(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 532 332**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/30 (2006.01)
G09C 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.04.2010 E 10767169 (5)**

(97) Fecha y número de publicación de la concesión europea: **07.01.2015 EP 2423904**

(54) Título: **Sistema de compartición de secretos, aparato de compartición, aparato de gestión de partes, aparato de adquisición, métodos de procesamiento de los mismos, método de compartición de secretos, programa y medio de grabación**

(30) Prioridad:

24.04.2009 JP 2009106031

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.03.2015

(73) Titular/es:

NIPPON TELEGRAPH AND TELEPHONE CORPORATION (100.0%)
3-1 Otemachi 2-chome Chiyoda-ku
Tokyo 100-8116, JP

(72) Inventor/es:

NISHIMAKI, RYO y
SUZUKI, KOUTAROU

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema de compartición de secretos, aparato de compartición, aparato de gestión de partes, aparato de adquisición, métodos de procesamiento de los mismos, método de compartición de secretos, programa y medio de grabación

CAMPO TÉCNICO

La presente invención se refiere a técnicas de compartición de secretos.

ANTECEDENTES DE LA TÉCNICA

El almacenamiento de información secreta implica el riesgo de pérdida o destrucción de la información secreta y el riesgo de robo. El riesgo de pérdida o destrucción se puede reducir almacenando una pluralidad de copias de la información secreta. Esto, no obstante, aumenta el riesgo de robo. Una solución para eliminar estos riesgos es un esquema de compartición de secretos (SSS) (referencia a la bibliografía no de patente 1 y 2, por ejemplo).

En el esquema de compartición de secretos, se generan una pluralidad de partes SH(1) a SH(N) a partir de la información secreta MSK y se gestionan separadamente por una pluralidad de aparatos de gestión de partes PA(1) a PA(N) y la información secreta MSK se puede reconstruir solamente cuando se obtiene un número predeterminado o mayor de partes entre las partes SH(1) a SH(N). Un método típico para el esquema de compartición de secretos se describirá a continuación.

[Esquema de compartición de secretos de umbral (N,N)]

En un esquema de compartición de secretos de umbral (N, N), si se dan todas las partes SH(1) a SH(N), se puede reconstruir la información secreta MSK, mientras que si se dan cualesquiera (N – 1) partes SH(ϕ_1) a SH(ϕ_{N-1}), nunca se puede obtener la información secreta MSK. Un ejemplo se dará más adelante.

- SH_1, …, SH_{N-1} se seleccionan aleatoriamente.
- SH_N = MSK – (SH_1 + … + SH_{N-1}) se calcula.
- Las partes SH_1, …, SH_N se gestionan separadamente por una pluralidad de aparatos de gestión de partes PA(1), …, PA(N).
- Si se dan todas las partes SH_1, …, SH_N, se puede reconstruir la información secreta MSK por el procesamiento de reconstrucción representado como MSK = SH_1 + … + SH_N.

La operación MSK = SH_1 + … + SH_N para reconstruir la información secreta MSK a partir de las partes SH_1 a SH_N es lineal. Si el procesamiento de reconstrucción se realiza con los resultados de la misma operación lineal CALC para las partes individuales, usando las partes SH(1) a SH(N) y un valor σ como operandos, los resultados que son las partes SH'(1) a SH'(N), se puede obtener el resultado de la operación lineal CALC usando la información secreta MSK y el valor σ como operandos. Si el procesamiento de reconstrucción se ejecuta con SH'(1) = σ·SH(1), …, SH'(N) = σ·SH(N) como las partes SH'(1), …, SH'(N), se puede obtener lo siguiente, por ejemplo.

σ·SH(1) + … + σ·SH(N)
= σ·(SH(1) + … + SH(N))
= σ·MSK (1)

Por otra parte, si el procesamiento de reconstrucción se ejecuta con los resultados de la misma operación lineal CALC para las partes individuales, usando las partes SH(1) a SH(N) y los valores independientes σ(1) a σ(N) como operandos, los resultados que son las partes SH'(1) a SH'(N), no se puede obtener normalmente el resultado de la operación usando la información secreta MSK como operando. Si el procesamiento de reconstrucción se ejecuta con SH'(1) = σ(1)·SH(1), …, SH'(N) = σ(N)·SH(N) como las partes SH'(1), …, SH'(N), se puede obtener lo siguiente, por ejemplo.

$$\sigma(1)\cdot SH(1) + \ldots + \sigma(N)\cdot SH(N) \qquad (2)$$

[Esquema de compartición de secretos de umbral (K, N)]

En un esquema de compartición de secretos de umbral (K, N), si se dan cualesquiera K partes diferentes SH(ϕ_1) a SH(ϕ_K), se puede reconstruir la información secreta MSK, mientras que si se dan cualesquiera (K – 1) partes SH(ϕ_1) a SH(ϕ_{K-1}), nunca se puede obtener la información secreta MSK. Se da un ejemplo más adelante.

- Se selecciona aleatoriamente un polinomio de grado de orden (K – 1) $f(x) = \xi_0 + \xi_1 \cdot x + \xi_2 \cdot x^2 + \ldots + \xi_{K-1} \cdot x^{K-1}$ que satisface f(0) = MSK. Es decir, se especifica ξ_0 = MSK y se seleccionan aleatoriamente ξ_1 a ξ_{k-1}.

Las partes se dan por $SH_\rho = (\rho, f(\rho))$ (ρ = 1 a N).

- Si se obtienen cualesquiera K partes diferentes SH(ϕ_1) a SH(ϕ_K) ((ϕ_1, ..., ϕ_K) $\subset$ (1, ..., N)), la información secreta MSK se puede reconstruir por el procesamiento de reconstrucción siguiente, usando la Expresión de interpolación de Lagrange, por ejemplo.

$$MSK = f(0) = \lambda_1 \cdot f(\varphi_1) + \ldots + \lambda_K \cdot f(\varphi_K) \qquad (3)$$

$$\lambda_\rho(x) = \frac{(x-\phi_1)\cdots\overset{\rho}{\vee}\cdots(x-\phi_K)}{(\phi_\rho-\phi_1)\cdots\overset{\rho}{\vee}\cdots(\phi_\rho-\phi_K)} \in F_q \qquad (4)$$

Aquí, el símbolo $\cdots\overset{\rho}{\vee}\cdots$ indica que el operando de orden ρ [elemento (ϕ_ρ - ϕ_ρ) del denominador, elemento (x - ϕ_ρ) del numerador] no está presente desde el principio. El denominador de la Expresión (4) es

$$(\phi_\rho - \phi_{\rho 1})\cdot \ldots \cdot (\phi_\rho - \phi_{\rho-1})\cdot(\phi_\rho - \phi_{\rho+1})\cdot \ldots \cdot(\phi_\rho - \phi_K)$$

y el numerador de la Expresión (4) es

$$(x - \phi_1)\cdot \ldots \cdot(x - \phi_{\rho-1})\cdot (x - \phi_{\rho+1})\cdot \ldots \cdot(x - \phi_K)$$

Estas relaciones mantienen en el campo.

La operación de la Expresión (3) es lineal. Un valor reconstruido con los resultados de la misma operación lineal CALC para partes individuales, que usa las partes SH(ϕ_1) a SH(ϕ_K) y el valor σ como operandos, los resultados que son las partes SH(ϕ_1) a SH(ϕ_K), llegan a ser iguales al resultado de la operación lineal CALC que usa la información secreta MSK y el valor σ como operandos. Si un valor se reconstruye con los resultados de la misma operación lineal CALC para las partes individuales usando las partes SH(ϕ_1) a SH(ϕ_K) y los valores independientes $\sigma(\phi_1)$ a $\sigma(\phi_K)$ como operandos, los resultados que son las partes SH'(ϕ_1) a SH'(ϕ_K), el resultado de la operación que usa la información secreta MSK como un operando que no se puede obtener normalmente.

La bibliografía no de patente 3 describe esquemas para compartir secretos multinivel entre grupos usando concatenación de códigos Reed-Solomon. En los esquemas propuestos se puede reconstruir un secreto de nivel inferior por un número de grupos menor, mientras que reconstruir un secreto de nivel mayor necesita la colaboración de un número de grupos mayor.

A partir de la bibliografía de patente 1 un método y aparato para almacenamiento de datos seguro que usa bases de datos distribuidas genera una primera pluralidad de partes, usando un primer esquema de umbral, basado en un bloque de datos, con al menos un subconjunto de la primera pluralidad de partes que se necesitan para recrear el bloque de datos. La primera pluralidad de partes entonces se distribuye a una pluralidad de bases de datos distribuidas.

BIBLIOGRAFÍA DE LA TÉCNICA ANTERIOR

BIBLIGRAFÍA NO DE PATENTES

Bibliografía no de patente 1: Kaoru Kurosawa, Wakana Ogata, “Introduction to Modern Cryptography” (escrita en japonés), (ciclo de conferencias de Ingenieros Electrónicos, de Información y Comunicaciones), CORONA PUBLISHING Co, Ltd., marzo de 2004, páginas 116 – 119.

Bibliografía no de patente 2: A Shamir, “How to Share a Secret”, Comunicaciones de la ACM, noviembre de 1979, Volumen 22, Número 11, páginas 612-613.

Bibliografía no de patente 3: Hachiro Fujita et al., “Sharing Multilevel Secrets among Groups using Concatenation of Reed-Solomon Codes”, EL INSTITUTO DE INGENIEROS ELECTRÓNICOS, DE INFORMACIÓN Y COMUNICACIÓN, GIJUTSU HOKOKU, INFORME TÉCNICO DEL IEICE, vol. 108, nº 472, 9 de marzo de 2009,

páginas 65-70.

BIBLIOGRAFÍA DE PATENTE

Bibliografía de patente 1: US 6 363 481 B1

COMPENDIO DE LA INVENCIÓN
PROBLEMAS A SER RESUELTOS POR LA INVENCIÓN

Se considera un sistema que satisface las siguientes condiciones.

Condición 1: Un aparato de compartición genera una pluralidad de partes SH(1) a SH(N) mediante compartición de secretos de la información secreta MSK y permite a una pluralidad de aparatos de gestión de partes PA(1) a PA(N) gestionar las partes separadamente.
Condición 2: El aparato de gestión de partes PA(1) a PA(N) ejecuta algún tipo de operaciones separadamente.
Condición 3: Un aparato de adquisición no puede obtener la información secreta MSK, pero si se dan los resultados de operación generados por un número predeterminado o mayor de aparatos de gestión de partes, se puede obtener la información de generación SK, que es la misma que el resultado de una operación que usa la información secreta MSK y un valor dado σ como operandos.

No obstante, no es fácil implementar ese tipo de sistema. Si los aparatos de gestión de partes PA(1) a PA(N) ejecutan las operaciones usando los valores independientes σ(1) a σ(N), el aparato de adquisición no puede generar la información de generación SK por procesamiento de reconstrucción usando los resultados de las operaciones por los aparatos de gestión de partes como partes. Además, dado que el valor σ puede ser información a partir de cual se predice la información de generación SK, se prefiere desde la perspectiva de seguridad que todos los aparatos de gestión de partes PA(1) a PA(N) no comparten el valor σ en sí mismo.

En vista de ese punto, un objeto de la presente invención es implementar de manera segura un sistema que satisface las condiciones 1 a 3.

MEDIOS PARA RESOLVER LOS PROBLEMAS
En vista de los problemas anteriores, la presente invención proporciona un sistema de compartición de secretos, un aparato de compartición, un aparato de gestión de partes, un aparato de adquisición, un método de compartición de secretos, un método de procesamiento para un aparato de compartición, un método de procesamiento para un aparato de gestión de partes y un método de procesamiento para un aparato de adquisición que tiene los rasgos de las reivindicaciones independientes respectivas. Las realizaciones preferidas de la invención se describen en las reivindicaciones dependientes.

Según la presente invención, un aparato de compartición genera las partes SH(α, h(α)) por compartición de secretos de información secreta separadamente para cada uno de los subconjuntos SUB(α), cada uno de los subconjuntos SUB(α) que está formado de H(α) aparatos de gestión de partes PA(α, 1) a PA(α, H(α)) que pertenece a un conjunto de $\sum_{\alpha=1}^{L} h(\alpha)$ aparatos de gestión de partes PA(α, h(α)) (α = 1, …, L, L $\geq$ 2, h(α) = 1, …, H(α), H(α) $\geq$ 2) y saca las partes SH(α, h(α)). Cada uno de los aparatos de gestión de partes PA(α, h(α)) genera un valor de secreto compartido DSH(α, h(α)) realizando una operación común a la parte SH(α, h(α)) e información común que contiene un valor común σ(α) compartido en cada uno de los subconjuntos SUB(α) y saca el valor de secreto compartido DSH(α, h(α)). La información común usada por los generadores de valores de secretos compartidos de los aparatos de gestión de partes PA(α, h(α)) que pertenecen al mismo subconjunto SUB(α) es el mismo y los generadores de valores de secretos compartidos de los aparatos de gestión de partes PA(α, h(α)) que pertenecen al mismo subconjunto SUB(α) realizan la misma operación común.

Un aparato de adquisición genera valores de secretos reconstruidos SUBSK(α) que corresponden a los subconjuntos SUB(α) respectivamente. Cada uno de los valores de secretos reconstruidos SUBSK(α) se genera por procesamiento de reconstrucción para cada subconjunto SUB(α) usando una pluralidad de valores de secretos compartidos DSH(α, h(α)) que corresponden al mismo subconjunto SUB(α). El aparato de adquisición saca los valores de secretos reconstruidos SUBSK(α). El aparato de adquisición entonces genera información de generación SK usando los valores de secretos reconstruidos SUBSK(α) y saca la información de generación SK.

