(12) **PATENT**

(19) NO (11) **321409** (13) **B1**

NORGE (51) Int Cl.
H04L 9/30 (2006.01)

Patentstyret

(21)	Søknadsnr	19963141	(86)	Int.inng.dag og søknadsnr	
(22)	Inng.dag	1996.07.26	(85)	Videreføringsdag	
(24)	Løpedag	1996.07.26	(30)	Prioritet	1995.07.27, FR, 9509179
(41)	Alm.tilgj	1997.01.28			
(45)	Meddelt	2006.05.08			

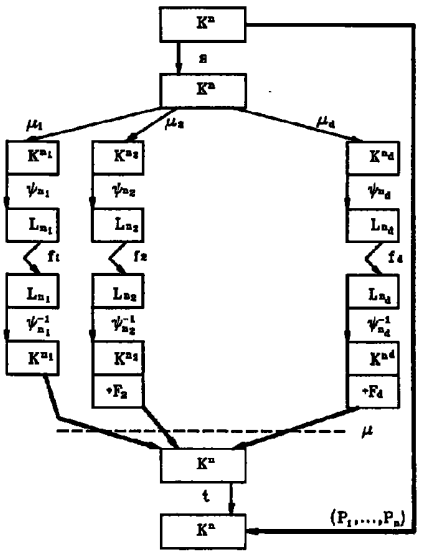
(73)	Innehaver	CP8 Technologies , 36-38, Rue de la princesse, 78430 LOUVECIENNES, FR
(72)	Oppfinner	Jacques Patarin, Viroflay, FR
(74)	Fullmektig	Bryn Aarflot AS , Postboks 449 Sentrum, 0104 OSLO, NO

(54) Benevnelse **Fremgangsmåte for kryptografisk kommunikasjon**

(56) Anførte publikasjoner Ingen

(57) Sammendrag

Et hittil ukjent asymmetrisk kryptografisk skjema som kan anvendes for koding, signering og autentifikasjon. Skjemaet er basert på lavere grads offentlige polynomlikninger med verdier i en endelig ring (K).
Mekanismen er ikke nødvendigvis bijektiv. Den hemmelige nøkkelen gjør det mulig å skjule polynomlikninger med verdier i utvidelser av ringen (K). Løsningen av disse likningene gjør det mulig, hvis en har den hemmelige nøkkelen, å utføre operasjoner som ikke er mulig å utføre med den offentlige nøkkelen alene.



Oppfinnelsen angår en asymmetrisk kryptografisk kommunikasjonsfremgangsmåte for å prosessere meldinger og beskytte kommunikasjon mellom deltakerne. Den kan anvendes til å kode meldinger asymmetrisk eller signere dem, også dette asymmetrisk. Den kan også anvendes til asymmetrisk autentifikasjon.

En velkjent første løsning ble utviklet i 1977. Denne løsningen var gjenstand for patent 4,405,829 i USA, innlevert av oppfinnerne Rivest, Shamir og Adleman 14. desember, 1977. Denne løsningen, ofte kalt RSA etter navnene til oppfinnerne, anvender to typer nøkler. Den første nøkkelen (Kp) tillater koding av meldinger, og den andre (Ks) tillater dekoding av disse. Denne prosessen, som er verdenskjent, danner grunnlaget for asymmetrisk kryptografi, og kalles dette fordi forskjellige nøkler anvendes for koding og dekoding. I det samme nettverket innehar hvert medlem (i) et slikt par av nøkler. Den første (Kp_i) er offentlig og kan derfor være kjent av alle; den andre (Ks_i) er hemmelig og må aldri kommuniseres.

Kodet kommunikasjon mellom to kommunikatorer (1) og (2) i det samme nettverket utføres på følgende måte: (1) og (2) utveksler først de offentlige nøklene (Kp_1) og (Kp_2); når (1) ønsker å sende en melding (M) til (2), koder han så meldingen med nøkkelen (Kp_2), og straks (2) mottar denne meldingen kan den dekodes med hjelp av den hemmelige nøkkelen (Ks_2) som (2) innehar:

Koding: $M' = RSA(M, Kp_2)$

Dekoding $M = RSA(M', Ks_2)$

Når (2) ønsker å sende en melding til (1), koder han den med den offentlige nøkkelen som tilhører (1): (Kp_1) som igjen dekoder den med sin egen hemmelige nøkkel (Ks_1).

RSA-prosessen kan også anvendes for signatur: meldingen kodes da med avsenderens individuelle hemmelige nøkkel, og den kodede meldingen, kalt signaturen, overføres så sammen med meldingen i ukodet form; mottakeren av meldingen ber da om tilgang til avsenderens offentlige nøkkel og bruker den til å dekode signaturen; hvis den dekodede teksten samsvarer med den ukodede meldingen er signaturen autentisk.

Denne kryptografiske kommunikasjonsfremgangsmåten har mange ulemper. Tallene som skal manipuleres er store (typisk 512 bits i dag), noe som krever at det utføres mange regneoperasjoner og leder til signaturer som er veldig lange. Dessuten vil sikkerheten til RSA bringes i fare dersom det oppnås nye gjennombrudd i faktorisering.

Andre asymmetriske kryptografiske kommunikasjonsfremgangsmåter har vært foreslått for å utføre funksjonene for asymmetrisk koding eller signering av meldinger, for eksempel de som anvender "ryggsekk"-baserte algoritmer eller MATSUMOTO-IMAI

algoritmen. Disse to eksemplene har vist seg å ha en grad av sikkerhet som er helt utilstrekkelig.

Foreliggende oppfinnelse foreslår en løsning som ikke har ulempene til disse to eksemplene, men som beholder et visst antall av fordelene deres. Foreliggende oppfinnelse anvender en ny algoritme kalt en " Hidden Fields Algorithm " eller HFE (Hidden Fields Equation) som, i likhet med RSA, kan anvendes til funksjonene autentifisering, koding og signering. Dessuten, mens RSA hovedsakelig er basert på problemet med å faktorisere store tall, er HFE-algoritmen basert på et helt annet problem: å løse flervariable, laveregrads-likninger (typisk av 2. eller 3. grad). Det må nevnes at MATSUMOTO-IMAI algoritmen også har denne egenskapen, men den har som allerede indikert, en utilstrekkelig sikkerhetsgrad, noe som gjør den uegnet for anvendelse i en kryptografisk kommunikasjonsfremgangsmåte. Forfatteren av foreliggende oppfinnelse er også personen som oppdaget at MATSUMOTO-IMAI algoritmen ikke var kryptografisk fullkommen.

Blant de nye elementene som kan bidra til sikkerhet for HFE-algoritmen, er det faktum at denne algoritmen ikke nødvendigvis er bijektiv, og det faktum at den kan anvende veldig generelle polynom-likninger.

