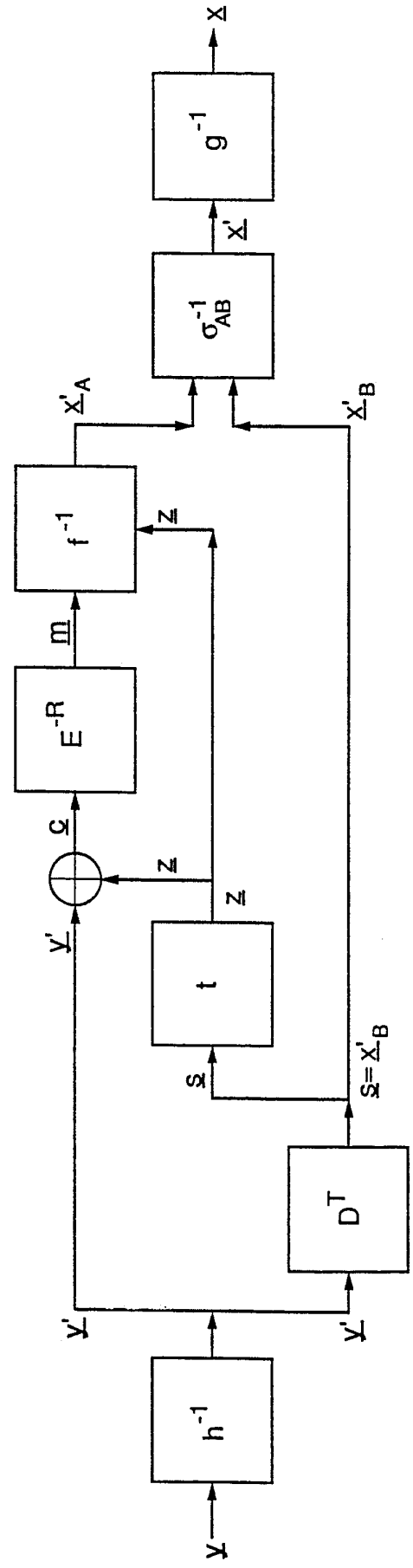


FIG. 3(b)