Según la presente invención, la información secreta se comparte secretamente separadamente para cada subconjunto SUB(α) y los valores de secretos compartidos DSH(α, h(α)) se generan usando información común que contiene un valor común σ(α) compartido en cada subconjunto SUB(α). Cada uno de los valores de secretos reconstruidos SUBSK(α) obtenidos por procesamiento de reconstrucción para cada subconjunto SUB(α)

llega a ser el mismo que el resultado de una operación que incluye la información secreta y la información común que contiene el valor común $\sigma(\alpha)$ como operandos. Por lo tanto, la información de generación SK generada usando los valores de secretos reconstruidos SUBSK(α) después de la reconstrucción puede ser la misma que el resultado de una operación que contiene la información secreta y un valor dado σ como operandos. Según la presente invención, no todos los aparatos de gestión de partes PA(α, h(α)) comparten el valor dado σ, de manera que se proporciona un alto nivel de seguridad.

EFECTOS DE LA INVENCIÓN

Como se describió anteriormente, según la presente invención, se puede implementar de manera segura un sistema que satisface las condiciones 1 a 3.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama de bloques que ilustra la estructura general de un sistema de compartición de secretos según una primera realización;

La Figura 2 es un diagrama de bloques que ilustra la estructura de un aparato de compartición en la Figura 1;

La Figura 3A es un diagrama de bloques que ilustra la estructura de un aparato de gestión de partes en la primera realización;

La Figura 3B es un diagrama de bloques que ilustra la estructura de un generador de valor común en la primera realización;

La Figura 4 es un diagrama de bloques que ilustra la estructura de un aparato de adquisición en la primera realización;

La Figura 5A es un diagrama de bloques que ilustra una unidad de compartición de secretos en la Figura 2 en detalle;

La Figura 5B es un diagrama de bloques que ilustra un generador de valores de secretos compartidos en la Figura 3A en detalle;

La Figura 6 es un diagrama de bloques que ilustra una unidad de reconstrucción en la Figura 4 en detalle;

La Figura 7 es una vista que ilustra el procesamiento de compartición de secretos entero en la primera realización;

La Figura 8A es una vista que ilustra un ejemplo de procesamiento en el aparato de compartición en la primera realización;

La Figura 8B es una vista que ilustra un ejemplo de procesamiento en el paso S112 en detalle;

La Figura 9A es una vista que ilustra un ejemplo de procesamiento en el aparato de gestión de partes en la primera realización;

La Figura 9B es una vista que ilustra un ejemplo de procesamiento en el paso S124 en detalle;

La Figura 10A es una vista que ilustra un ejemplo de procesamiento en el aparato de adquisición en la primera realización;

La Figura 10B es una vista que ilustra un ejemplo de procesamiento en el paso S134;

La Figura 11A es una vista que ilustra la estructura de una unidad de compartición de secretos en una primera modificación de la primera realización;

La Figura 11B es una vista que ilustra la estructura de un generador de valores de secretos compartidos en la primera modificación de la primera realización;

La Figura 12A es una vista que ilustra la estructura de un generador de valores de secretos compartidos en una segunda modificación de la primera realización;

La Figura 12B es una vista que ilustra la estructura de una unidad de reconstrucción en la segunda modificación de la primera realización;

La Figura 13A es una vista que ilustra la estructura de una unidad de compartición de secretos en una tercera modificación de la primera realización;

La Figura 13B es una vista que ilustra la estructura de un generador de valores de secretos compartidos en la tercera modificación de la primera realización;

La Figura 13C es una vista que ilustra la estructura de una unidad de reconstrucción en la tercera modificación de la primera realización;

La Figura 14A es una vista que ilustra la estructura de una unidad de compartición de secretos en una cuarta modificación de la primera realización;

La Figura 14B es una vista que ilustra la estructura de un generador de valores de secretos compartidos en la cuarta modificación de la primera realización;

La Figura 14C es una vista que ilustra la estructura de una unidad de reconstrucción en la cuarta modificación de la primera realización;

La Figura 15 es un diagrama de bloques que ilustra la estructura de un aparato de compartición según una segunda realización;

La Figura 16 es un diagrama de bloques que ilustra la estructura de un aparato de gestión de partes en la segunda realización;

La Figura 17 es un diagrama de bloques que ilustra la estructura de un aparato de adquisición en la segunda realización;

La Figura 18 es un diagrama de bloques que ilustra la estructura de una unidad de composición en la Figura 17;

La Figura 19 es una vista que ilustra el procesamiento de compartición de secretos entero en la segunda realización;
La Figura 20 es una vista que ilustra un ejemplo de procesamiento en el aparato de compartición en la segunda realización;
La Figura 21 es una vista que ilustra un ejemplo de procesamiento en el aparato de gestión de partes en la segunda realización; y
La Figura 22 es una vista que ilustra un ejemplo de procesamiento en el aparato de adquisición en la segunda realización.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES

Las realizaciones de la presente invención se describirán más adelante con referencia a los dibujos.

[Primera realización]

Se describirá primero una primera realización de la presente invención.

[Definiciones]

Se describirán primero los términos y símbolos a ser usados en la realización.

F_q: F_q representa un campo finito de orden q, donde q es un entero igual o mayor que 1. Por ejemplo, el orden q es un número primo de una potencia de un número primo. En otras palabras, el campo finito F_q es un campo primo o un campo de extensión sobre el campo primo, por ejemplo. Se pueden definir fácilmente operaciones en el campo finito primo F_q como operaciones de módulo con el orden q como módulo, por ejemplo. Se pueden definir fácilmente operaciones en el campo de extensión F_q definido como operaciones de módulo con un polinomio irreducible como módulo, por ejemplo. Se describe un método específico para configurar un campo finito F_q, por ejemplo, en la bibliografía de referencia 1, “ISO/IEC 18033-2: Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers”.

0_F: 0_F representa un elemento identidad aditivo del campo finito F_q.
1_F: 1_F representa un elemento identidad multiplicativo del campo finito F_q.
E: E representa una curva elíptica sobre el campo finito F_q. E se define como un conjunto que tiene un punto específico O llamado un punto en el infinito y otros puntos (x,y) de $x,y \in F_q$ que satisface la siguiente ecuación de Weierstrass en coordenadas afines:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

donde a_1, a_2, a_3, a_4, a_6, $\in F_q$. Una operación binaria “+” llamada una adición de curva elíptica se puede definir para cualesquiera dos puntos en la curva elíptica E y una operación unitaria “-“ llamada una inversa aditiva se puede definir para cualquier punto en la curva elíptica E. Es bien conocido que un conjunto finito de puntos racionales en la curva elíptica E forma un grupo con respecto a la adición de curva elíptica. También es bien conocido que una operación llamada una multiplicación escalar de curva elíptica se puede definir con la adición de curva elíptica. Un método de operación específica de operaciones elípticas tal como la adición de curva elíptica en un ordenador también es bien conocido. (Por ejemplo, ver la bibliografía de referencia 1, bibliografía de referencia 2, “RFC 5091: Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems” y la bibliografía de referencia 3, Ian F. Blake, Gadiel Seroussi y Nigel P. Smart, “Elliptic Curves in Cryptography”, Pearson Education, ISBN 4-89471-431-0).

Un conjunto finito de puntos racionales en la curva elíptica E tiene un subgrupo de orden p ($p \geq 1$). Por ejemplo, un conjunto finito E[p] de p puntos de división en la curva elíptica E forma un subgrupo de puntos racionales en la curva elíptica, donde #E representa el recuento de elementos del conjunto finito de los p puntos de división en la curva elíptica E y #E es divisible por el primo grande p. Los p puntos de división en la curva elíptica E son puntos A en la curva elíptica E que satisfacen la multiplicación escalar de curva elíptica $p \cdot A = O$.

G: G representa un grupo cíclico. Ejemplos del grupo cíclico G incluyen el conjunto finito E[p] de p puntos de división en la curva elíptica E, subgrupos de los mismos y grupos de residuos. En la realización, una operación definida en el grupo cíclico G se expresa aditivamente. Más específicamente, $\chi \cdot \Omega \in G$ para $\chi \in F_q$ y $\Omega \in G$ significa que la operación definida en el grupo cíclico G se aplica a $\Omega \in G$, χ veces y $\Omega_1 + \Omega_2 \in G$ para Ω_1, $\Omega_2 \in G$ significa que la operación definida en el grupo cíclico G se aplica a $\Omega_1 \in G$ y $\Omega_2 \in G$.
g: g representa un generador del grupo cíclico G.

[Estructura general]

La Figura 1 es un diagrama de bloques que ilustra la estructura general de un sistema de compartición de secretos 1 según una primera realización.

Como se ilustra en la Figura 1, el sistema de compartición de secretos 1 en esta realización incluye un aparato de compartición 110, $\sum_{\alpha=1}^{L} h(\alpha)$ aparatos de gestión de partes [PA(α , h(α)) (α = 1 a L, L $\geq$ 2, h(α) = 1 a H(α), H(α) $\geq$ 2] 120-α -h(α), un aparato de adquisición 130 y generadores de valores comunes 140-1 a 140-L y esas unidades se estructuran para permitir comunicación entre ellas a través de la red 150. En aras de la simplicidad, una estructura que incluye un único aparato de compartición 110 y un único aparato de adquisición 130 se describirán en esta realización aunque la estructura puede incluir dos o más aparatos de compartición 110 y/o dos o más aparatos de adquisición 130. Por la misma razón, se describirá en esta realización una estructura que incluye un único conjunto de $\sum_{\alpha=1}^{L} h(\alpha)$ aparatos de gestión de partes [PA(α , h(α))] 120-α -h(α), aunque se puede incluir una pluralidad de estos conjuntos.

Como se muestra en la Figura 1, el conjunto de $\sum_{\alpha=1}^{L} h(\alpha)$ aparatos de gestión de partes [PA(α , h(α))] 120-α -h(α) se divide en una pluralidad de subconjuntos SUB(α) que incluye H(α) aparatos de gestión de partes PA(α , 1) a PA(α , H(α)). Cada subconjunto SUB(α) corresponde a un generador de valor común 140-α para generar un valor σ (α) a ser compartido en cada subconjunto SUB(α).

[Aparato de compartición 110]
La Figura 2 es un diagrama de bloques que ilustra la estructura del aparato de compartición 110 en la Figura 1. La Figura 5A es un diagrama de bloques que ilustra una unidad de compartición de secretos 114-α en la Figura 2 en detalle.

Como se muestra en la Figura 2, el aparato de compartición 110 en esta realización incluye un almacenamiento temporal 111, un almacenamiento 112, un controlador 113, unidades de compartición de secretos 114-α (α = 1 a L) y un transmisor 115. Como se muestra en la Figura 5A, la unidad de compartición de secretos 114-α en esta realización incluye una unidad de selección de función 114a-α , un generador de índices 114b-α y una unidad de procesamiento de compartición 114c-α .

El aparato de compartición 110 en esta realización es un aparato especial que incluye un ordenador conocido o especializado dotado con una unidad central de proceso (CPU), una memoria de acceso aleatorio (RAM), una memoria solamente de lectura (ROM) y similares y un programa especial, por ejemplo. El almacenamiento temporal 111 y el almacenamiento 112 son, por ejemplo, un almacenamiento auxiliar tal como una RAM, un registro, una memoria caché, un dispositivo en un circuito integrado o un disco duro o un área de almacenamiento formada combinando al menos alguno de estos. El controlador 113 y las unidades de compartición de secretos 114-α (α = 1 a L) son unidades de procesamiento implementadas por la CPU ejecutando programas predeterminados, por ejemplo. Al menos una parte del controlador 113 y las unidades de compartición de secretos 114-α (α = 1 a L) se pueden implementar por un circuito integrado especializado. El transmisor 115 es un dispositivo de comunicación tal como un módem o una tarjeta de red de área local (LAN).

El aparato de compartición 110 ejecuta un procesamiento bajo el control del controlador 113. Cada parte de datos sacada desde cada unidad de procesamiento se almacena en el almacenamiento temporal 111 o en el almacenamiento 112 y una descripción de los mismos se simplificará más adelante. Los datos almacenados en el almacenamiento temporal 111 o el almacenamiento 112 se lee, introduce a una unidad de procesamiento y usa para procesamiento de los mismos, cuando sea necesario.

[Aparato de gestión de partes [PA(α , h(α))] 120-α -h(α)]
La Figura 3A es un diagrama de bloques que ilustra la estructura del aparato de gestión de partes PA(α , h(α))] 120-α -h(α) en la primera realización. La Figura 5B es un diagrama de bloques que ilustra un generador de valores de secretos compartidos 124-α -h(α) en la Figura 3A en detalle.

Como se muestra en la Figura 3A, cada uno de los aparatos de gestión de partes [PA(α , h(α))] 120-α -h(α) en esta realización incluye un almacenamiento temporal 121-α -h(α), un almacenamiento 122-α -h(α), un controlador 123-α -h(α), el generador de valores de secretos compartidos 124-α -h(α), un transmisor 125-α -h(α) y un receptor 126-α -h(α). Como se muestra en la Figura 5B, el generador de valores de secretos compartidos 124-α -h(α) incluye una unidad de operación lineal 124a-α -h(α) y una unidad de composición de valores de secretos compartidos 124b-α -h(α).

Cada uno de los aparatos de gestión de partes [PA(α , h(α))] 120-α -h(α) es un aparato especial que incluye un ordenador conocido o especializado dotado con una CPU, una RAM, una ROM y similares y un programa especial, por ejemplo. Más específicamente, el almacenamiento temporal 121-α -h(α) y el almacenamiento 122-α -h(α) son, por ejemplo, un almacenamiento auxiliar tal como una RAM, un registro, una memoria caché, un dispositivo en

un circuito integrado o un disco duro o un área de almacenamiento formada combinando al menos alguno de estos. El controlador 123-α -h(α) y el generador de valores de secretos compartidos 124-α -h(α) son unidades de procesamiento implementadas por la CPU que ejecuta programas predeterminados, por ejemplo. Al menos una parte del controlador 123-α -h(α) y el generador de valores de secretos compartidos 124-α - h(α) 114-α se pueden implementar por un circuito integrado especializado. El transmisor 125-α -h(α) y el receptor 126-α -h(α) son dispositivos de comunicación tales como un módem o una tarjeta LAN.