En annen fordel som oppnås ved oppfinnelsen er HFE-algoritmens kapabilitet til å beregne ultrakorte signaturer (mindre enn 200 bits), mens de korteste asymmetriske signaturene kjent i dag er av orden 220 eller 320 bits (oppnådd ved hjelp av SCHNORR-algoritmen eller DSS-algoritmen, som kun kan anvendes til signering eller autentifisering, ikke til koding/dekoding). Det er fordelaktig å bruke minst 512 bits ved anvendelse av RSA.

Definisjoner:

1. En "utvidelse" med grad N av en ring A er en hvilken som helst isomorf algebraisk struktur med A[X]/g(X), der A[X] er ringen av polynomer med en indeterminant på A, og g(X) er et polynom av n-te grad.

Et spesielt fordelaktig tilfelle er det der A er et endelig felt F_q og g er et irreduktibelt polynom av n-te grad på F_q. I dette tilfellet er A[X]/g(X) et endelig isomorft felt med F_qn.

2. En "basis" for en utvidelse L_n av A med grad n er en familie med n elementer på L_n $(e_1, e_2, \ldots, e_n)$, slik at hvert element e i L_n kan uttrykkes entydig på formen

$$e = \sum_{i=1}^{n} \alpha_i e_i \quad \text{med } \alpha_i \in A.$$

Foreliggende oppfinnelse angår således en kryptografisk kommunikasjons-fremgangsmåte som transformerer en verdi (X), representert av (n) elementer i en endelig ring (K), til en billedverdi (Y) representert ved (n') elementer i ringen (K), som kjennetegnes ved at

a) hvert element (n') av billedverdien (Y) er i form av en offentlig polynomlikning av lav grad (D) større enn eller lik 2 sammensatt av elementene (n) fra verdien (X);

b) billedverdien (Y) også kan fås fra verdien (X) ved hjelp av en transformasjon omfattende følgende trinn, der minst noen av dem krever kjennskap til en kryptografisk hemmelighet:

b1) det anvendes på verdien (X) en første hemmelig polynom- transformasjon (s) av grad 1 sammensatt av de (n) elementene til verdien (X) for å frembringe et første bilde (I1) med (n) elementer;

b2) de (n) elementene i det første bildet (I1) tenkes å representere en variabel eller et lite antall (k) variabler (x, x', x", ..., x^k) tilhørende en utvidelse (L_w) med graden W av ringen (K) med W*k = n, ved å anvende på det første bildet (I1) en transformasjon definert som følger:

f: $L_w^k \rightarrow L_w^k$

$(x, x', x'', ..., x^k) \_\rightarrow (y, y', y'', ..., y^k)$

hvor $(y, y', y'', ..., y^k)$ er bildet av $(x, x', x'', ..., x^k)$ fra transformasjonen f, der f verifiserer følgende to egenskaper:

-b2.1) i en basis (B) av ringutvidelsen (L_w) er hver komponent av bildet $(y, y', y'', ..., y^k)$ uttrykt i form av et polynom sammensatt av komponentene til $(x, x', x'', ..., x^k)$ i denne basisen, hvilket polynom har total grad mindre enn eller lik graden (D) på den offentlige polynomlikningen;

-b2.2) uttrykt ved ringutvidelsen (L_w) er transformasjonen (f) slik at det er mulig å beregne forleddene til (f) når de eksisterer, kanskje bortsett fra spesielle biter, der antallet slike er neglisjerbart relativt til det totale antallet biter;

b3) det første bildet (I1) som er således transformert, utgjør et andre bilde (I2);

b4) det anvendes på det andre bildet (I2) en andre hemmelig polynomtransformasjon (t) av grad 1 sammensatt av elementer i det andre bildet (I2) for å frembringe et tredje bilde (I3) som har et bestemt antall elementer; og

b5) det velges ut (n') elementer fra settet av elementer i det tredje bildet (I3) for å danne den nevnte billedverdien (Y).

Oppfinnelsen vedrører også en kryptografisk kommunikasjonsfremgangsmåte som transformerer en verdi (X), representert av (n) elementer i en endelig ring (K), til en billedverdi (Y) representert ved (n') elementer i ringen (K). Fremgangsmåten kjennetegnes ved at

a) hvert element (n') av billedverdien (Y) er i form av en offentlig polynomlikning av lav grad (D) større enn eller lik 2 sammensatt av elementene (n) fra verdien (X);

b) billedverdien (Y) også kan frembringes fra verdien (X) ved å anvende en transformasjon omfattende følgende trinn, der noen av disse krever kjennskap til en kryptografisk hemmelighet:

b1) det anvendes på verdien (X) en første hemmelig polynom- transformasjon (s) av grad 1 sammensatt av de (n) elementene til verdien (X) for å frembringe et første bilde (I1) med (n) elementer;

b2) det dannes én eller flere grener, der hver av disse grenene er sammensatt av elementer fra det første bildet (I1) og,

• i minst én (e) av grenene er de (n_e) elementene i grenen tenkt å representere en variabel, eller et lite antall (k) variabler (x, x', x", ..., x^k) som tilhører en utvidelse (L_w) med grad W av ringen (K) med $W*k = n_e$, og det anvendes på minst denne grenen (e) en transformasjon som følger:

$f_e: L_w^k \rightarrow L_w^k$

$(x, x', x", ..., x^k) \_\rightarrow (y, y', y", ..., y^k)$

hvor (y, y', y", ..., y^k) er bildet av (x, x', x", ..., x^k) fra transformasjonen f_e, der f_e verifiserer følgende to egenskaper:

-b2.1) i en basis (B) av utvidelsen (L_w) av ringen er hver komponent av bildet (y, y', y", ..., y^k) uttrykt i form av et polynom sammensatt av komponentene til (x, x', x", ..., x^k) i denne basisen, hvilket polynom har en total grad mindre enn eller lik den nevnte graden (D) på den offentlige polynomlikningen;

-b2.2) uttrykt ved utvidelsen (L_w) av ringen er transformasjonen (f_e) slik at det er mulig å beregne forleddene til (f_e) når de eksisterer, kanskje bortsett fra spesielle biter, idet antallet slike er neglisjerbart i forhold til det totale antallet biter.

• og ved å anvende på de andre mulige grenene polynomtransformasjoner med grad mindre enn eller lik den nevnte graden (D) dannet av komponentene med verdi i ringen (K);

b3) grenen som er således transformert, eller mangfoldet av grener som er således transformert, så sammenkjedet, utgjør et andre bilde (I2);

b4) det anvendes på det andre bildet (I2) en andre hemmelig polynomtransformasjon (t) av grad 1 sammensatt av elementer i det andre bildet (I2) for å frembringe et tredje bilde (I3) som har et bestemt antall elementer; og

b5) det velges ut (n') elementer blant settet av elementer i det tredje bildet (I3) for å danne billedverdien (Y).