9202284

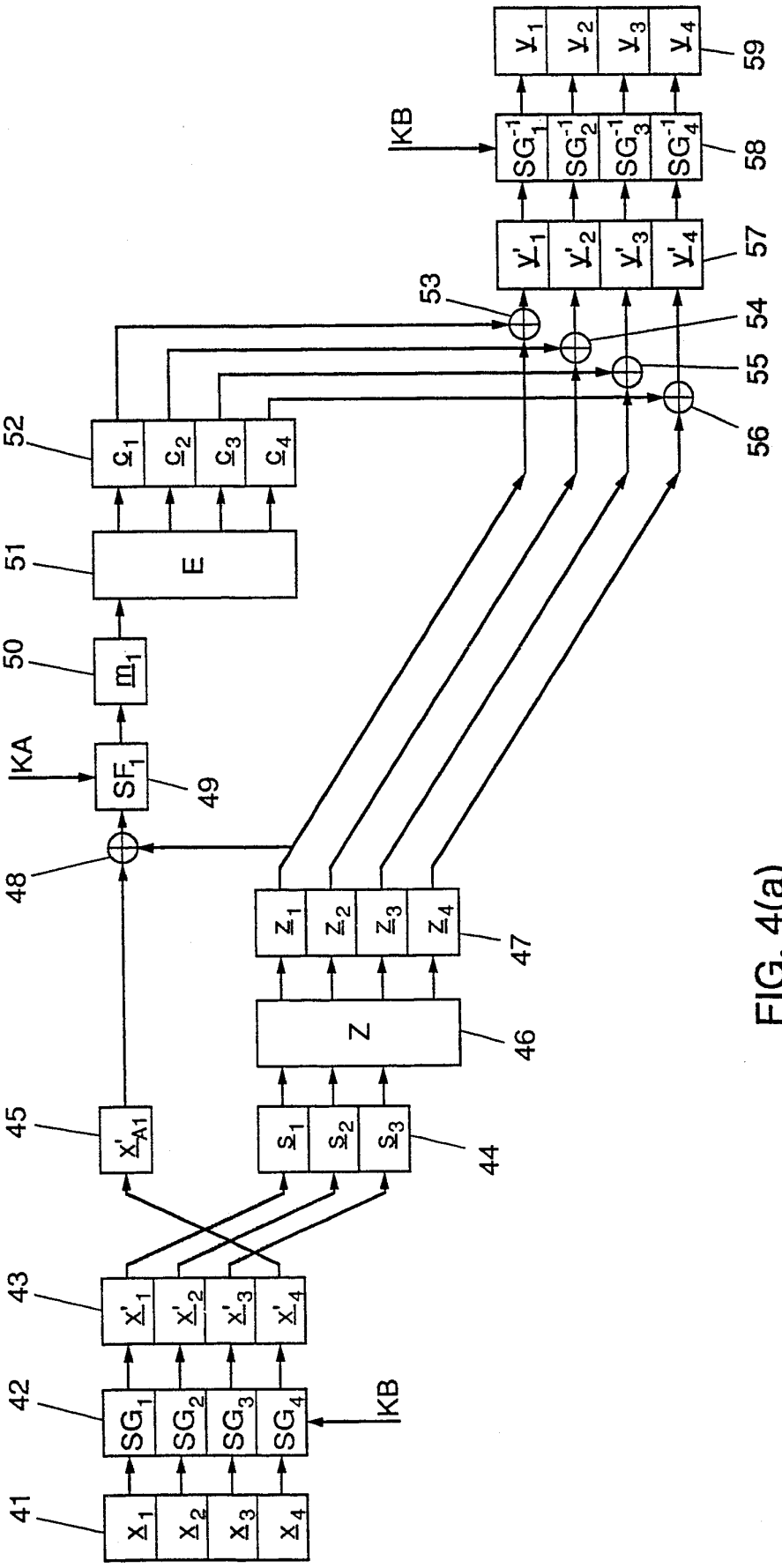


FIG. 4(a)

9202284

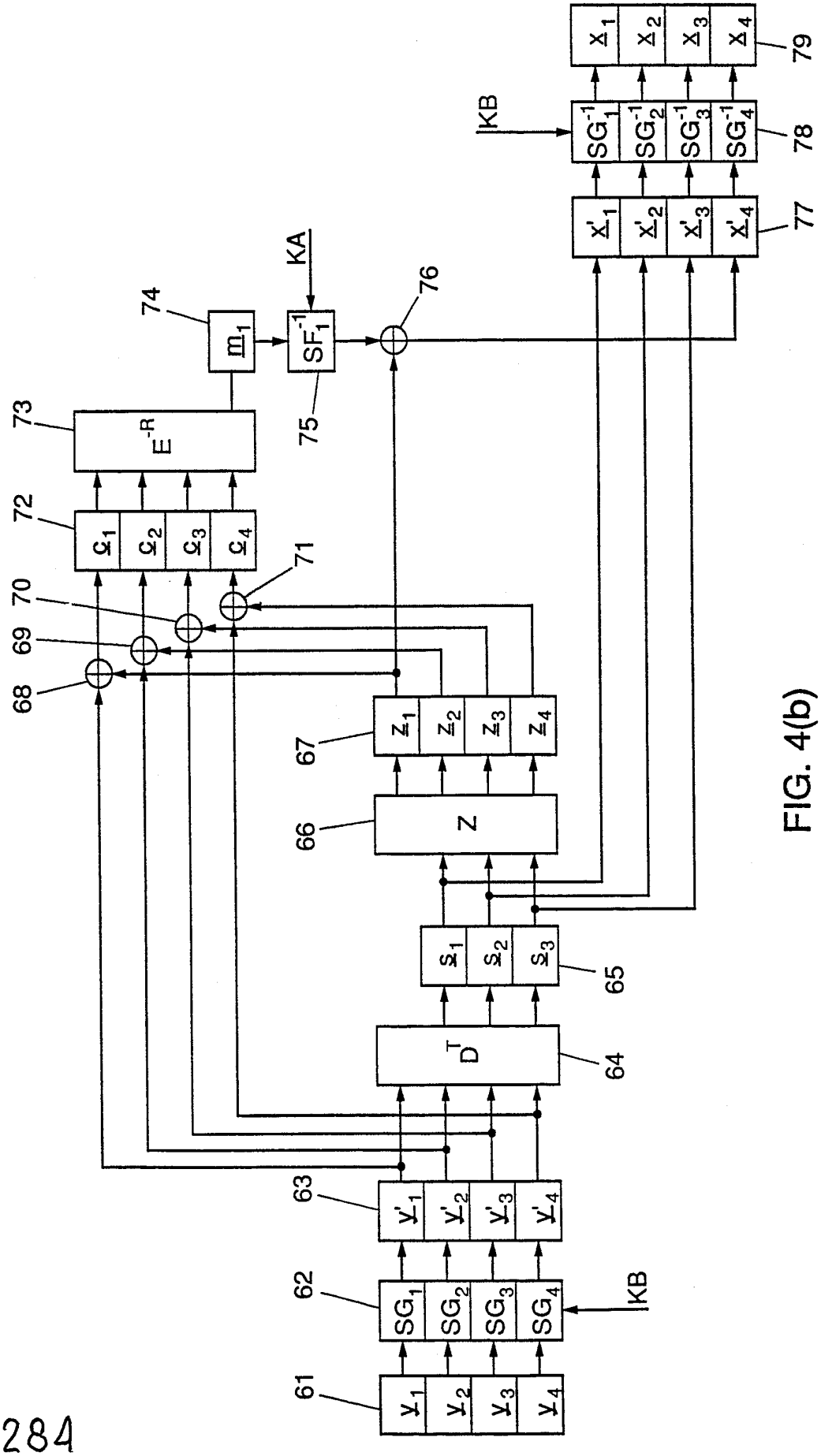


FIG. 4(b)