Cada uno de los aparatos de gestión de partes [PA(α , h(α))] 120-α -h(α) ejecuta un procesamiento bajo el control del controlador 123-α -h(α). Cada parte de datos sacada de cada unidad de procesamiento se almacena en el almacenamiento temporal 121-α -h(α) o el almacenamiento 122-α -h(α) y una descripción de los mismos se simplificará más adelante. Los datos almacenados en el almacenamiento temporal 121-α -h(α) o el almacenamiento 122-α -h(α) se leen, introducen a una unidad de procesamiento y usan para procesamiento de los mismos, cuando sea necesario.

[El generador de valor común 140-α]
La Figura 3B es un diagrama de bloques que ilustra la estructura de un generador de valor común 140-α en la primera realización.

Como se muestra en la Figura 3B, cada uno de los generadores de valores comunes 140-α en esta realización incluye un generador de números aleatorios 141-α y un transmisor 142-α . El generador de valor común 140-α en esta realización es una unidad especial que incluye un ordenador conocido o especializado dotado con una CPU, una RAM, una ROM y similares y un programa especial, por ejemplo y el generador de números aleatorios 141-α se puede implementar por un circuito integrado especializado.

[Aparato de adquisición 130]
La Figura 4 es un diagrama de bloques que ilustra la estructura del aparato de adquisición 130 en la primera realización. La Figura 6 es un diagrama de bloques que ilustra una unidad de reconstrucción 134-α en la Figura 4 en detalle.

Como se muestra en la Figura 4, el aparato de adquisición 130 en esta realización incluye un almacenamiento temporal 131, un almacenamiento 132, un controlador 133, unidades de reconstrucción 134-α (α = 1 a L), una unidad de composición 137, un transmisor 135 y un receptor 136. Como se muestra en la Figura 6, cada una de las unidades de reconstrucción 134-α incluye una unidad de cálculo de coeficientes 134a-α y una unidad de operación de polinomios 134b-α .

El aparato de adquisición 130 en esta realización es un aparato especial que incluye un ordenador conocido o especializado dotado con una CPU, una RAM, una ROM y similares y un programa especial, por ejemplo. Más específicamente, el almacenamiento temporal 131 y el almacenamiento 132 son, por ejemplo, un almacenamiento auxiliar tal como una RAM, un registro, una memoria caché, un dispositivo en un circuito integrado o un disco duro o un área de almacenamiento formada combinando al menos alguno de estos. El controlador 133, las unidades de reconstrucción 134-α y la unidad de composición 137 son unidades de procesamiento implementadas por la CPU que ejecuta programas predeterminados. Al menos una parte del controlador 133, las unidades de reconstrucción 134-α (α = 1 a L) y la unidad de composición 137 se pueden implementar por un circuito integrado especializado. El transmisor 135 y el receptor 136 son dispositivos de comunicación tales como un módem o una tarjeta LAN.

El aparato de adquisición 130 ejecuta un procesamiento bajo el control del controlador 133. Cada parte de datos sacada de cada unidad de procesamiento se almacena en el almacenamiento temporal 131 o almacenamiento 132 y la descripción se simplificará más adelante. Los datos almacenados en el almacenamiento temporal 131 o el almacenamiento 132 se leen, introducen a una unidad de procesamiento y usan para procesamiento de los mismos, cuando es necesario.

[Procesamiento de compartición de secretos]
El procesamiento de compartición de secretos en esta realización se describirá a continuación.

[Procesamiento preparatorio]
En el procesamiento preparatorio para procesamiento de compartición de secretos en esta realización, la información $\theta \in F_q$ para identificar la información secreta $\theta \cdot g \in G$ se almacena en el almacenamiento 112 del aparato de compartición 110.

[Procesamiento de compartición de secretos entero]
La Figura 7 es una vista que ilustra el procesamiento de compartición de secretos entero en la primera realización. El procesamiento de compartición de secretos entero en esta realización se describirá a continuación con referencia a la Figura 7.

En esta realización, el aparato de compartición 110 (Figura 1) primero genera las partes SH(α, h (α)) realizando una compartición de secretos de la información secreta $\theta \cdot g \in G$ separadamente para cada subconjunto SUB(α) y saca las partes SH(α, h (α)) (paso S11). Las partes SH(α, h (α)) se envían separadamente a través de la red 150 a los aparatos de gestión de partes [PA(α, h(α))] 120-α -h(α).

Cada uno de los aparatos de gestión de partes [PA(α, h(α))] 120-α -h(α) a los cuales se enviaron las partes SH(α, h (α)) genera un valor de secreto compartido DSH(α, h (α)) realizando una operación común predeterminada a la parte SH(α, h (α)) y una información común que incluye un valor común σ (α) compartido en cada subconjunto SUB(α) y saca el valor de secreto compartido DSH(α, h (α)) (paso S12).

En esta realización, los valores comunes σ (α) compartidos separadamente en diferentes subconjuntos SUB(α) son independientes unos de otros. Los aparatos de gestión de partes [PA(α, h(α))] 120-α -h(α) en el mismo subconjunto SUB(α) usan la misma información común. En particular, la información común usada como un ejemplo en esta realización contiene el valor común σ (α) y la información proporcionada w en común con todos los aparatos de gestión de partes [PA(α, h(α))] 120-α -h(α), proporcionados por los aparatos de adquisición 130. Los aparatos de gestión de partes [PA(α, h(α))] 120-α -h(α) que pertenecen al mismo subconjunto SUB(α) realizan la misma operación común. En esta realización, todas las operaciones comunes son la misma. La operación común en esta realización es una operación lineal.

Los valores de secretos compartidos DSH(α, h (α)) sacados por los aparatos de gestión de partes [PA(α, h(α))] 120-α -h(α) se envían separadamente a través de la red 150 al aparato de adquisición 130. El aparato de adquisición 130 genera un valor de secreto reconstruido SUBSK(α) por procesamiento de reconstrucción para cada subconjunto SUB(α) usando una pluralidad de valores de secretos compartidos DSH(α, h(α)) que corresponden al mismo subconjunto SUB(α) (paso S13).

El aparato de adquisición 130 entonces crea la información de generación SK usando los valores de secretos reconstruidos SUBSK(α) generados separadamente para los subconjuntos SUB(α) y saca la información de generación SK (paso S14). En esta realización, el aparato de adquisición 130 crea la información de generación SK realizando una combinación lineal de los valores de secretos reconstruidos SUBSK(α).

[Procesamiento (en el paso S11) en el aparato de compartición]
La Figura 8A es una vista que ilustra un ejemplo de procesamiento en el aparato de compartición en la primera realización. La Figura 8B es una vista que ilustra un ejemplo de procesamiento en el paso S112 en detalle. El procesamiento en el aparato de compartición 110 se describirá a continuación en detalle con referencia a esas figuras.

El controlador 113 del aparato de compartición 110 (Figura 2) especifica α = 1 y almacena el ajuste en el almacenamiento temporal 111 (paso S111). La información $\theta \in F_q$ para identificar la información secreta $\theta \cdot g \in G$ se lee a continuación desde el almacenamiento 112 e introduce a la unidad de compartición de secretos 114-α. La unidad de compartición de secretos 114-α comparte la información secreta $\theta \cdot g$ usando la información $\theta \in F_q$, genera H(α) partes SH(α, 1) a SH(α, H(α)) que corresponden al subconjunto SUB(α) y las saca (paso S112).

Detalles del paso S112:
La unidad de compartición de secretos 114-α en esta realización genera las partes SH(α, h(α)) realizando compartición de secretos de la información secreta para cada subconjunto SUB(α) usando un esquema de compartición de secretos de umbral (R(α), H(α)) (R(α) es una constante que satisface $2 \leq R(\alpha) < H(\alpha)$).

Como se muestra en la Figura 8B, la unidad de selección de función 114a-α en la unidad de compartición de secretos 114-α (Figura 5A) selecciona aleatoriamente un polinomio de grado de orden (R(α) – 1) $f(\alpha, x) \in F_q$ que satisface $f(\alpha, \omega) = \theta$ con respecto a un elemento predeterminado $\omega \in F_q$ de un campo finito F_q y lo saca (paso S112a), donde x es una variable formada por un elemento del campo finito F_q y un ejemplo del elemento $\omega \in F_q$ es 0_F.

El generador de índices 114b-α entonces genera los índices $\phi(h(\alpha)) \in F_q$ que corresponde a cada uno de h(α) = 1 a H(α) y los saca (paso S112b). Si los índices son $\phi(h(\alpha)) = h(\alpha) \in F_q$ o si los índices $\phi(h(\alpha)) \in F_q$ ya se han obtenido, se puede omitir el procesamiento en el paso S112.

La unidad de procesamiento de compartición 114c-α usa el polinomio $f(\alpha, x) \in F_q$ y los índices $\phi(h(\alpha)) \in F_q$

para generar las partes

$$SH(\alpha,\ h(\alpha)) = (\varphi(h(\alpha)),\ f(\alpha,\ \varphi(h(\alpha)))\cdot g \in G) \qquad (5)$$

y las saca (paso S112c, fin de la descripción detallada del paso S112).

El controlador 113 juzga si α almacenado en el almacenamiento temporal 111 es L (paso S113). Si no se juzga que α = L, el controlador 113 especifica α + 1 como un nuevo valor de α, almacena el ajuste en el almacenamiento temporal 111 (paso S114) y ejecuta el procesamiento en el paso S112 con el nuevo valor de α. Si se juzga en el paso S113 que α = L, las partes SH(α, h(α)) sacadas de las unidades de compartición de secretos 114-α se envían al transmisor 115. El transmisor 115 envía las partes SH(α, h(α)) a través de la red 150 a los aparatos de gestión de partes correspondientes [PA(α, h(α))] 120-α-h(α) (paso S115). La parte SH(1, 1) se envía al aparato de gestión de partes [PA(1, 1)] 120-1-1; la parte SH(1, 2) se envía al aparato de gestión de partes [PA(1, 2)] 120-1-2; …; la parte SH(L, H(L)) se envía al aparato de gestión de partes [PA(L, H(L))] 120-L-H(L).

[Procesamiento en generador de valor común]
El generador de valor común 140-α (Figura 3B) genera el valor común $\sigma(\alpha)$ compartido por los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) incluidos en el subconjunto SUB(α) que corresponde al generador de valor común 140-α. En esta realización se especifica un número aleatorio generado por el generador de números aleatorios 141-α como el valor común $\sigma(\alpha)$ y el transmisor 142-α envía el valor común $\sigma(\alpha)$ a los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) incluidos en el subconjunto SUB(α).

[Procesamiento (en el paso S12) en los aparatos de gestión de partes]
La Figura 9A es una vista que ilustra un ejemplo de procesamiento en los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) en la primera realización. La Figura 9B es una vista que ilustra un ejemplo de procesamiento en el paso S124 en detalle. El procesamiento en los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) en esta realización se describirá a continuación con referencia a esas figuras.

Cada uno de los receptores 126-α-h(α) de los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) (Figura 3A) recibe la parte enviada SH(α, h (α)) y la almacena en el almacenamiento 122-α-h(α) (paso S121). Si el procesamiento en el paso S121 fue ejecutado en el pasado y si la parte SH(α, h (α)) ya ha sido almacenada en el almacenamiento 122-α-h(α) del aparato de gestión de partes [PA(α, h(α))] 120-α-h(α), se puede omitir el procesamiento en el paso S121.

Cada uno de los receptores 126-α-h(α) de los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) también recibe el valor común $\sigma(\alpha)$ enviado desde cada uno de los generadores de valores comunes 140-α y lo almacena en cada uno de los almacenamientos 122-α-h(α) (paso S122).

En esta realización, la información proporcionada w leída desde el almacenamiento 132 del aparato de adquisición 130 (Figura 4) se envía desde el transmisor 135 a través de la red 150 a los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α). La información proporcionada w es común a todos los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α). La información proporcionada w se recibe por cada uno de los receptores 126-α-h(α) de los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) (Figura 3A) y se almacena en cada uno de los almacenamientos 122-α-h(α) (paso S123).

Cada uno de los generadores de valores de secretos compartidos 124-α-h(α) lee la parte SH(α, h(α)), el valor común $\sigma(\alpha)$ y la información proporcionada w desde cada uno del almacenamiento 122-α-h(α). Cada uno de los generadores de valores de secretos compartidos 124-α-h(α) genera un valor de secreto compartido DSH(α, h(α)) realizando una operación común FNC1 a la parte SH(α, h(α)) e información común que incluye el valor común $\sigma(\alpha)$ y la información proporcionada w y saca el valor de secreto compartido DSH(α, h(α)) (paso S124).

Detalles del paso S124:
La información común usada por los generadores de valores de secretos compartidos 124-α-h(α) de los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) en el mismo subconjunto SUB(α) es la misma y los generadores de valores de secretos compartidos 124-α-h(α) de los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) en el mismo subconjunto SUB(α) realizan la misma operación común. Las partes en esta realización se expresan por la Expresión (5).