Oppfinnelsen angår også en asymmetrisk signaturverifikasjonsfremgangsmåte og en asymmetrisk autentifikasjonsfremgangsmåte som kjennetegnes ved at signaturen er frembrakt ved å anvende på en melding, eller på en offentlig transformasjon av en melding, en transformasjon som samsvarer med den inverse transformasjon av den som er angitt ovenfor, og ved at verifikasjonen består av å kontrollere at et resultat (Y) er oppnådd som samsvarer med forutbestemte relasjoner knyttet til meldingen som skal signeres.

Andre detaljer og fordeler med oppfinnelsen fremgår fra den følgende beskrivelse av flere foretrukne men ikke begrensende utforminger, med referanse til de vedføyde tegningene, hvor

Figur 1 viser sammenkjedingen av transformasjonene anvendt for å prosessere en melding;

Figur 2 viser en kommunikasjonsanordning anvendt for å utføre koding/dekoding av en melding; og

Figur 3 viser den samme anordningen anvendt for utføring av signatur for en melding og dens verifikasjon.

Først, før oppfinnelsen presenteres, vil det bli gitt et kort matematisk tilbakeblikk spesielt med hensyn på egenskapene til endelige felter.

Beskrivelse av egenskaper ved endelige felter.

1) Funksjon f:

La K være et endelig felt med kardinal q og karakteristikk p (typisk, men ikke nødvendigvis, så er q = p = 2). La L_N være en utvidelse av K med grad N, la $\beta_{i,j}$, $\alpha_{i,j}$ og μ_0 være elementer i L_n, la $\theta_{i,j}$, $\varphi_{i,j}$ og ξ_i være heltall, og la f være den følgende applikasjonen

$f: L_N \dashrightarrow L_N$

$x\rangle \dashrightarrow \sum_{i,j} \beta_{i,j} * x^{Q+P} + \sum_i \alpha_i * x^S + \mu_0$

$$\text{der } Q = q^{\theta i,j},\ P = q^{\varphi i,j} \text{ og } S = q^{\xi i}$$

der f er et polynom bestående av x og (*) betegner multiplikasjon. Det nevnes at Q, P og S muligens kan betegne mange verdier i denne kryptografen siden det kan være mange $\theta_{i,j}$, $\varphi_{i,j}$ og ξ_i.

Dessuten, for ethvert heltall λ, er $x\rangle \dashrightarrow x^{q\lambda}$ en lineær applikasjon på LN $\dashrightarrow$ LN. f er derfor en kvadratisk funksjon.

Hvis B er en basis for L_N, er uttrykket for f i basisen B:

$f(x_1, ..., x_N) = (P_1(x_1, ..., x_N), ..., P_N(x_1, ..., x_N))$

der $P_1, ..., P_N$ er polynomer med total grad 2 sammensatt av N variabler $x_1, ..., x_N$.

Polynomene $P_1, ..., P_N$ beregnes ved anvende en representasjon av L_N. En representasjon av L_N er typisk fikspunktet til et irreduktibelt polynom $i_N(X)$ på K, med grad N, som gjør det mulig å identifisere L_N med $K[X]/(i_N(X))$. Det er da enkelt å beregne polynomene $P_1, ..., P_N$.

Inversjon av f

La μ være graden i x for polynomet f. f er ikke nødvendigvis en bijeksjon av L_N $\dashrightarrow$ L_N; likevel:

1) med "a" som et element i L_N finnes det kjente algoritmer som gjør det relativt enkelt å finne alle verdiene til x i L_N (hvis det eksisterer noen) slik at $f(x) = a$ når μ ikke er for stor (for eksempel for $\mu \geq 1{,}000$).

2) Dessuten, for hver "a" i L_N er det maksimalt "μ" løsninger for x slik at $f(x) = a$.

3) I noen tilfeller kan f være bijektive.

Grunnleggende HFE-algoritme for kodings-/dekodingssystemet

En første versjon av den nye HFE-algoritmen vil nå bli beskrevet. Denne versjonen er ikke begrensende, og mer generelle versjoner presenteres i påfølgende seksjoner.

Et felt K omfattende $q = p^m$ elementer er offentlig. Hver melding er sammensatt av n elementer i K. For eksempel, hvis p = 2 har hver melding n*m bits. n er også offentlig og er separert i d heltall: $n = n_1 + ... + n_d$.

Hvert av disse heltallene n_e ($1 <= e <= d$) assosieres med en utvidelse Ln_e av feltet K med grad n_e (symbolet <= betyr mindre enn eller lik).

La "ord" være en verdi representert av komponenter fra K. For eksempel kan et element fra Ln_e ($1 <= e <= d$) representeres som et ord med lengde n_e. I kodingsmekanismen som beskrives her vil kvadratiske funksjoner $f_1, ..., f_d$, som er analoge med funksjonen f beskrevet over, bli anvendt med $N = n_1$ for f_1, $N = n_2$ for f_2 osv. Disse funksjonene vil generere d ord. Disse d ordene vil så kombineres til ett ord med lengden n.

• De hemmelige objektene er:

1) to affine bijektive transformasjoner s og t fra K^n ------- → K^n. Disse affine bijeksjonene kan representeres i en basis med polynomer av grad 1 og med koeffisienter i K.

2) separasjonen av n i d heltall: $n = n_1 + ... + n_d$.

3) Representasjonen av feltene $Ln_1, ..., Ln_d$. Disse "representasjonene" er resultatet av et valg av d irreduktible polynomer. Ψn_e betegnes som isomorfismen fra K^{ne} til Ln_e beskrevet av denne representasjonen med e slik at $1<= e <= d$.

4) De kvadratiske funksjonene $f_1, ..., f_d$ er av den samme typen som funksjonen f beskrevet i avsnittet med tittelen "funksjonen f" (ved å bruke $N = n_e$ og $1 <= e <=d$).

Første anmerkning: alle disse objektene er hemmelige a priori, men objektene i punktene 2), 3) og 4) over kan også være offentlig a priori. I realiteten ligger sikkerheten i algoritmen hovedsakelig i de hemmelige transformasjonene s og t.

Andre anmerkning: s og t er bijektive applikasjoner, men de kan også være kvasi-bijektive i betydningen at de kan være applikasjoner som ikke har mer enn noen få forledd.

Kodingsmekanismen er beskrevet i figur 1. Sekvensen av operasjoner løper fra topp til bunn. Den affine bijektive transformasjonen s av K^n ----- → K^n opptrer først.

Funksjonene $\mu_1, ..., \mu_d$ er projeksjonsfunksjoner av K^n ---- → K^{ne}

(der $1 <= e <= d$), og μ er den inverse sammenkjedningsfunksjonen. På en måte separerer funksjonene μ_1, ..., μ_d de n elementene i d "grener".