Como se muestra en la Figura 9B, cada una de las unidades de operación lineal 124a-α-h(α) en los generadores de valores de secretos compartidos 124-α-h(α) en esta realización se da el valor común $\sigma(\alpha)$, la información

proporcionada w y f(α, ϕ(h(α)))·g en la parte SH(α, (h(α)) = (ϕ(h(α)), f(α, ϕ(h(α)))·g). La unidad de operación lineal 124a-α -h(α) realiza la operación dada por

$$dsh(\alpha,\ \varphi(h(\alpha))) = \sigma(\alpha)\cdot w\cdot f(\alpha,\ \varphi(h(\alpha)))\cdot g \in G \qquad (6)$$

y saca el resultado de la operación dsh(α, ϕ(h(α))) (paso S124a).

Cada resultado de operación de salida dsh(α, ϕ(h(α))) se introduce a cada una de las unidades de composición de valores de secretos compartidos 124b-α -h(α). Además, cada índice ϕ(h(α)) de la parte SH(α, (h(α)) = (ϕ(h(α)), f(α, ϕ(h(α)))·g) se introduce a cada f de las unidades de composición de valores de secretos compartidos 124b-α -h(α) y cada una de las unidades de composición de valores de secretos compartidos 124b-α -h(α) genera un valor de secreto compartido DSH(α, (h(α)) por la operación dada por

$$DSH(\alpha,h(\alpha)) = (\varphi(h(\alpha)),\ dsh(\alpha,\varphi(h(\alpha)))) \qquad (7)$$

y lo saca (paso S124b, fin de la descripción detallada del paso S124).

Cada valor de secreto compartido generado DSH(α, (h(α)) se envía a cada uno de los transmisores 125-α -h(α). Cada transmisor 125-α -h(α) envía el valor de secreto compartido DSH(α, (h(α)) a través de la red 150 al aparato de adquisición 130 (paso S125).

[Procesamiento (en los pasos S13 y S14) en el aparato de adquisición]
La Figura 10A es una vista que ilustra un ejemplo de procesamiento en los aparatos de adquisición en la primera realización y la Figura 10B es una vista que ilustra un ejemplo de procesamiento en el paso S134.

Los valores de secretos compartidos DSH(α, (h(α)) enviados desde los aparatos de gestión de partes [PA(α, h(α))] 120-α -h(α) se reciben por el receptor 136 en el aparato de adquisición 130 (Figura 4) y almacenan en el almacenamiento 132 (paso S131).

El controlador 133 juzga si el número de valores de secretos compartidos DSH(α, (h(α)) almacenados en el almacenamiento 132 es mayor o igual a un número requerido (paso S132). En esta realización, se juzga si R(α) (2 $\leq$ R(α) < H(α)) o mayor que diferentes valores de secretos compartidos DSH(α, (h(α)) se almacenan en el almacenamiento 132 con respecto a cada uno de α = 1 a L. Si no se juzga aquí que el número de valores de secretos compartidos DSH(α, (h(α)) almacenados en el almacenamiento 132 es mayor o igual al número requerido, el procesamiento vuelve al paso S131.

Si se juzga que el número de valores de secretos compartidos DSH(α, (h(α)) almacenados en el almacenamiento 132 es mayor o igual al número requerido, el controlador 133 especifica α = 1 y almacena el ajuste en el almacenamiento temporal 131 (paso S133). Entonces, el número requerido de los valores de secretos compartidos DSH(α, (h(α)), que corresponden al subconjunto SUB(α) se leen desde el almacenamiento 132 e introducen a la unidad de reconstrucción 134-α. La unidad de reconstrucción 134-α genera un valor de secreto reconstruido SUBSK(α) por un procesamiento de reconstrucción para cada subconjunto SUB(α) usando los valores de secretos compartidos de entrada DSH(α, (h(α)) y saca el valor de secreto reconstruido SUBSK(α) para cada subconjunto SUB(α) (paso S134).

Detalles del paso S134:
Los valores de secretos compartidos DSH(α, (h(α)) en esta realización se dan por la Expresión (7). La unidad de reconstrucción 134-α (Figura 6) da R(α) diferentes valores de secretos compartidos DSH(α, (h(α)) para cada valor de α. Los valores de secretos compartidos DSH(α, (h(α)) que corresponden a cada valor de α introducido a la unidad de reconstrucción 134-α se expresarán como sigue.

$$DSH(\alpha,\ \varphi_1(\alpha)) = (\varphi_1(\alpha),\ dsh(\alpha,\ \varphi_1(\alpha)))$$
$$\ldots \qquad (8)$$
$$DSH(\alpha,\ \varphi_{R(\alpha)}(\alpha)) = (\varphi_{R(\alpha)}(\alpha),\ dsh(\alpha,\ \varphi_{R(\alpha)}(\alpha))$$

donde

$$(\varphi_1(\alpha),\ \ldots,\ \varphi_{R(\alpha)}(\alpha)) \subset (\varphi(1),\ \ldots,\ \varphi(H(\alpha))) \qquad (9)$$

$$(dsh_1(\alpha),\ \ldots,\ dsh_{R(\alpha)}(\alpha)) \subset (dsh(\alpha,\ \varphi(1)),\ \ldots,\ dsh(\alpha,\ \varphi(H(\alpha))))$$

Como se muestra en la Figura 10B, los índices $\phi_1(\alpha)$ a $\phi_{R(\alpha)}(\alpha)$ de DSH(α, $\phi_1(\alpha)$) a DSH(α, $\phi_{R(\alpha)}(\alpha)$) dados por la Expresión (8) se introducen a la unidad de cálculo de coeficientes 134a-α y la unidad de cálculo de coeficientes 134a-α realiza la siguiente operación para cada valor de ρ = 1 a R(α).

$$\lambda_\rho(x) = \frac{(x-\phi_1(\alpha))\cdots\overset{\rho}{\vee}\cdots(x-\phi_{R(\alpha)}(\alpha))}{(\phi_\rho(\alpha)-\phi_1(\alpha))\cdots\overset{\rho}{\vee}\cdots(\phi_\rho(\alpha)-\phi_{R(\alpha)}(\alpha))} \in F_q \qquad (11)$$

Los coeficientes λ_ρ(x) (ρ = 1 a R(α)) se generan y sacan (paso S134a).

Los coeficientes generados λ_ρ(x) y $dsh_1(\alpha)$ a $dsh_{R(\alpha)}(\alpha)$ que corresponden a DSH(α, $\phi_1(\alpha)$) a DSH(α, $\phi_{R(\alpha)}(\alpha)$) dados por la Expresión (8) se introducen a la unidad de operación de polinomios 134b-α. La unidad de operación de polinomios 134b-α genera el valor de secreto reconstruido SUBSK(α) del subconjunto SUB(α) por la operación dada por

$$SUBSK(\alpha) = \lambda_1(\omega)\ y\ dsh_1(\alpha) + \ldots + \lambda_{R(\alpha)}(\omega)\cdot dsh_{R(\alpha)}(\alpha) \in G \qquad (12)$$

y lo saca (paso S134b, fin de la descripción detallada del paso S134).

Entonces, el controlador 133 juzga si α almacenado en el almacenamiento temporal 131 es L (paso S135). Si no se juzga que α = L, el controlador 133 especifica α + 1 como un nuevo valor de α, almacena el ajuste en el almacenamiento temporal 131 (paso S136) y ejecuta el procesamiento en el paso S134 con el nuevo valor de α.

Si se juzga en el paso S135 que α = L, los valores de secretos reconstruidos SUBSK(α) sacados de las unidades de reconstrucción 134-α se envían a la unidad de composición 137. La unidad de composición 137 genera la información de generación

$$SK = FNC2(SUBSK(1), \ldots, SUBSK(L)) \qquad (13)$$

usando los valores de secretos reconstruidos SUBSK(α) generados para los subconjuntos SUB(α) y saca la información de generación SK (paso S141).

Detalles del paso S141:

Se darán más adelante ejemplos de la Expresión (13).

Ejemplo 1:

$$SK = SUBSK(1) + \ldots + SUBSK(L) \in G \qquad (14)$$

Ejemplo 2:

$$SK = CE_1\cdot SUBSK(1) + \ldots + CE_L\cdot SUBSK(L) \in G \qquad (15)$$

donde $CE_\alpha \in F_q$ es un coeficiente y un ejemplo del coeficiente es el elemento inverso de multiplicación $(L)^{-1} \in F_q$ de L. Algunos de los coeficientes CE_1 a CE_L pueden ser 0_F. En ese caso, la información de generación SK se genera usando solo un término parcial de SUBSK(1) + … + SUBSK(L). La unidad de composición 137 puede seleccionar aleatoriamente que un coeficiente sea 0_F a partir de los coeficientes CE_1 a CE_L. Esto mejorará el nivel de seguridad. La unidad de composición 137 también se puede adaptar para especificar los coeficientes CE_1 a CE_L libremente.

Esto permite al aparato de adquisición 130 generar la información de generación SK sin usar los valores de secretos reconstruidos SUBSK(α') que corresponden a los subconjuntos SUB(α') que tienen un nivel de fiabilidad bajo, por ejemplo (fin de la descripción detallada del paso S141).

[Rasgos de la primera realización]
En esta realización, el aparato de compartición 110 genera las partes SH(α, (h(α)) realizando compartición de secretos de la información secreta θ·g $\in$ G para cada subconjunto SUB(α) separadamente; los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) generan los valores de secretos compartidos DSH(α, (h(α)) conduciendo la operación común, usando las partes SH(α, (h(α)) y la información común que incluye los valores comunes σ(α) y la información proporcionada w; el aparato de adquisición 13 genera los valores de secretos reconstruidos SUBSK(α) realizando el procesamiento de reconstrucción para cada subconjunto SUB(α), usando una pluralidad de valores de secretos compartidos DSH(α, (h(α)) que corresponden al mismo subconjunto SUB(α) y genera la información de generación SK usando los valores de secretos reconstruidos SUBSK(α).

Como se describió anteriormente, se usa el valor común σ(α) compartido en cada subconjunto SUB(α) y la compartición de secretos, la operación común y el procesamiento de reconstrucción se realizan para cada subconjunto SUB(α). Por lo tanto, son posibles todas estas partes de procesamiento. No todos los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) comparten el valor σ y el valor común σ(α) se comparte en cada uno de los subconjuntos SUB(α), de manera que se proporciona un alto nivel de seguridad. Especialmente, en esta realización, los valores comunes σ(α) compartidos en diferentes subconjuntos SUB(α) son independientes unos de otros. Esto asegura un alto nivel de seguridad.

En esta realización, todos los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) (α = 1 a L) realizan la misma operación común FNC1. La operación común FNC1 es lineal. Por lo tanto, en esta realización, generando la información de generación SK a través de una combinación lineal de los valores de secretos reconstruidos SUBSK(α), la información de generación SK generada usando los valores de secretos reconstruidos SUBSK(α) se puede hacer igual al resultado obtenido realizando la operación común FNC1 usando la información secreta θ·g y un valor σ dado como operandos.

Esta realización usa el esquema de compartición de secretos de umbral (R(α), H(α)) para compartición de secretos de la información secreta θ·g $\in$ G en cada subconjunto SUB(α). En este esquema, cada una de las partes SH(α, (h(α)) incluye un elemento f(α, ϕ(h(α)))·g $\in$ G de un grupo cíclico G, donde x representa una variable x que está formada de un elemento de un campo finito F_q, f(α, x) $\in$ F_q representa un polinomio de grado de orden (R(α) - 1) que satisface f(α, ω) = θ con respecto a un elemento predeterminado $\omega \in F_q$ del campo finito F_q y ϕ(h(α)) representa un índice que corresponde a h(α). La compartición de secretos de la información secreta θ·g $\in$ G, la cual es un elemento del grupo cíclico, evita que θ se escape incluso si la información secreta θ·g reconstruida a partir de las partes SH(α, (h(α)) se escapa, bajo la suposición de que es difícil resolver un problema logarítmico discreto en el grupo cíclico G. Esto proporciona un alto nivel de seguridad.

[Primera modificación de la primera realización]
Se describirá a continuación una primera modificación de la primera realización.

En la primera realización, un elemento del grupo cíclico G es una información secreta θ·g $\in$ G y la información secreta se comparte. Se puede compartir el elemento $\theta \in F_q$ del campo finito F_q. En ese caso, las partes SH(α, (h(α)) obtenidas por compartición de secretos usando el esquema de compartición de secretos de umbral (R(α), H(α)) incluyen un elemento f(α, ϕ(h(α))) $\in$ F_q del campo finito F_q donde una variable formada por un elemento del campo finito F_q es x, un polinomio de grado de orden (R(α) - 1) f(a, x) $\in$ F_q satisface f(α, ω) = θ con respecto a un elemento predeterminado $\omega \in F_q$ del campo finito F_q y un índice que corresponde a h(α) es ϕ(h(α)).

La Figura 11A es una vista que ilustra la estructura de una unidad de compartición de secretos 214-α en la primera modificación de la primera realización y la Figura 11B es una vista que ilustra la estructura de un generador de valores de secretos compartidos 224-α-h(α) en la primera modificación de la primera realización. En estas figuras, a componentes idénticos a aquellos en la primera realización se dan los mismos números de referencia que en la primera realización.

En la primera modificación de la primera realización, las unidades de compartición de secretos 114-α en la Figura

5A se sustituyen con las unidades de compartición de secretos 214-α ; y los generadores de valores de secretos compartidos 124-α -h(α) en la Figura 5B se sustituyen con los generadores de valores de secretos compartidos 224-α -h(α). Los otros componentes son los mismos que aquellos en la primera realización.

Modificación del paso S112 en la primera modificación de la primera realización
En la primera modificación de la primera realización, el procesamiento en el paso S112 ilustrado en la Figura 8B se modifica como sigue.