Isomorfismen Ψn_e anvendes fra de forskjellige feltene K^{ne} til de forskjellige feltrepresentasjonene Ln_1, ..., Ln_d, så anvendes de respektive kvadratiske funksjonene f_1, ..., f_d fra hhv. Ln_1, ..., Ln_d til Ln_1, ..., Ln_d. Deretter anvendes den inverse isomorfismen $(\Psi n_e)^{-1}$ fra de forskjellige feltrepresentasjonene Ln_1, ..., Ln_d til de forskjellige feltene K^{ne}.

Deretter anvendes den inverse sammenkjedningsfunksjonen μ fra K^{ne} til K^n. Til slutt opptrer den affine bijektive transformasjonen t, som har en generell form lik transformasjonen s, fra K^n, ----- $\rightarrow K^n$.

F_2 er en funksjon av grad mindre enn eller lik (D) som avhenger av variablene i blokken lengst til venstre.

Mer generelt er F_i ($2 <= i <= d$) en funksjon av grad mindre enn eller lik (D) som avhenger av variablene i blokkene 1, 2, ..., i-I.

MERK: Disse funksjonene F_2, ..., F_d produserer et Feisteldiagram i blokker. Ofte anvendes de ikke i HFE-algoritmen, og i det tilfellet er $F_2 = ... = F_d = 0$.

Det må nevnes, og dette er et viktig poeng, at sammensetningen av alle disse operasjonene genererer en kvadratisk funksjon når denne funksjonen uttrykkes med hensyn på sine komponenter i en basis. Denne funksjonen kan derfor bli gitt av n polynomer ($P_1, \ldots, P_n$) med koeffisienter i K, og disse polynomene gjør det mulig å beregne den kodede teksten (y) som funksjon av den ukodede teksten x.

• De offentlige objektene er:

1) Feltet K av $1 = p^m$ elementer, og lengden n av meldingene.

2) De n polynomene ($P_1, \ldots, P_n$) sammensatt av n variabler i K. Hvem som helst kan derfor kode en melding (kodingsalgoritmen er offentlig i overensstemmelse med karakteristikken av den krevde oppfinnelsen).

Videre er dekoding mulig hvis de hemmelige objektene er kjent. I realiteten er det da mulig å invertere alle operasjonene beskrevet i figur 1. Inversjonen av funksjonene f_e består derfor i å løse en polynomlikning med en ukjent i feltet Ln_e som indikert for f i avsnittet med tittelen "inversjon av f". Det må imidlertid nevnes at f_e ikke nødvendigvis er bijektiv. Det er da mulig å få mange forledd. I dette tilfellet vil valget av ukodet tekst bli bestemt ved hjelp av en overflødighet lagt inn i den ukodede teksten, og den dekodede teksten vil være den som

inneholder denne overflødigheten. Hvis funksjonene ikke er bijektive vil det være nødvendig å tenke på å legge denne overflødigheten systematisk inn i den ukodede meldingen.

Eksempel på anvendelse av algoritmen for signatur.

To tilfeller må tas i betraktning

• Funksjonene er bijektive.

Dersom H er resultatet av spredningsfunksjonen

("the hash-function") anvendt på en melding som skal signeres (for eksempel har H et format på 128 bits), så er signaturen $S = HFE^{-1}(H)$.

Ved det faktum at HFE-kodingsfunksjonen er offentlig kan derfor hvem som helst verifisere signaturen ved å utføre: $H' = HFE(S)$ og ved å verifisere at $H' = H$. Avsenderen av signaturen må selvfølgelig kjenne hemmeligheten for å beregne S.

• Funksjonene er ikke bijektive.

I dette tilfellet er det mulig å velge et antall bits ved innsendingen til HFE som er større enn antallet bits ved utsendingen for å være nesten sikker på å kunne beregne forleddene ved å anvende HFE-algoritmen.

Eksempelvis kan H uttrykkes i 128 bits og S i 128+20 = 148 bits.

Spesifikke tilfeller av implementasjon

Det finnes mange måter å utføre HFE-algoritmen på som alle gir store fordeler angående den praktiske utføring og implementasjon.

• Tilfellet med algoritmen med kun én gren (dvs. d = 1).

Denne versjonen har bare én (stor) gren, og i hver likning er derfor alle variablene – dvs. alle bitser i meldingen – involvert. Tatt i betraktning denne grenens store størrelse har ikke denne utførelsen den potensielle svakheten som grener av liten størrelse.

• Tilfellet med små grener med den samme funksjonen f.

Dette spesielle tilfellet involverer små grener, eksempelvis med verdier på 12 bits, og med den samme funksjonen f. Denne versjonen er spesielt fordelaktig fordi den enkelt kan

implementeres i små sentralprosessorer for eksempel inneholdt i chip-kort, og implementasjonen av denne er mulig ved hjelp av et program eller en matematisk koprosessor.

Første variant av HFE-algoritmen

Funksjonen f anvendt i hver gren, som allerede nevnt i dette dokumentet, er en polynomlikning med en enkelt variabel x i et endelig felt. Uttrykt i en basis er denne funksjonen f uttrykt som en likning med total grad lik to.

Faktisk kan det anvendes en annen type funksjon f som avviker litt fra den vanlige modellen tidligere definert. Denne nye, ukjente typen består av å velge for f en funksjon som avhenger av flere endelig-felt-variabler, for eksempel to variabler x_1 og x_2 slik at, i en basis, beholder uttrykket som funksjon av koordinatene, en total grad lik to og at det alltid er mulig å tilbakeberegne forleddene for en gitt verdi av f når de eksisterer.

Denne varianten vil bli bedre forstått gjennom det numeriske eksempelet under. Betrakt en gren av algoritmen med verdier på 64 bits og med p=2. I denne varianten, la f avhenge av to variabler x og x' på 32 bits hver, med f(x, x') = (y,y') slik at :

$$\begin{cases} y = x^4 = x*x' = x' & (1) \\ y' = x^{17} + x^4 * x' + x'^3 & (2) \end{cases}$$

(det skal bemerkes at anvendelsen av denne eksakte funksjonen ikke nødvendigvis er å anbefale og kun er gitt som et eksempel).

For å bestemme paret (x, x') fra (y, y') et det for eksempel mulig å gå frem på følgende måte:

Fra likningen (1), has: $x' = (y - x^4)/(x + 1)$ (3)

Fra likningen (2) has derfor:

$y'(x + 1)^3 = x^{17}(x + 1)^3 + x^4(y - x^4)(x + 1)^2 + (y - x^4)^3$ (4)

Merk at (4) er en polynomlikning med en enkelt variabel x. Som indikert over kjenner matematikerne allerede til noen generelle metoder for å løse denne typen likninger, og det er derfor mulig å løse (4), noe som gjør det mulig å finne verdiene for x som løser likningen; x' kan deretter finnes ved å substituere disse verdiene for x i likning (3).

MERK: Dagens kjente teknikker for å løse likninger med flere variabler i endelige felt gjør det mulig å korrekt løse andre typer likninger enn den som er illustrert i dette eksempelet. Spesielt likninger der det ikke er nødvendig å uttrykke en variabel som funksjon av de andre for så å substituere for den.

Andre variant av HFE-algoritmen

Naturligvis begrenser ikke beskrivelsen av HFE-algoritmen og dens varianter oppfinnelsen som kreves til anvendelse av polynomlikninger av kun én grad: graden 2. Det er fullt mulig å anvende 3. grad; i dette tilfellet er det en offentlig form av 3. grad.

Likeledes er graden 4 eller til og med 5 mulig. Det er imidlertid nødvendig at graden er lav nok til at de offentlige likningene som resulterer fra den holder seg enkle for en computer å lagre og beregne.

Valget av parametrene er også viktig for å sikre maksimal sikkerhet og for å unngå, i størst mulig grad, forsøk på kodeanalyse. Det er derfor av sikkerhetsgrunner fordelaktig at:

1) det i hver gren er minst én variabel på 32bits, og fortrinnsvis minst 64bits,

2) det ikke er likninger på formen: $\sum\gamma_{ij}\, x_i y_j + \sum\alpha_i\, x_i \sum\beta_j y_j + \delta_0 = 0$, hvor minst én av koeffisientene γ_{ij}, α_i, β_j eller δ_0 er forskjellig fra null, og som alltid verifiseres dersom y_j-koeffisientene er komponentene i den kodede teksten og x_i-koeffisientene er komponentene i den ukodede teksten. MERK: det var blant annet på grunn av at en slik betingelse ikke var verifisert at Matsumoto-Imai-algoritmen nevnt over ble avslørt ikke å være fullstendig sikker.

3) det ikke er likninger på formen

$\sum\gamma_{ijk}\, x_i y_j y_k + \sum\alpha_{ij}\, x_i y_j + \sum\beta_{ij} y_i y_i + \sum\mu_i x_i + \sum\nu_i y_i + \delta_0 = 0$

det vil si totalt av 3. grad og av første grad i x,

4) mer generelt er det av sikkerhetsgrunner foretrukket at det ikke finnes noen likning av "lav" grad som alltid er verifisert mellom koordinatene i de ukodede og kodede meldingene, bortsett fra de lineære kombinasjonene av produktene i de offentlige likningene i små polynomer.

Tredje variant av HFE-algoritmen

Det er blitt indikert at for å anvende HFE-algoritmen når funksjonen ikke er bijektiv, er det mulig å introdusere overflødigheter i den ukodede teksten.

Det er en annen mulighet: i realiteten er det mulig at størrelsen på den kodede verdien Y er større enn størrelsen på den ukodede verdien X hvis nye elementer fra K settes inn i den kodede verdien. Disse nye elementene er også de som resulterer fra likninger av andre grad dannet av komponentene til X. Mer generelt, med bruk av notasjonen i figur 1, kunne det samme elementet til s(x) bli overført til flere grener. Det er også mulig å legge til en eller flere grener sammensatt av vilkårlige likninger av andre grad i en basis, hvor i dette tilfellet disse ytterligere grenene blir anvendt for å skille ut det riktige forleddet for de andre grenene.

Fjerde variant av HFE-algoritmen

I stedet for å gjøre offentlige alle likningene som resulterer i den siste funksjonen i figur 1, kan én eller flere av dem holdes hemmelige. Dette betyr at isteden for å gjøre (P_1, ...,P_n) offentlige, er det mulig å gjøre kun deler av disse likningene offentlige, og i dette tilfellet utføres kodingen ved å beregne kun de offentlige av de (P_1, ...,P_n) polynomene.

I dekoding forsøkes alle de mulige verdier for de ikke-offentlige polynomene P_i, noe som a priori gir flere mulige dekodede meldinger, og den korrekte meldingen er merket som før: enten ved å introdusere overflødigheter i den ukodede meldingen, eller ved anvendelse av metoden indikert i den tredje varianten.

MERK: det faktum at én eller flere offentlige likninger derfor elimineres kan i noen tilfeller gjøre det enda vanskeligere å oppdage strukturen i feltene skjult av HFE-algoritmen.

Forklaring på figur 2

Figur 2 illustrerer skjematisk et eksempel på kodings/dekodingssystemet ved å anvende HFE-algoritmen beskrevet over.

Anta at det er to enheter A og B som tilhører det samme kommunikasjonsnettverket, og som hver har sitt respektive sender-/mottakerutstyr for meldinger 1, 2. Dette utstyret inkluderer beregningsanordninger, f.eks. en datamaskin, designet for å utføre koding/dekoding av meldinger, og lagringsanordninger. I det minste deler av disse

beregnings- og lagringsanordningene kan legges til et portabelt objekt som inkorporerer en mikroprosessor eller logiske kretser med mikroledninger, som definerer områder til hvilke tilgang blir kontrollert, og kan derfor inneholde hemmelig informasjon så som kryptografiske nøkler (se for eksempel det portable objektet beskrevet i det franske patentet Nr. 2.401.459).

Hver anordning inkorporerer HFE-algoritmen som beskrevet over, spesielt i form av et program, i tillegg til den inverse algoritmen HFE^{-1}.

De to anordningene forbindes med en kommunikasjonslinje 3.

Både A og B innehar et nøkkelpar, hhv. en offentlig nøkkel Cp^A og Cp^B og en hemmelig nøkkel Cs^A og Cs^B innbyrdes forbundet med den samsvarende offentlige nøkkelen Cp^A eller Cp^B. Hvis A og B ikke har anordningene for å beregne nøkkelparene, kan denne beregningen utføres av nettverket ved å gi det en gitt myndighet med hensyn på hvert medlem i nettverket. Hvis disse to enhetene ønsker å føre dialog med hverandre i en beskyttet modus, dvs. uten at noen skal kunne forstå dataene som utveksles, vil de implementere følgende prosedyre:

A sender B sin offentlige nøkkel Cp^A, og B sender A sin offentlige nøkkel Cp^B. I en variant kan nettverket ha de offentlige nøklene til alle medlemmene i primærlageret og kommunisere dem til medlemmene på anmodning. Med en gang A har mottatt den offentlige nøkkelen Cp^B, vil A anvende denne til å kode, ved hjelp av den kryptografiske algoritmen HFE, en melding M som den ønsker å overføre til B, og en melding M'. Denne meldingen blir med en gang den mottas av B dekodet ved hjelp av den kryptografiske algoritmen HFE^{-1} og den hemmelige nøkkelen Cs^B. Kun B kan dekode meldingen siden den er det eneste medlemmet av nettverket som innehar denne nøkkelen. For overføring av meldinger fra B til A er fremgangsmåten helt analog.

Forklaring av figur 3

Figur 3 illustrerer skjematisk et eksempel på anvendelsen av systemet i figur 2 for å implementere en beregnings- og signaturverifikasjonsprosedyre som anvender den kryptografiske algoritmen beskrevet over.