Los pasos S112a y S112b mostrados en la Figura 8B se ejecutan primero. Entonces, en lugar del paso S112c, cada una de las unidades de procesamiento de compartición 214c-α (Figura 11A) en la unidad de compartición de secretos 214-α genera las partes

$$SH(\alpha, h(\alpha)) = (\varphi(h(\alpha)), f(\alpha, \varphi(h(\alpha)))) \quad (16)$$

usando el polinomio $f(\alpha, x) \in F_q$ y el índice $\phi(h(\alpha)) \in F_q$ y las saca (fin de la descripción de la modificación del paso S112 en la primera modificación de la primera realización).

Modificación del paso S124 en la primera modificación de la primera realización:

En la primera modificación de la primera realización, el procesamiento en el paso S124 en la Figura 9B se modifica como sigue.

En lugar del paso S124a, a cada una de las unidades de operación lineal 224a-α -h(α) (Figura 11B) se da el valor común $\sigma(\alpha)$, la información proporcionada w y $f(\alpha, \phi(h(\alpha)))$ en la parte $SH(\alpha, h(\alpha)) = (\phi(h(\alpha)), f(\alpha, \phi(h(\alpha))))$ y realiza la operación dada por

$$dsh(\alpha, \varphi(h(\alpha))) = \sigma(\alpha) \cdot w \cdot f(\alpha, \varphi(h(\alpha))) \cdot g \in G \quad (17)$$

y saca el resultado $dsh(\alpha, \phi(h(\alpha))) \in G$. Cada resultado de operación $dsh(\alpha, \phi(h(\alpha))) \in G$ llega a ser una información parcial del valor de secreto compartido DSH(α , h(α)). Entonces, se ejecuta el procesamiento en el paso S124b mostrado en la Figura 9B (fin de la descripción de una modificación del paso S124 en la primera modificación de la primera realización). El otro procesamiento es el mismo que en la primera realización.

[Segunda modificación de la primera realización]
Se describirá a continuación una segunda modificación de la primera realización.

En la segunda modificación de la primera realización, el elemento $\theta \in F_q$ del campo finito F_q se comparte con un esquema de compartición de secretos también. Una diferencia de la primera modificación de la primera realización es que cada uno de los resultados de operación $dsh(\alpha, \phi(h(\alpha)))$ no es un elemento del grupo cíclico G sino que es un elemento del campo finito F_q.

La Figura 12A es una vista que ilustra la estructura de un generador de valores de secretos compartidos 324-α -h(α) en la segunda modificación de la primera realización y la Figura 12B es una vista que ilustra la estructura de una unidad de reconstrucción 334-α en la segunda modificación de la primera realización. En estas figuras, a componentes idénticos a aquellos en la primera realización se dan los mismos números de referencia que en la primera realización.

En la segunda modificación de la primera realización, los generadores de valores de secretos compartidos 124-α -h(α) en la Figura 5B se sustituyen con generadores de valores de secretos compartidos 324-α -h(α) y las unidades de reconstrucción 134-α en la Figura 6 se sustituyen con las unidades de reconstrucción 334-α . Como en la primera modificación de la primera realización, las unidades de procesamiento de compartición 114c-α en la Figura 5A se sustituyen con las unidades de procesamiento de compartición 214c-α . Los otros componentes son los mismos que en la primera realización.

Modificación del paso S112 en la segunda modificación de la primera realización:
Una modificación del paso S112 en la segunda modificación de la primera realización es la misma que la modificación del paso S112 en la primera modificación de la primera realización.

Modificación del paso S124 en la segunda modificación de la primera realización:

En la segunda modificación de la primera realización, el procesamiento en el paso S124 en la Figura 9B se modifica como sigue.

En lugar del paso S124a, a cada una de las unidades de operación lineal 324a-α-h(α) (Figura 12A) se da el valor común $\sigma(\alpha)$, la información proporcionada w y f(α, ϕ(h(α))) en la parte SH(α, h(α)) = (ϕ(h(α)), f(α, ϕ(h(α)))) y realiza la operación dada por

$$dsh(\alpha, \varphi(h(\alpha))) = \sigma(\alpha)\cdot w\cdot f(\alpha, \varphi(h(\alpha))) \in F_q \qquad (18)$$

y saca el resultado dsh(α, ϕ(h(α)))$\in$ F_q. Cada resultado de operación dsh(α, ϕ(h(α)))$\in$ F_q llega a ser una información parcial del valor de secreto compartido DSH(α, h(α)). Entonces, se ejecuta el procesamiento en el paso S124b mostrado en la Figura 9B.

Modificación del paso S134 en la segunda modificación de la primera realización:

Se ejecuta primero el procesamiento en el paso S134a mostrado en al Figura 10B. Entonces, en lugar del procesamiento en el paso S134b mostrado en al Figura 10B, a cada una de las unidades de operación de polinomios 334b-α (Figura 12B) se da los coeficientes $\lambda_p(x)$ y $dsh_1(\alpha)$ a $dsh_{R(\alpha)}(\alpha)$ de DSH(α, $\phi_1(\alpha)$) a DSH(α, $\phi_{R(\alpha)}(\alpha)$) dados por la Expresión (8) y genera un valor de secreto reconstruido SUBSK(α) del subconjunto SUB(α) por la operación dada más adelante

$$SUBSK(\alpha)$$

$$= \{\lambda_1(\omega)\cdot dsh_1(\alpha) + ... + \lambda_{R(\alpha)}(\omega)\cdot dsh_{R(\alpha)}(\alpha)\}\cdot g \in G \qquad (19)$$

y lo saca (fin de la descripción de la modificación del paso S134 en la segunda modificación de la primera realización). El otro procesamiento es el mismo que en la primera realización.

[Tercera modificación de la primera realización]
En una tercera modificación de la primera realización, la información secreta se comparte usando el esquema de compartición de secretos de umbral (H(α), H(α)) en lugar del esquema de compartición de secretos de umbral (R(α), H(α)).

La Figura 13A es una vista que ilustra la estructura de una unidad de compartición de secretos 414-α en la tercera modificación de la primera realización, la Figura 13B es una vista que ilustra la estructura de un generador de valores de secretos compartidos 424-α-h(α) en la tercera modificación de la primera realización y la Figura 13C es una vista que ilustra la estructura de una unidad de reconstrucción 434-α en la tercera modificación de la primera realización.

En la tercera modificación de la primera realización, las unidades de compartición de secretos 114-α en la Figura 5A se sustituyen con unidades de compartición de secretos 414-α, los generadores de valores de secretos compartidos 124-α-h(α) en la Figura 5B se sustituyen con los generadores de valores de secretos compartidos 424-α-h(α) y las unidades de reconstrucción 134-α en la Figura 6 se sustituyen con las unidades de reconstrucción 434-α. Los otros componentes son los mismos que en la primera realización.

Modificación del paso S112 en la tercera modificación de la primera realización:

En la tercera modificación de la primera realización, el procesamiento en el paso S112 mostrado en la Figura 8B se modifica como sigue.

Cada uno de los generadores de números aleatorios 414a-α en la unidad de compartición de secretos 414-α (Figura 13A) selecciona (H(α) – 1) elementos

$$SH(\alpha, 1), \ldots, SH(\alpha, H(\alpha)-1) \in G \qquad (20)$$

del grupo cíclico G aleatoriamente y los saca.

La información secreta θ.g$\in$ G y (H(α) – 1) elementos SH(α, 1) a SH(α, H(α)-1) $\in$ G del grupo cíclico G se introducen a una unidad de operación de elemento inverso 414b-α. La unidad de operación de elemento inverso

414b-α genera SH(α , h(α)) por la operación dada por

$$SH(\alpha , h(\alpha)) = \theta \cdot g - \{ SH(\alpha , 1) + \ldots + SH(\alpha , H(\alpha)-1)\} \in G \qquad (21)$$

y la saca.

Cada una de las unidades de compartición de secretos 414-α saca

$$SH(\alpha , 1), \ldots, SH(\alpha , H(\alpha)) \in G$$

como partes del subconjunto SUB(α). Estas partes satisfacen

$$SH(\alpha , 1) + SH(\alpha , 2) + \ldots + SH(\alpha , H(\alpha)) = \theta \cdot g \in G \qquad (22)$$

(fin de la descripción de una modificación del paso S112 en la tercera modificación de la primera realización).

Modificación del paso S124 en la tercera modificación de la primera realización:

En la tercera modificación de la primera realización, el procesamiento en el paso S124 mostrado en la Figura 9B se modifica como sigue.

A cada uno de los generadores de valores de secretos compartidos 424-α -h(α) (Figura 13B) se da el valor común σ (α), la información proporcionada w y las partes SH(α , 1) a SH(α , H(α)), genera los valores de secretos compartidos DSH(α , h(α)) por la operación dada por

$$DSH(\alpha , h(\alpha)) = \sigma (\alpha)\cdot w \cdot SH(\alpha , h(\alpha)) \in G \qquad (23)$$

y los saca (fin de la descripción de una modificación del paso S124 en la tercera modificación de la primera realización).

Modificación del paso S132 en la tercera modificación de la primera realización:
En la tercera modificación de la primera realización, el procesamiento en el paso S132 mostrado en la Figura 10A se modifica como sigue.

En la tercera modificación, el controlador 133 juzga si el número de valores de secretos compartidos DSH(α , h(α)) almacenados en el almacenamiento 132 es mayor o igual que un número requerido y el número requerido en la tercera modificación es H(α). En otras palabras, se juzga en la tercera modificación si todos los valores de secretos compartidos DSH(α , (h(α)) están almacenados en el almacenamiento 132 con respecto a cada uno de α = 1 a L.

Modificación del paso S134 en la tercera modificación de la primera realización:
En la tercera modificación de la primera realización, el procesamiento en el paso S134 mostrado en la Figura 10B se modifica como sigue.

El valor de secreto compartido DSH(α , (h(α)) en la tercera modificación se da por la Expresión (23). Todos los valores de secretos compartidos DSH(α , (h(α)) (h(α) = 1 a H(α)) que corresponden a α se introducen a la unidad de reconstrucción 434-α (Figura 13C). La unidad de reconstrucción 434-α entonces genera un valor de secreto reconstruido SUBSK(α) que corresponde al subconjunto SUB(α) por la operación dada por

$$SUBSK(\alpha) = DSH(\alpha , 1) + \ldots + DSH(\alpha , H(\alpha)) \in G \qquad (24)$$

y lo saca (fin de la descripción de la modificación del paso S134 en la tercera modificación de la primera realización). El otro procesamiento es el mismo que en la primera realización.

[Cuarta modificación de la primera realización]
También en una cuarta modificación de la primera realización, la información secreta se comparte usando el esquema de compartición de secretos de umbral (H(α), H(α)) en lugar del esquema de compartición de secretos de umbral (R(α), H(α)). Una diferencia con la tercera modificación es que la información secreta $\theta \in F_q$, la cual es un elemento del campo finito F_q, se comparte con el esquema de compartición de secretos.

La Figura 14A es una vista que ilustra la estructura de una unidad de compartición de secretos 514-α en la cuarta modificación de la primera realización; la Figura 14B es una vista que ilustra la estructura de un generador de

valores de secretos compartidos 524-α-h(α) en la cuarta modificación de la primera realización; y la Figura 14C es una vista que ilustra la estructura de una unidad de reconstrucción 534-α en la cuarta modificación de la primera realización.

En la cuarta modificación de la primera realización, las unidades de compartición de secretos 114-α en la Figura 5A se sustituyen con las unidades de compartición de secretos 514-α; los generadores de valores de secretos compartidos 124-α-h(α) en la Figura 5B se sustituyen con los generadores de valores de secretos compartidos 524-α-h(α); y las unidades de reconstrucción 134-α en la Figura 6 se sustituyen con las unidades de reconstrucción 534-α. Los otros componentes son los mismos que en la primera realización.

Modificación del paso S112 en la cuarta modificación de la primera realización:
En la cuarta modificación de la primera realización, el procesamiento en el paso S112 mostrado en la Figura 8B se modifica como sigue.

Cada uno de los generadores de números aleatorios 514a-α en la unidad de compartición de secretos 514-α (Figura 14A) selecciona (H(α) – 1) elementos

$$SH(\alpha, 1), \ldots, SH(\alpha, H(\alpha)-1) \in F_q \quad (25)$$

del elemento finito F_q aleatoriamente y los saca.

A cada una de la unidad de operación de elementos inversos 514b-α se da la información secreta $\theta \in F_q$ y los (H(α) – 1) elementos SH(α, 1) a SH(α, H(α)-1) $\in F_q$ del elemento finito F_q, genera SH(α, h(α)) por la operación dada por

$$SH(\alpha, h(\alpha)) = \theta - \{ SH(\alpha, 1) + \ldots + SH(\alpha, H(\alpha)-1)\} \in F_q \quad (26)$$

y la saca.

Cada una de la unidad de compartición de secretos 514-α saca

$$SH(\alpha, 1), \ldots, SH(\alpha, H(\alpha)) \in F_q \quad (27)$$

como partes del subconjunto SUB(α). Estas partes satisfacen

$$SH(\alpha, 1) + SH(\alpha, 2) + \ldots + SH(\alpha, H(\alpha)) = \theta \in F_q \quad (28)$$

(fin de la descripción de la modificación del paso S112 en la cuarta modificación de la primera realización).

Modificación del paso S124 en la cuarta modificación de la primera realización:
En la cuarta modificación de la primera realización, el procesamiento en el paso S124 mostrado en la Figura 9B se modifica como sigue.

A cada uno de los generadores de valores de secretos compartidos 524-α-h(α) (Figura 14B) se da el valor común $\sigma(\alpha)$, la información proporcionada w y las partes SH(α, 1) a SH(α, H(α)), genera un valor de secreto compartido DSH(α, h(α)) por la operación dada por

$$DSH(\alpha, h(\alpha)) = \sigma(\alpha) \cdot w \cdot SH(\alpha, h(\alpha)) \in F_q \quad (29)$$

y lo saca (fin de la descripción de una modificación del paso S124 en la cuarta modificación de la primera realización).