I dette tilfellet er det nødvendig at overføringen av meldinger gjøres med autentifikasjon, dvs. at mottakeren av meldingen M har mulighet å forsikre seg om at meldingen kommer fra en spesiell person. Anta for eksempel at A ønsker å sende B en autentifisert melding. De to kommunikatorene vil implementere følgende prosedyre:

A vil først sende B sin offentlige nøkkel Cp^A, eller i en variant kan B også be om nøkkelen fra nettverket.

A vil deretter kode meldingen med sin egen hemmelige nøkkel Cs^A og den kryptografiske algoritmen HFE^{-1}. Det oppnådde resultatet kalles signaturen S til meldingen. Deretter sendes meldingen (som i dette tilfellet går ukodet) og dennes signatur til B. B dekoder signaturen ved hjelp av den kryptografiske algoritmen HFE og den offentlige nøkkelen Cp^A som han tidligere har fått. Resultatet oppnådd av dette, betegnet M", må være det samme som den mottatte meldingen M. Dersom dette faktisk er tilfelle beviser det at signaturen ble beregnet ved hjelp av den hemmelige nøkkelen Cs^A og derfor at meldingen faktisk kommer fra A, det eneste medlemmet av nettverket som innehar denne nøkkelen.

En kjent forbedring av dette systemet består av å beregne ikke bare signaturen til meldingen, men signaturen til en konsentrasjon av meldingen. Ved å anvende en spredningsfunksjon kan derfor en relativt stor melding bli komprimert til et fikspunkt H som er karakteristisk for meldingen. Denne spredningsfunksjonen kan implementeres ved å anvende standard spredningsfunksjoner (som f.eks. MD5 eller SHA).

Kortfattet resulterer oppfinnelsen i følgende:

1. Oppfinneren har vist (jfr. document Crypto '95, s.248 - 261) at den initielle algoritmen til Matsumoto og Imai ikke var kryptografisk fullkommen. Denne algoritmen besto av å "gjemme" en bijeksjon f på formen $f(b) = a^{1+Q}$ der $Q = q^\theta$ ved to affine transformasjoner s og t.

2. Oppfinneren har vist at det er mulig å anvende mye mer generelle funksjoner for f. Oppfinneren har faktisk vist, på den ene siden, at det var mulig å anvende ikke-bijektive funksjoner f, og på den andre siden at det var mulig å anvende det faktum at det er kjent hvordan en beregner forleddene for veldig forskjellige familier av polynomer, for eksempel ved å anvende PGCD-beregninger av polynomer eller resultanter av polynomer, eller ved å anvende GRÖBNER basiser.

3. Det er nødvendig at minst en av grenene ikke er for liten. Oppfinneren oppdaget at små grener leder til svake HFE-algoritmer.

4. Oppfinneren merket dessuten at det noen ganger er mulig å velge ut bare noen av elementene som utgjør det tredje bildet (I3) som resulterer fra transformasjon av det andre bildet (I2) ved hjelp av den andre hemmelige polynom-transformasjonen.

PATENTKRAV

1. En kryptografisk kommunikasjonsfremgangsmåte som transformerer en verdi (X), representert av (n) elementer i en endelig ring (K), til en billedverdi (Y) representert ved (n') elementer i ringen (K),

karakterisert ved at

a) hvert element (n') av billedverdien (Y) er i form av en offentlig polynomlikning av lav grad (D) større enn eller lik 2 sammensatt av elementene (n) fra verdien (X);

b) billedverdien (Y) også kan fås fra verdien (X) ved hjelp av en transformasjon omfattende følgende trinn, der minst noen av dem krever kjennskap til en kryptografisk hemmelighet:

b1) det anvendes på verdien (X) en første hemmelig polynom- transformasjon (s) av grad 1 sammensatt av de (n) elementene til verdien (X) for å frembringe et første bilde (I1) med (n) elementer;

b2) de (n) elementene i det første bildet (I1) tenkes å representere en variabel eller et lite antall (k) variabler (x, x', x", ..., x^k) tilhørende en utvidelse (L_w) med graden W av ringen (K) med W*k = n, ved å anvende på det første bildet (I1) en transformasjon definert som følger:

f: $L_w^k \rightarrow L_w^k$

$(x, x', x'', ..., x^k) \rightarrow (y, y', y'', ..., y^k)$

hvor $(y, y', y'', ..., y^k)$ er bildet av $(x, x', x'', ..., x^k)$ fra transformasjonen f, der f verifiserer følgende to egenskaper:

-b2.1) i en basis (B) av ringutvidelsen (L_w) er hver komponent av bildet $(y, y', y'', ..., y^k)$ uttrykt i form av et polynom sammensatt av komponentene til $(x, x', x'', ..., x^k)$ i denne basisen, hvilket polynom har total grad mindre enn eller lik graden (D) på den offentlige polynomlikningen;

-b2.2) uttrykt ved ringutvidelsen (L_w) er transformasjonen (f) slik at det er mulig å beregne forleddene til (f) når de eksisterer, kanskje bortsett fra spesielle biter, der antallet slike er neglisjerbart relativt til det totale antallet biter;

b3) det første bildet (I1) som er således transformert, utgjør et andre bilde (I2);

b4) det anvendes på det andre bildet (I2) en andre hemmelig polynomtransformasjon (t) av grad 1 sammensatt av elementer i det andre bildet (I2) for å frembringe et tredje bilde (I3) som har et bestemt antall elementer; og

b5) det velges ut (n') elementer fra settet av elementer i det tredje bildet (I3) for å danne den nevnte billedverdien (Y).

2. Fremgangsmåte i følge krav 1

k a r a k t e r i s e r t v e d at den nevnte lave graden (D) på den offentlige polynomlikningen er lik 1.

3. Fremgangsmåte i følge krav 1

k a r a k t e r i s e r t v e d at antallet k variabler er lik 1.

4. Fremgangsmåte i følge krav 3,

k a r a k t e r i s e r t v e d at den nevnte lave graden (D) på den offentlige polynomlikningen er lik 2, (K) er et endelig felt, og den nevnte transformasjonen (F) har følgende form:

$f: L_w \text{ ----- } \rightarrow L_w$

$x \text{ - } \rightarrow \sum_{i,j} \beta_{i,j} * x^{Q+P} + \sum_i \alpha_i * x^S + \mu_0$

der q er kardinalen til feltet (K); $Q = q^{\theta i,j}$, $P = q^{\varphi i,j}$ og $S = q^{\xi i}$, $\beta_{i,j}$, α_i og μ_0 er elementer i L_w, og $\theta^{i,j}$, $\varphi^{i,j}$ og ξ^i er heltall, og hvor graden i x av polynomet f er mindre enn eller lik 1,000.

5. Fremgangsmåte i følge krav 1,

k a r a k t e r i s e r t v e d at det ikke er polynomlikninger av lav total grad sammensatt av komponentene (x, x', x", ..., x^k) og (y, y', y", ..., y^k) andre enn lineære kombinasjoner av produktene til de offentlige likingene i små polynomer.

6. Fremgangsmåte ifølge krav 1,

k a r a k t e r i s e r t v e d at det ikke er polynomlikninger på formen:

$\sum\gamma_{ij} x_i y_j + \sum\alpha_i x_i \sum\beta_j y_j + \delta_0 = 0$ med minst én av koeffisientene γ_{ij}, α_i, β_j eller δ_0 forskjellig fra null, som alltid verifiseres dersom koeffisientene y_j er komponentene i den kodede meldingen og koeffisientene x_i er komponentene i den ukodede meldingen.

7. Fremgangsmåte ifølge krav 1,

karakterisert ved at ringen (K) er et endelig felt og utvidelsen (L_w) av ringen er en utvidelse med graden W av ringen (K), som betyr at (L_w) er isomorf med K[X]/g(X), der g er et irreduktibelt polynom av grad W på K.

8. Fremgangsmåte for asymmetrisk autentifikasjon, ved en første person kalt kontrollør, av en annen person kalt en bevisfører,

karakterisert ved at

-kontrolløren sender bevisføreren en første verdi (Y);

-bevisføreren returnerer til kontrolløren en andre verdi (X) oppnådd ved å anvende en transformasjon på den første verdien (Y) som samsvarer med den inverse transformasjonen ifølge krav 1;

-kontrolløren anvender transformasjonen ifølge krav 1 på den andre verdien (X) og verifiserer at resultatet samsvarer med en forutbestemt relasjon knyttet til den første verdien (Y).

9. Kryptografisk kommunikasjonsfremgangsmåte som transformerer en verdi (X), representert av (n) elementer i en endelig ring (K), til en billedverdi (Y) representert ved (n') elementer i ringen (K),

karakterisert ved at

a) hvert element (n') av billedverdien (Y) er i form av en offentlig polynomlikning av lav grad (D) større enn eller lik 2 sammensatt av elementene (n) fra verdien (X);

b) billedverdien (Y) også kan frembringes fra verdien (X) ved å anvende en transformasjon omfattende følgende trinn, der noen av disse krever kjennskap til en kryptografisk hemmelighet:

b1) det anvendes på verdien (X) en første hemmelig polynom- transformasjon (s) av grad 1 sammensatt av de (n) elementene til verdien (X) for å frembringe et første bilde (I1) med (n) elementer;

b2) det dannes én eller flere grener, der hver av disse grenene er sammensatt av elementer fra det første bildet (I1) og,

• i minst én (e) av grenene er de (n_e) elementene i grenen tenkt å representere en variabel, eller et lite antall (k) variabler (x, x', x", ..., x^k) som tilhører en utvidelse (L_w) med

grad W av ringen (K) med $W^*k = n_e$, og det anvendes på minst denne grenen (e) en transformasjon som følger:

$f_e: L_w^k \rightarrow L_w^k$

$(x, x', x'', ..., x^k) \_\rightarrow (y, y', y'', ..., y^k)$

hvor $(y, y', y'', ..., y^k)$ er bildet av $(x, x', x'', ..., x^k)$ fra transformasjonen f_e, der f_e verifiserer følgende to egenskaper:

-b2.1) i en basis (B) av utvidelsen (L_w) av ringen er hver komponent av bildet $(y, y', y'', ..., y^k)$ uttrykt i form av et polynom sammensatt av komponentene til $(x, x', x'', ..., x^k)$ i denne basisen, hvilket polynom har en total grad mindre enn eller lik den nevnte graden (D) på den offentlige polynomlikningen;

-b2.2) uttrykt ved utvidelsen (L_w) av ringen er transformasjonen (f_e) slik at det er mulig å beregne forleddene til (f_e) når de eksisterer, kanskje bortsett fra spesielle biter, idet antallet slike er neglisjerbart i forhold til det totale antallet biter.

• og ved å anvende på de andre mulige grenene polynomtransformasjoner med grad mindre enn eller lik den nevnte graden (D) dannet av komponentene med verdi i ringen (K);

b3) grenen som er således transformert, eller mangfoldet av grener som er således transformert, så sammenkjedet, utgjør et andre bilde (I2);

b4) det anvendes på det andre bildet (I2) en andre hemmelig polynomtransformasjon (t) av grad 1 sammensatt av elementer i det andre bildet (I2) for å frembringe et tredje bilde (I3) som har et bestemt antall elementer; og

b5) det velges ut (n') elementer blant settet av elementer i det tredje bildet (I3) for å danne billedverdien (Y).

10. Fremgangsmåte ifølge krav 9,
karakterisert ved at et polynom med grad mindre enn eller lik (D) legges til utsendingsdataene fra grenen således transformert eller andre grener hvilket polynom avhenger kun av variablene i grenene anbrakt rett før denne grenen.

11. Fremgangsmåte ifølge krav 9,
karakterisert ved at det første bildet (I1) har flere grener , hvor en av disse grenene manipulerer verdier på minst 32 bits.

12. Fremgangsmåte for asymmetrisk signaturverifikasjon og autentifikasjon av en melding (X),

k a r a k t e r i s e r t v e d at signaturen er frembrakt ved å anvende på en melding, eller på en offentlig transformasjon av en melding, en transformasjon som samsvarer med den inverse transformasjon av den som er angitt i fremgangsmåten ifølge krav 1 eller krav 9, og ved at verifikasjonen består av å kontrollere at et resultat (Y) er oppnådd som samsvarer med forutbestemte relasjoner knyttet til meldingen som skal signeres.