Modificación del paso S132 en la cuarta modificación de la primera realización:
La modificación del paso S132 en la cuarta modificación de la primera realización es la misma que en la tercera modificación de la primera realización.

Modificación del paso S134 en la cuarta modificación de la primera realización:

En la cuarta modificación de la primera realización, el procesamiento en el paso S134 mostrado en la Figura 10B se modifica como sigue.

El valor de secreto compartido DSH(α, h(α)) en la cuarta modificación se da por la Expresión (29). Todos los

valores de secretos compartidos DSH(α, (h(α)) (h(α) = 1 a H(α)) que corresponden a α se introducen a la unidad de reconstrucción 534-α que corresponden a α (Figura 14C). La unidad de reconstrucción 534-α entonces genera un valor de secreto reconstruido SUBSK(α) del subconjunto SUB(α) por la operación dada por

$$SUBSK(\alpha) = \{DSH(\alpha, 1) + \ldots + DSH(\alpha, H(\alpha))\} \cdot g \in G \quad (30)$$

y lo saca (fin de la descripción de la modificación del paso S134 en la cuarta modificación de la primera realización). El otro procesamiento es el mismo que en la primera realización.

[Otras modificaciones de la primera realización]
Se pueden hacer otras modificaciones de la primera realización dentro del alcance de la presente invención. Por ejemplo, la operación dada por

$$DSH(\alpha, h(\alpha)) = \sigma(\alpha) \cdot w \cdot SH(\alpha, h(\alpha)) \in F_q \quad (31)$$

se puede llevar a cabo en lugar de la Expresión (29) en la cuarta modificación de la primera realización y la operación de la Expresión (24) se puede llevar a cabo en lugar de la Expresión (30). El valor de secreto reconstruido SUBSK(α) puede ser un elemento del campo finito F_q.

En esta realización, se usa el mismo esquema de compartición de secretos en cada subconjunto SUB(α) para compartir un secreto. Se pueden usar diferentes esquemas de compartición de secretos para diferentes subconjuntos SUB.

El generador de valor común 140-α se proporciona para cada subconjunto SUB(α) en esta realización. Cualquier aparato de gestión de partes dado en cada subconjunto SUB(α) puede tener la función del generador de valor común. En ese caso, el generador de valor común 140-α llega a ser innecesario.

En esta realización, la operación común FNC1 se lleva a cabo usando las partes SH(α, h(α)) y la información común que contiene el valor común $\sigma(\alpha)$ y la información proporcionada w para generar el valor de secreto compartido DSH(α, h(α)). El valor de secreto compartido DSH(α, h(α)) se puede generar usando el valor común $\sigma(\alpha)$ como la información común sin usar la información proporcionada. La información común puede contener el valor común $\sigma(\alpha)$, la información proporcionada w y otra información.

La operación común para obtener los valores de secretos compartidos DSH(α, h(α)) debe ser la misma en cada subconjunto SUB(α). No obstante, diferentes subconjuntos SUB(α) no siempre necesitan llevar a cabo la misma operación común.

[Segunda Realización]
Se describirá a continuación una segunda realización de la presente invención. Esta realización es una aplicación de la primera realización para generación de claves en cifrado de predicado de producto interior.

[Definiciones]
Se definirán primero los términos y símbolos a ser usados en las realizaciones.

Matriz: Una matriz representa una disposición rectangular de elementos de un conjunto en el cual se definen unas operaciones. No solamente los elementos de un anillo sino también los elementos de un grupo pueden formar una matriz.

$(\cdot)^T$: $(\cdot)^T$ representa una matriz traspuesta de "$\cdot$".
$(\cdot)^{-1}$: $(\cdot)^{-1}$ representa una matriz inversa de "$\cdot$".
$\wedge$: $\wedge$ representa AND Lógica
$\vee$: $\vee$ representa OR Lógica
Z: Z representa un conjunto de enteros
k: k representa un parámetro de seguridad ($k \in Z, k > 0$)
F_q: F_q representa un campo finito de orden q, donde q es un entero igual o mayor que 1. Por ejemplo, el orden q es un número primo de una potencia de un número primo. En otras palabras, el campo finito F_q es un campo primo o un campo de extensión sobre el campo primo, por ejemplo.
0_F: 0_F representa un elemento identidad aditivo del campo finito F_q
1_F: representa un elemento identidad multiplicativo del campo finito F_q δ
(i,j): δ (i,j) representa una función delta de Kronecker. Cuando i = j, δ (i,j) = 1_F.
Cuando $i \neq j$, δ (i,j) = 0_F.
E: E representa una curva elíptica sobre el campo finito F_q.

G_1, G_2, G_T: G_1, G_2, G_T representan grupos cíclicos de orden q, respectivamente. Ejemplos de los grupos cíclicos G_1 y G_2 incluyen el conjunto finito E[p] de p puntos de división en la curva elíptica E y subgrupos de los mismos. G_1 puede ser igual a G_2 o G_1 puede no ser igual a G_2. Ejemplos del grupo cíclico G_T incluyen un conjunto finito que forma un campo de extensión del campo finito F_q. Un ejemplo específico del mismo es un conjunto finito de la raíz de orden p de 1 en el cierre algebraico del campo finito F_q.

En la realización, operaciones definidas en los grupos cíclicos G_1 y G_2 se expresan aditivamente y una operación definida en el grupo cíclico G_T se expresa multiplicativamente. Más específicamente, $\chi \cdot \Omega \in G_1$ para $\chi \in F_q$ y $\Omega \in G_1$ significa que la operación definida en el grupo cíclico G_1 se aplica a $\Omega \in G_1$, χ veces y $\Omega_1 + \Omega_2 \in G_1$ para Ω_1, $\Omega_2 \in G_1$ significa que la operación definida en el grupo cíclico G_1 se aplica a $\Omega_1 \in G_1$ y $\Omega_2 \in G_1$. De la misma forma, $\chi \cdot \Omega \in G_2$ para $\chi \in F_q$ y $\Omega \in G_2$ significa que la operación definida en el grupo cíclico G_2 se aplica a $\Omega \in G_2$, χ veces y $\Omega_1 + \Omega_2 \in G_2$ para Ω_1, $\Omega_2 \in G_2$ significa que la operación definida en el grupo cíclico G_2 se aplica a $\Omega_1 \in G_2$ y $\Omega_2 \in G_2$. Al contrario, $\Omega^{\chi} \in G_T$ para $\chi \in F_q$ y $\Omega \in G_T$ significa que la operación definida en el grupo cíclico G_T se aplica a $\Omega \in G_T$, χ veces y $\Omega_1 \cdot \Omega_2 \in G_T$ para Ω_1, $\Omega_2 \in G_T$ significa que la operación definida en el grupo cíclico G_T se aplica a $\Omega_1 \in G_T$ y $\Omega_2 \in G_T$.

n: n representa un entero igual o mayor que 1

ζ : ζ representa un entero igual o mayor que 1. Un ejemplo de ζ es 2 o 3.

$G_1^{n+\zeta}$: $G_1^{n+\zeta}$ representa un producto directo de (n + ζ) grupos críticos G_1.

$G_2^{n+\zeta}$: $G_2^{n+\zeta}$ representa un producto directo de (n + ζ) grupos críticos G_2.

g_1, g_2, g_T: g_1, g_2, g_T representa generadores de los grupos cíclicos G, G_1, G_2, G_T, respectivamente.

V: V representa un espacio de vector (n + ζ) dimensional formado del producto directo de los (n + ζ) grupos cíclicos G_1.

V*: V* representa un espacio de vector (n + ζ) dimensional formado del producto directo de los (n + ζ) grupos cíclicos G_2.

e: e representa una función (en lo sucesivo conocida como “función bilineal”) para calcular un mapa bilineal no degenerado que correlaciona el producto directo $G_1^{n+\zeta}$ x $G_2^{n+\zeta}$ del producto directo $G_1^{n+\zeta}$ y el producto directo $G_2^{n+\zeta}$ al grupo cíclico G_T. La función bilineal e saca un elemento del grupo cíclico G_T en respuesta a la entrada de (n + ζ) elementos γ_{β} (β = 1, …, n + ζ) del grupo cíclico G_1 y (n + ζ) elementos γ_{β}* (β = 1, …, n + ζ) del grupo cíclico G_2.

$$e: G_1^{n+\zeta} \times G_2^{n+\zeta} \rightarrow G_T \qquad (32)$$

La función bilineal e satisface las siguientes características:

- Bilinealidad: Las siguiente relación se satisface para todo $\Gamma_1 \in G_1^{n+\zeta}$, $\Gamma_2 \in G_2^{n+\zeta}$ y ν, $\kappa \in F_q$

$$e(\nu \cdot \Gamma_1, \kappa \cdot \Gamma_2) = e(\Gamma_1, \Gamma_2)^{\nu \cdot \kappa} \qquad (33)$$

- No degeneración: Esta función no correlaciona todo $\Gamma_1 \in G_1^{n+\zeta}$ y $\Gamma_2 \in G_2^{n+\zeta}$ sobre el elemento de identidad del grupo cíclico G_T.

- Computabilidad: Existe un algoritmo para calcular eficientemente e(Γ_1, Γ_2) para todo

$$\Gamma_1 \in G_1^{n+\zeta}, \Gamma_2 \in G_2^{n+\zeta} \qquad (34)$$

En la realización, la función bilineal e se forma siguiendo una función bilineal que correlaciona el producto directo G_1 x G_2 de los grupos cíclicos G_1 y G_2 al grupo cíclico G_T.

$$\text{Par:} \quad G_1 \times G_2 \rightarrow G_T \qquad (35)$$

La función bilineal e saca un elemento del grupo cíclico G_T en respuesta a un vector (n + ζ) dimensional de entrada

(γ_1, ..., $\gamma_{n+\zeta}$) formado de (n + ζ) elementos γ_β (β = 1, ..., n + ζ) del grupo cíclico G_1 y un vector (n + ζ) dimensional de entrada (γ_1*, ..., $\gamma_{n+\zeta}$*) formado de (n + ζ) elementos γ_β* (β = 1, ..., n + ζ) del grupo cíclico G_2.

$$e = \prod_{\beta=1}^{n+\zeta} \text{Par}(\gamma_\beta, \gamma_\beta^*) \quad (36)$$

La función bilineal Par saca un elemento del grupo cíclico G_T en respuesta a un elemento de entrada del grupo cíclico G_1 y un elemento de entrada del grupo cíclico G_2 y satisface las siguientes características:

- Bilinealidad: La siguiente relación se satisface para todo $\Omega_1 \in G_1$, $\Omega_2 \in G_2$, y ν, $\kappa \in F_q$

$$\text{Par}(\nu \cdot \Omega_1, \kappa \Omega_2) = \text{Par}(\Omega_1, \Omega_2)^{\nu \cdot \kappa} \quad (37)$$

- No degeneración: Esta función no correlaciona todo

$$\Omega_1 \in G_1 \text{ y } \Omega_2 \in G_2 \quad (38)$$

sobre el elemento identidad del grupo cíclico G_T.

- Computabilidad: Existe un algoritmo para calcular eficientemente Par(Ω_1, Ω_2) para todo $\Omega_1 \in G_1$, $\Omega_2 \in G_2$.

Un ejemplo específico de la función bilineal Par es una función para realizar una operación de cálculo de emparejamiento tal como un emparejamiento de Weil o un emparejamiento de Tate. (Ver la bibliografía de referencia 4, Alfred. J. Menezes, “Elliptic Curve Public Key Cryptosystems”, Kluwer Academic Publishers, ISBN 0-7923-9368-6, páginas 61-81, por ejemplo). Dependiendo del tipo de curva elíptica E, una función de emparejamiento e(Ω_1, phi(Ω_2)) ($\Omega_1 \in G_1$, $\Omega_2 \in G_2$) que es una combinación de una función predeterminada phi y la función para cálculo de emparejamiento tal como un emparejamiento de Tate se pueden usar como la función bilineal Par (ver la bibliografía de referencia 2, por ejemplo). Como el algoritmo para realizar un cálculo de emparejamiento en un ordenador, se puede usar el algoritmo de Miller (ver la bibliografía de referencia 5, V. S. Miller, “Short Programs for Functions on Curves”, 1986, http://crypto.stanford.edu/miller/miller.pdf) o algún otro algoritmo conocido. Los métodos de formación de un grupo cíclico y una curva elíptica para cálculo de emparejamiento eficaz han sido conocidos. (Por ejemplo, ver la bibliografía de referencia 2; la bibliografía de referencia 6, A. Miyaji, M. Nakabayashi, y S. Takano, “New Explicit Conditions of Elliptic Curve Traces for FR Reduction”, IEICE Trans. Fundamentals, Vol. E84-A, Nº 5, páginas 1234-1243, mayo de 2001, la bibliografía referencia 7, P. S. L. M. Barreto, B. Lynn, M. Scott, “Constructing Elliptic Curves with Prescribed Embedding Degrees”, Actas SCN ‘2002, LNCS 2576, páginas 257-267, Springer-Verlag. 2003; y la bibliografía referencia 8, R. Dupont, A. Enge, F. Morain, “Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields”, http//eprint.iacr.org/2002/094/.

- a_i (i = 1, ..., n + ζ): a_i (i = 1, ..., n + ζ) representa unos vectores de base (n + ζ) dimensional que tiene (n + ζ) elementos del grupo cíclico G_1 como elementos.

Por ejemplo, cada uno de los vectores de base a_i es el vector (n + 1) dimensional en el que el elemento i-dimensional es $\kappa_1 \cdot g_1 \in G_1$ y los elementos restantes son elementos identidad (cada uno de los cuales se expresa aditivamente como “0”) del grupo cíclico G_1. En ese caso, los elementos de los vectores de base (n + ζ) dimensional a_i (i = 1, ..., n + ζ) se pueden enumerar como sigue:

$$a_1 = (\kappa_1 \cdot g_1, 0, 0, \ldots, 0)$$

$$a_2 = (0, \kappa_1 \cdot g_1, 0, \ldots, 0) \quad (39)$$

……

$$a_{n+\zeta} = (0, 0, 0, \ldots, \kappa_1 \cdot g_1)$$

Aquí, κ_1 es una constante que es un elemento del campo finito F_q distinto del elemento identidad aditivo 0_F. Un ejemplo de $\kappa_1 \in F_q$ es $\kappa_1 = 1_F$. Los vectores de base a_i son bases ortogonales. Cada vector (n + ζ) dimensional

que tiene (n + ζ) elementos del grupo cíclico G_1 como elementos se expresa por una combinación lineal de los vectores de base (n + ζ) dimensionales a_i (i = 1, …, n + ζ). Es decir, los vectores de base (n + ζ) dimensionales a_i extienden el espacio de vector V, descrito anteriormente.

a_i^* (i = 1, …, n + ζ): a_i^* (i = 1, …, n + ζ) representa los vectores de base (n + ζ) dimensionales que tienen (n + ζ) elementos del grupo cíclico G_2 como elementos. Por ejemplo, cada uno de los vectores de base a_i^* es el vector (n + ζ) dimensional en el que el elemento de orden i es $\kappa_2 \cdot g_2 \in G_2$ y los elementos restantes son elementos identidad (cada uno de los cuales se expresa aditivamente como “0”) del grupo cíclico G_2. En ese caso, los elementos de los vectores de base a_i* (i = 1, …, n + ζ) se pueden enumerar como sigue:

$$a_1^* = (\kappa_2 \cdot g_2, 0, 0, \ldots, 0)$$

$$a_2^* = (0, \kappa_2 \cdot g_2, 0, \ldots, 0) \qquad (40)$$

……

$$a_{n+\zeta}^* = (0, 0, 0, \ldots, \kappa_2 \cdot g_2)$$

Aquí, κ_2 es una constante que es un elemento del campo finito F_q distinto del elemento identidad aditivo 0_F. Un ejemplo de $\kappa_2 \in F_q$ es $\kappa_2 = 1_F$. Los vectores de base a_i* son bases ortogonales. Cada vector (n + ζ) dimensional que tiene (n + ζ) elementos del grupo cíclico G_2 como elementos se expresa por una combinación lineal de los vectores de base (n + ζ) dimensionales a_i^* (i = 1, …, n + ζ). Es decir, los vectores de base (n + ζ) dimensionales a_i* extienden el espacio de vector V*, descrito anteriormente.

Los vectores de base a_i y los vectores de base a_i* satisfacen la siguiente expresión para un elementos $\tau = \kappa_1 \cdot \kappa_2$ del campo finito F_q distinto de 0_F.

$$e(a_i, a_j^*) = g_T^{\tau\delta(i,j)} \qquad (41)$$

Cuando i = j, se satisface la siguiente expresión a partir de las Expresiones (36) y (37).

$$e(a_i, a_j^*) = Par(\kappa_1 \cdot g_1, \kappa_2 \cdot g_2) \cdot Par(0, 0) \cdot \ldots \cdot Par(0, 0)$$

$$= Par(g_1, g_2)^{\kappa_1 \kappa_2} \cdot Par(g_1, g_2)^{0 \cdot 0} \cdot \ldots \cdot Par(g_1, g_2)^{0 \cdot 0}$$

$$= Par(g_1, g_2)^{\kappa_1 \kappa_2} = g_T^{\tau}$$

Cuando i ≠ j, el lado derecho de $e(a_i, a_j^*) = \prod_{i=1}^{n+\zeta}$ Par (a_i, a_j^*) no incluye Par($\kappa_1 \cdot g_1$, $\kappa_2 \cdot g_2$) y es el producto de Par($\kappa_1 \cdot g_1$, 0), Par(0, $\kappa_2 \cdot g_2$) y Par(0, 0). Además, se satisface la siguiente expresión a partir de la Expresión (37).

$$Par(g_1, 0) = Par(0, g_2) = Par(g_1, g_2)^0$$

Por lo tanto, cuando i ≠ j, se satisface la siguiente expresión.

$$e(a_i, a_j^*) = e(g_1, g_2)^0 = g_T^0$$

Especialmente cuando $\tau = \kappa_1 \cdot \kappa_2 = 1_F$ (por ejemplo, $\kappa_1 = \kappa_2 = 1_F$), se satisface la siguiente expresión.

$$e(a_i, a_j^*) = g_T^{\delta(i,j)} \qquad (42)$$

Aquí, $g_T^0 = 1$ es el elemento identidad del grupo cíclico G_T y $g_T^1 = g_T$ es un generador del grupo cíclico G_T. En ese caso, los vectores de base a_i y los vectores de base a_i* son bases ortogonales normales duales y el espacio de vector V y el espacio de vector V* son un espacio de vector dual en el que se puede definir la correlación bilineal (espacio de vector de emparejamiento dual (DPVS)).

A: “A” representa una matriz de (n + ζ) filas por (n + ζ) columnas que tiene los vectores de base a_i (i = 1, …, n +

ζ) como elementos. Cuando los vectores de base a_i (i = 1, ..., n + ζ) se expresan por la Expresión (39), por ejemplo, la matriz A es como sigue:

$$A = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} \kappa_1 \cdot g_1 & 0 & \cdots & 0 \\ 0 & \kappa_1 \cdot g_1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_1 \cdot g_1 \end{pmatrix} \qquad (43)$$

A*: "A*" representa una matriz de (n + ζ) filas por (n + ζ) columnas que tiene los vectores de base a_i* (i = 1, ..., n + ζ) como elementos. Cuando los vectores de base a_i* (i = 1, ..., n + ζ) se expresan por la Expresión (40), por ejemplo, la matriz A* es como sigue:

$$A^* = \begin{pmatrix} a_1^* \\ a_2^* \\ \vdots \\ a_{n+1}^* \end{pmatrix} = \begin{pmatrix} \kappa_2 \cdot g_2 & 0 & \cdots & 0 \\ 0 & \kappa_2 \cdot g_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_2 \cdot g_2 \end{pmatrix} \qquad (44)$$

X: X representa una matriz de (n + ζ) filas por (n + ζ) columnas que tiene elementos del campo finito F_q como entradas. La matriz X se usa para transformación de coordenadas de los vectores de base a_i. La matriz X se expresas como $\chi_{i,j} \in F_q$, la matriz X es como sigue:

$$X = \begin{pmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,n+\zeta} \\ \chi_{2,1} & \chi_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+\zeta,1} & \chi_{n+\zeta,2} & \cdots & \chi_{n+\zeta,n+\zeta} \end{pmatrix} \qquad (45)$$

donde cada $\chi_{i,j} \in F_q$ es la entrada en la fila de orden i y la columna de orden j (i=1, ..., n+1, j=1, ..., n+1) de la matriz X.

Aquí, cada entrada $\chi_{i,j}$ de la matriz X se llama coeficiente de transformación.

X*: X* representa la matriz traspuesta de la matriz inversa de la matriz X. $X^* = (X^{-1})^T$. La matriz X* se usa para transformación de coordenadas de los vectores de base a_i*. La matriz X* es como sigue:

$$X^* = \begin{pmatrix} \chi_{1,1}^* & \chi_{1,2}^* & \cdots & \chi_{1,n+\zeta}^* \\ \chi_{2,1}^* & \chi_{2,2}^* & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+\zeta,1}^* & \chi_{n+\zeta,2}^* & \cdots & \chi_{n+\zeta,n+\zeta}^* \end{pmatrix} \qquad (46)$$

donde cada $\chi_{i,j}^* \in F_q$ es la entrada en la fila de orden i y la columna de orden j de la matriz X*.

Aquí, cada entrada $\chi_{i,j}^*$ de la matriz X* se llama coeficiente de transformación.

En ese caso, se satisface $X \cdot (X^*)^T = I$, donde "I" representa una matriz unidad de (n + 1) filas por (n + 1) columnas. En otras palabras, la matriz unidad se expresa como sigue.

$$I = \begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix} \qquad (47)$$

Se satisface la siguiente expresión.

$$\begin{pmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,n+\zeta} \\ \chi_{2,1} & \chi_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+\zeta,1} & \chi_{n+\zeta,2} & \cdots & \chi_{n+\zeta,n+\zeta} \end{pmatrix} \cdot \begin{pmatrix} \chi_{1,1}^* & \chi_{2,1}^* & \cdots & \chi_{n+\zeta,1}^* \\ \chi_{1,2}^* & \chi_{2,2}^* & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{1,n+\zeta}^* & \chi_{2,n+\zeta}^* & \cdots & \chi_{n+\zeta,n+\zeta}^* \end{pmatrix} \qquad (48)$$
$$= \begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix}$$

Aquí, los vectores (n + ζ) dimensionales se definirán más adelante.

$$\vec{\chi_i} = (\chi_{i,1}, \ldots, \chi_{i,n+\zeta}) \qquad (49)$$

$$\vec{\chi_j} = (\chi_{j,1}^*, \ldots, \chi_{j,n+\zeta}^*) \qquad (50)$$

El producto interior de los vectores (n + ζ) dimensionales $\vec{\chi_i}$ y $\vec{\chi_j}^*$ satisface la siguiente expresión a partir de la Expresión (48).

$$\vec{\chi_i} \cdot \vec{\chi_j}^* = \delta(i, j) \qquad (51)$$

b_i: b_i representa vectores de base (n + ζ) dimensionales que tienen (n + ζ) elementos del grupo cíclico G_1 como elementos. Los vectores de base b_i se obtiene por transformación de coordenadas de los vectores de base a_i (i = 1, …, n + 1) con la matriz X. Es decir, los vectores de base b_i se obtienen por el siguiente cálculo

$$b_i = \sum_{j=1}^{n+\zeta} \chi_{i,j} \cdot a_j \qquad (52)$$

Cuando los vectores de base a_j (j = 1, …, n + ζ) se expresan por la Expresión (39), cada elemento de los vectores de base b_i se muestra más adelante.

$$b_i = (\chi_{i,1} \cdot \kappa_1 \cdot g_1, \chi_{i,2} \cdot \kappa_1 \cdot g_1, \ldots, \chi_{i,n+\zeta} \cdot \kappa_1 \cdot g_1) \qquad (53)$$

Cada vector (n + ζ) dimensional que tiene (n + ζ) elementos del grupo cíclico G_1 como elementos se expresa por una combinación lineal de los vectores de base (n + ζ) dimensionales b_i (i = 1, …, n + ζ). Es decir, los vectores de base (n + ζ) dimensionales b_i expanden el espacio de vector V, descrito anteriormente.

b_i^*: b_i^* representa los vectores de base (n + ζ) dimensional que tienen (n + ζ) elementos del grupo cíclico G_2 como elementos. Los vectores de base b_i^* se obtienen por transformación de coordenadas de los vectores de base a_i^* (i = 1, …, n + ζ) con la matriz X*. Es decir, los vectores de base b_i^* se obtienen por el siguiente cálculo

$$b_i^* = \sum_{j=1}^{n+\zeta} \chi_{i,j}^* \cdot a_j^* \qquad (54)$$

Cuando los vectores de base a_j (j = 1, …, n + ζ) se expresan por la Expresión (40), cada elemento de los vectores de base b_i^* se muestran más adelante.

$$b_i^* = (\chi_{i,1}^* \cdot \kappa_2 \cdot g_2,\ \chi_{i,2}^* \cdot \kappa_2 \cdot g_2,\ \ldots,\ \chi_{i,n+\zeta}^* \cdot \kappa_2 \cdot g_2) \qquad (55)$$

Cada vector (n + ζ) dimensional que tiene (n + ζ) elementos del grupo cíclico G_2 como elementos se expresa por una combinación lineal de los vectores de base (n + ζ) dimensionales b_i^* (i = 1, …, n + ζ). Es decir, los vectores de base (n + ζ) dimensionales b_i^* expanden el espacio de vector V*, descrito anteriormente.

Los vectores de base b_i y los vectores de base b_i^* satisfacen la siguiente expresión para los elementos $\tau = \kappa_1 \cdot \kappa_2$ del campo finito F_q distinto de 0_F:

$$e(b_i, b_j^*) = g_T^{\tau \delta(i,j)} \qquad (56)$$

La siguiente expresión se satisface a partir de las Expresiones (36), (51), (53) y (55).

$$\begin{aligned}
e(b_i, b_j^*) &= \prod_{\beta=1}^{n+\zeta} \mathbf{Par}(\chi_{i,\beta} \cdot \kappa_1 \cdot g_1, \chi_{j,\beta}^* \cdot \kappa_2 \cdot g_2) \\
&= \mathbf{Par}(\chi_{i,1} \cdot \kappa_1 \cdot g_1, \chi_{j,1}^* \cdot \kappa_2 \cdot g_2) \cdot \ldots \cdot (\chi_{i,n} \cdot \kappa_1 \cdot g_1, \chi_{j,n}^* \cdot \kappa_2 \cdot g_2) \\
&\times \mathbf{Par}(\chi_{j,n+1} \cdot \kappa_1 \cdot g_1, \chi_{j,n+1}^* \cdot \kappa_2 \cdot g_2) \cdot \ldots \cdot \mathbf{Par}(\chi_{j,n+\zeta} \cdot \kappa_1 \cdot g_1, \chi_{j,n+\zeta}^* \cdot \kappa_2 \cdot g_2) \\
&= \mathbf{Par}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,1} \cdot \chi_{j,1}^*} \cdot \ldots \cdot \mathbf{Par}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,2} \cdot \chi_{j,2}^*} \\
&\quad \times \mathbf{Par}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,n+1} \cdot \chi_{j,n+1}^*} \cdot \ldots \cdot \mathbf{Par}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,n+\zeta} \cdot \chi_{j,n+\zeta}^*} \\
&= \mathbf{Par}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 (\chi_{i,1} \cdot \chi_{j,1}^* + \chi_{i,2} \cdot \chi_{j,2}^* + \ldots + \chi_{i,n+1} \cdot \chi_{j,n+1}^* + \ldots + \chi_{i,n+\zeta} \cdot \chi_{j,n+\zeta}^*)} \\
&= \mathbf{Par}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \vec{\chi_i} \cdot \vec{\chi_j}^*} \\
&= \mathbf{Par}(g_1, g_2)^{\tau \cdot \delta(i,j)} = g_T^{\tau \cdot \delta(i,j)}
\end{aligned}$$

Especialmente cuando $\tau = \kappa_1 \cdot \kappa_2 = 1_F$ (por ejemplo, $\kappa_1 = \kappa_2 = 1_F$), se satisface la siguiente expresión.

$$e(b_i, b_j^*) = g_T^{\delta(i,j)} \qquad (57)$$

En ese caso, los vectores de base b_i y los vectores de base b_i^* son la base ortogonal normal dual de un espacio de vector de emparejamiento dual (el espacio de vector V y el espacio de vector V*).