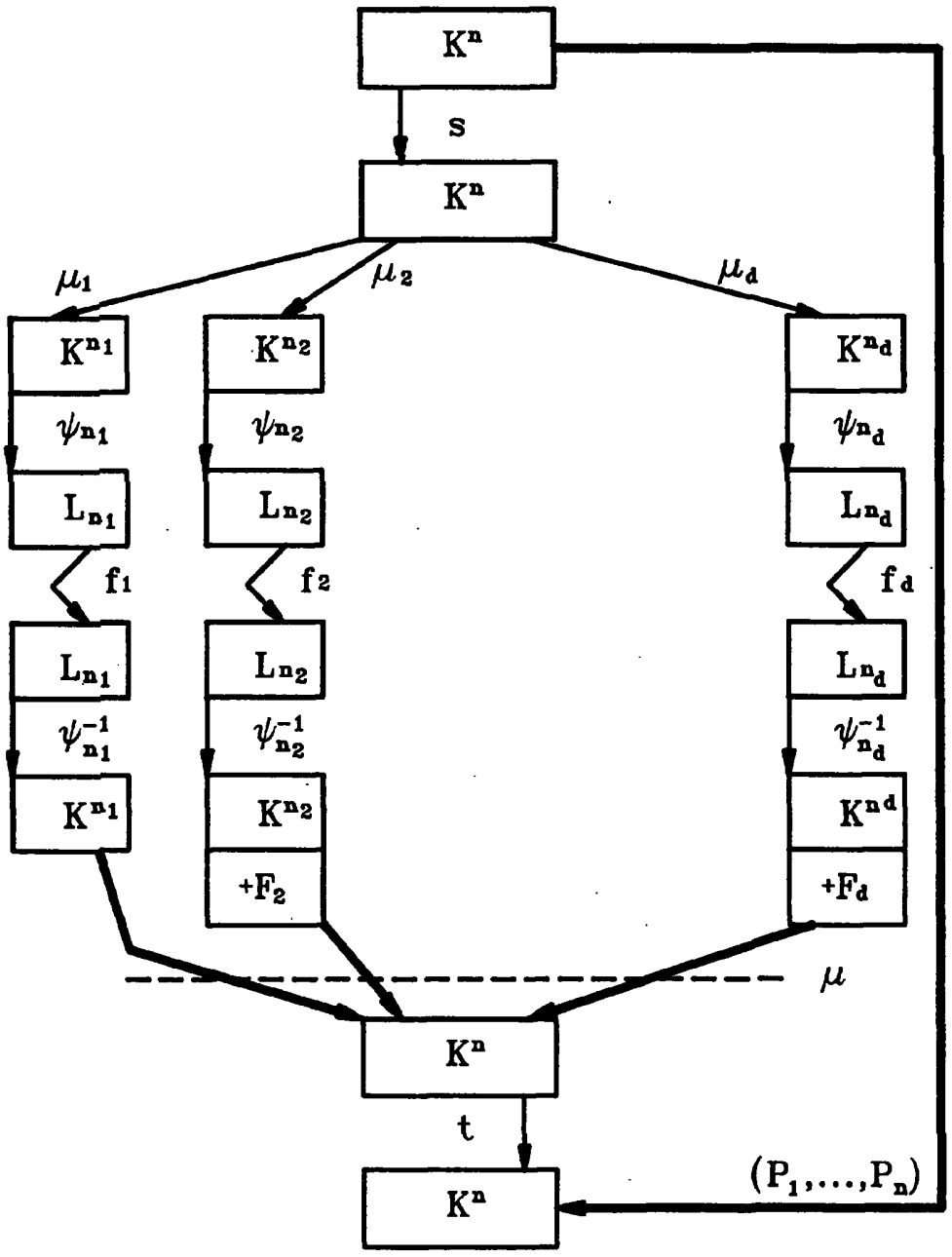

K^n
s
K^n
μ_1
μ_2
μ_d
K^{n_1}
K^{n_2}
K^{n_d}
ψ_{n_1}
ψ_{n_2}
ψ_{n_d}
L_{n_1}
L_{n_2}
L_{n_d}
f_1
f_2
f_d
L_{n_1}
L_{n_2}
L_{n_d}
$\psi^{-1}_{n_1}$
$\psi^{-1}_{n_2}$
$\psi^{-1}_{n_d}$
K^{n_1}
K^{n_2}
K^{n_d}
$+F_2$
$+F_d$
μ
K^n
t
K^n
$(P_1,\ldots,P_n)$

Fig. 1

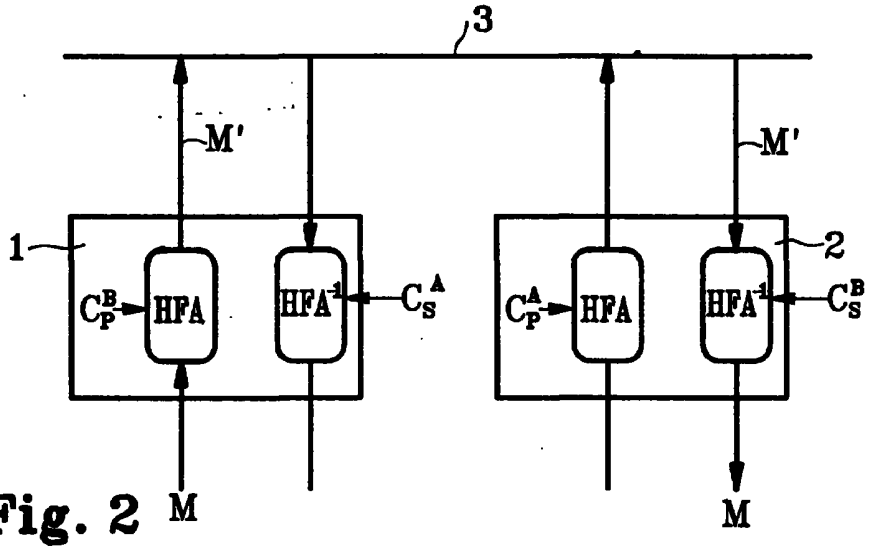

3
M'
M'
1
2
C_P^B
HFA
HFA^{-1}
C_S^A
C_P^A
HFA
HFA^{-1}
C_S^B
M
M

Fig. 2

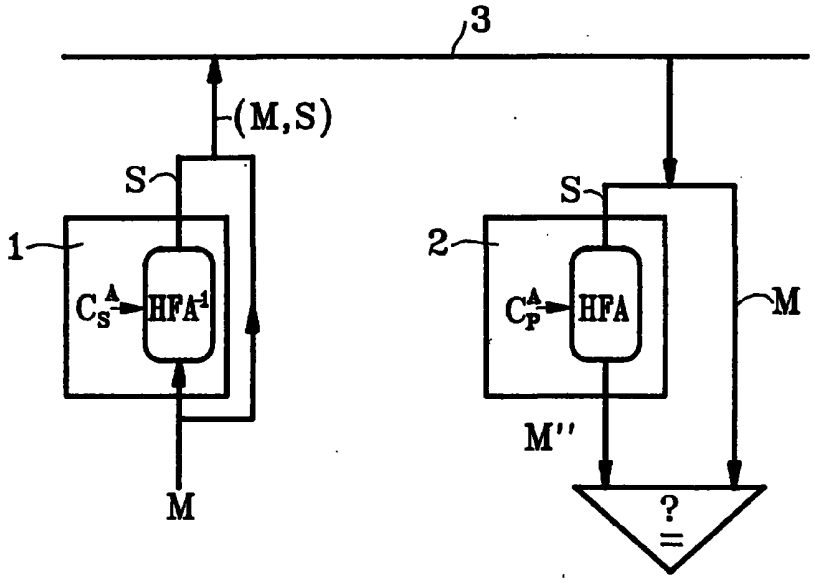

3
(M,S)
S
S
1
2
C_S^A
HFA^{-1}
C_P^A
HFA
M
M''
M
?
=

Fig. 3