Siempre que se satisface la Expresión (56), se pueden usar los vectores de base a_i y a_i^* distintos de los mostrados en las Expresiones (39) y (40) como ejemplos y los vectores de base b_i y b_i^* distintos de los mostrados en las Expresiones (52) y (54) como ejemplos.

B: B representa una matriz de (n + ζ) filas por (n + ζ) columnas que tiene los vectores de base b_i (i = 1, …, n + ζ) como elementos. Se satisface B = X·A. Cuando los vectores de base b_i se expresan por la Expresión (53), por ejemplo, la matriz B es como sigue:

$$B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n+\zeta} \end{pmatrix} = \begin{pmatrix} \chi_{1,1} \cdot \kappa_1 \cdot g_1 & \chi_{1,2} \cdot \kappa_1 \cdot g_1 & \cdots & \chi_{1,n+\zeta} \cdot \kappa_1 \cdot g_1 \\ \chi_{2,1} \cdot \kappa_1 \cdot g_1 & \chi_{2,2} \cdot \kappa_1 \cdot g_1 & & \vdots \\ \vdots & & \ddots & \chi_{n+\zeta-1,n+\zeta} \cdot \kappa_1 \cdot g_1 \\ \chi_{n+\zeta,1} \cdot \kappa_1 \cdot g_1 & \cdots & \chi_{n+\zeta,n+\zeta-1} \cdot \kappa_1 \cdot g_1 & \chi_{n+\zeta,n+\zeta} \cdot \kappa_1 \cdot g_1 \end{pmatrix} \quad (58)$$

B*: B* representa una matriz de (n + ζ) filas por (n + ζ) columnas que tiene los vectores de base b_i^* (i = 1, …, n + ζ) como elementos. Se satisface B* = X*·A*. Cuando los vectores de base b_i^* (i = 1, …, n + ζ) se expresan por la Expresión (55), por ejemplo, la matriz B* es como sigue:

$$B^* = \begin{pmatrix} b_1^* \\ b_2^* \\ \vdots \\ b_{n+\zeta}^* \end{pmatrix} = \begin{pmatrix} \chi_{1,1}^* \cdot \kappa_2 \cdot g_2 & \chi_{1,2}^* \cdot \kappa_2 \cdot g_2 & \cdots & \chi_{1,n+\zeta}^* \cdot \kappa_2 \cdot g_2 \\ \chi_{2,1}^* \cdot \kappa_2 \cdot g_2 & \chi_{2,2}^* \cdot \kappa_2 \cdot g_2 & & \vdots \\ \vdots & & \ddots & \chi_{n+\zeta-1,n+\zeta}^* \cdot \kappa_2 \cdot g_2 \\ \chi_{n+\zeta,1}^* \cdot \kappa_2 \cdot g_2 & \cdots & \chi_{n+\zeta,n+\zeta-1}^* \cdot \kappa_2 \cdot g_2 & \chi_{n+\zeta,n+\zeta}^* \cdot \kappa_2 \cdot g_2 \end{pmatrix} \quad (59)$$

$\vec{w}$: $\vec{w}$ representa un vector n dimensional que tiene elementos del campo finito F_q como elementos.

$$\vec{w} = (w_1, \ldots, w_n) \in F_q^n \quad (60)$$

w_μ: w_μ representa el elemento de orden μ (μ = 1, …, n) del vector n dimensional.

$\vec{v}$: $\vec{v}$ representa un vector n dimensional que tiene elementos del campo finito F_q como elementos.

$$\vec{v} = (v_1, \ldots, v_n) \in F_q^n \quad (61)$$

v_μ: v_μ representa el elemento de orden μ (μ = 1, …, n) del vector n dimensional.

[Cifrado de predicado del producto interior]
El esquema básico del cifrado de predicado del producto interior se describirá más adelante.

[Cifrado de predicado]
En el cifrado de predicado (algunas veces llamado cifrado de función), un texto cifrado se puede descifrar cuando una combinación de una información de atributo y una información de predicado hace verdadera una fórmula lógica predeterminada. Una de la información de atributo y la información de predicado se incorpora en el texto cifrado y la otra se incorpora en la información de clave. El cifrado de predicado convencional se describe, por ejemplo, en la bibliografía de referencia 9, Jonathan Katz, Amit Sahai y Brent Waters, “Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products”, uno de los cuatro documentos de Eurocrypt 2008 invitados por la Journal of Cryptology.

[Cifrado de predicado del producto interior]
En el cifrado de predicado del producto interior, un texto cifrado se puede descifrar cuando el producto interior de la información de atributo y la información de predicado que son vectores es cero. En el cifrado de predicado del producto interior, un producto interior de cero es equivalente a la fórmula lógica de verdadero.

[Relación entre fórmula lógica y polinomio]
En el cifrado de predicado del producto interior, la fórmula lógica formada de una(s) OR lógica(s) y/o una(s) AND lógica(s) se expresa por un polinomio.

La OR lógica $(x = \eta_1) \vee (x = \eta_2)$ de una proposición 1 que indica que x es η_1 y una proposición 2 que indica que x es η_2 se expresa por el siguiente polinomio.

$$(x - \eta_1)\cdot(x - \eta_2) \qquad (62)$$

Entonces, las relaciones entre valores verdaderos y los valores de función de la Expresión (62) se muestran en la siguiente tabla.

Tabla 1

Proposición 1 $(x = \eta_1)$	Proposición 2 $(x = \eta_2)$	OR lógica $(x = \eta_1) \vee (x = \eta_2)$	Valor de función $(x = \eta_1)\cdot(x = \eta_2)$
Verdadera	Verdadera	Verdadera	0
Verdadera	Falsa	Verdadera	0
Falsa	Verdadera	Verdadera	0
Falsa	Falsa	Falsa	Distinto de 0

Como se entiende a partir de la Tabla 1, cuando la OR lógica $(x = \eta_1) \vee (x = \eta_2)$ es verdadera, el valor de función de la Expresión (62) es cero; y cuando la OR lógica $(x = \eta_1) \vee (x = \eta_2)$ es falsa, el valor de función de la Expresión (62) es un valor distinto de cero. En otras palabras, la OR lógica $(x = \eta_1) \vee (x = \eta_2)$ de verdadera es equivalente al valor de función de cero en la Expresión (62). Por lo tanto, la OR lógica se puede expresar por la Expresión (62).
La AND lógica $(x = \eta_1) \wedge (x = \eta_2)$ de la proposición 1 que indica que x es η_1 y la proposición 2 que indica que x es η_2 se expresa por el siguiente polinomio.

$$\iota_1\cdot(x - \eta_1) + \iota_2\cdot(x - \eta_2) \qquad (63)$$

donde ι_1 y ι_2 son números aleatorios. Entonces, las relaciones entre valores verdaderos y los valores de función de la Expresión (63) se muestran en la siguiente tabla.

Tabla 2

Proposición 1 $(x = \eta_1)$	Proposición 2 $(x = \eta_2)$	AND lógica $(x = \eta_1) \wedge (x = \eta_2)$	Valor de función $\iota_1\cdot(x - \eta_1) + \iota_2\cdot(x - \eta_2)$
Verdadera	Verdadera	Verdadera	0
Verdadera	Falsa	Falsa	Distinto de 0
Falsa	Verdadera	Falsa	Distinto de 0
Falsa	Falsa	Falsa	Distinto de 0

Como se entiende a partir de la Tabla 2, cuando la AND lógica $(x = \eta_1) \wedge (x = \eta_2)$ es verdadera, el valor de función de la Expresión (63) es cero; y cuando la AND lógica $(x = \eta_1) \wedge (x = \eta_2)$ es falsa, el valor de función de la Expresión (63) es un valor distinto de cero. En otras palabras, una AND lógica $(x = \eta_1) \wedge (x = \eta_2)$ de verdadera es equivalente a un valor de función de cero en la Expresión (63). Por lo tanto, la AND lógica se puede expresar mediante la Expresión (63).

Como se describió anteriormente, usando las Expresiones (62) y (63), una fórmula lógica formada por una(s) OR lógica(s) y/o una(s) AND lógica(s) se puede expresar por el polinomio f(x). Un ejemplo se mostrará más adelante.

Fórmula lógica: $\{(x = \eta_1) \vee (x = \eta_2) \vee (x = \eta_3)\} \wedge (x = \eta_4) \wedge (x = \eta_5)$

Polinomio: $f(x) = \iota_1 \cdot \{(x - \eta_1) \cdot (x - \eta_2) \cdot (x - \eta_3)\} + \iota_2 \cdot (x - \eta_4) + \iota_3 \cdot (x - \eta_5)$

(64)

En la Expresión (62), se usa un elemento indeterminado x para expresar la OR lógica. También se puede usar una pluralidad de elementos indeterminados para expresar una OR lógica. Por ejemplo, cuando se usan dos elementos indeterminados x_0 y x_1, la OR lógica $(x_0 = \eta_0) \vee (x_1 = \eta_1)$ de la proposición 1 que indica que x_0 es η_0 y la proposición 2 que indica que x_1 es η_1 se puede expresar el siguiente polinomio.

$$(x_0 - \eta_0) \cdot (x_1 - \eta_1)$$

También se pueden usar tres o más elementos indeterminados para expresar una OR lógica por un polinomio.

En la Expresión (63), se usa un elemento indeterminado x para expresar la AND lógica. También se puede usar una pluralidad de elementos indeterminados para expresar una AND lógica. Por ejemplo, la AND lógica $(x_0 = \eta_0) \wedge (x_1 = \eta_1)$ de la proposición 1 que indica que x_0 es η_0 y la proposición 2 que indica que x_1 es η_1 se puede expresar por el siguiente polinomio.

$$\iota_0 \cdot (x_0 - \eta_0) + \iota_1 \cdot (x_1 - \eta_1)$$

También se pueden usar tres o más elementos indeterminados para expresar una AND lógica por un polinomio.

Una fórmula lógica que incluye una(s) OR lógica(s) y/o una(s) AND lógica(s) se expresa con H ($H \geq 1$) tipos de elementos indeterminados $x_0, \ldots, x_{H-1}$ como el polinomio $f(x_0, \ldots, x_{H-1})$. Se supone que una proposición para cada uno de los elementos indeterminados $x_0, \ldots, x_{H-1}$ es "x_h es η_h", donde η_h (h = 0, …, H-1) es una constante determinada para cada proposición. Entonces, en el polinomio $f(x_0, \ldots, x_{H-1})$ que indica la fórmula lógica, la proposición que indica que un elemento indeterminado x_h es una constante η_h se expresa por el polinomio que indica la diferencia entre el elemento indeterminado x_h y la constante η_h; la OR lógica de las proposiciones se expresa por el producto de los polinomios que indican las proposiciones; y la AND lógica de las proposiciones o las OR lógicas de las proposiciones se expresa por una combinación lineal de los polinomios que indican las proposiciones o las OR lógicas de las proposiciones. Por ejemplo, se usan cinco elementos indeterminados $x_0, \ldots, x_4$ para expresar una fórmula lógica

$$\{(x_0 = \eta_0) \vee (x_1 = \eta_1) \vee (x_2 = \eta_2)\} \wedge (x_3 = \eta_3) \wedge (x_4 = \eta_4)$$

por el siguiente polinomio

$$f(x_0, \ldots, x_4) = \iota_0 \cdot \{(x_0 - \eta_0) \cdot (x_1 - \eta_1) \cdot (x_2 - \eta_2)\} + \iota_1 \cdot (x_3 - \eta_3) + \iota_2 \cdot (x_4 - \eta_4)$$

[Relación entre polinomio y producto interior]
El polinomio $f(x_0, \ldots, x_{H-1})$ que indica una fórmula lógica se puede expresar por el producto interior de dos vectores n dimensionales. Más específicamente, el polinomio $f(x_0, \ldots, x_{H-1})$ es igual al producto interior de un vector

$$\vec{v} = (v_1, \ldots, v_n)$$

que tiene los elementos indeterminados de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos y un vector

$$\vec{w} = (w_1, \ldots, w_n)$$

que tiene los coeficientes de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos

$$f(x_0, \ldots, x_{H-1}) = \vec{w} \cdot \vec{v}$$

En otras palabras, si el polinomio $f(x_0, \ldots, x_{H-1})$ que indica una fórmula lógica es cero es equivalente a si el producto interior del vector $\vec{v}$ que tiene los elementos indeterminados de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos y el vector $\vec{w}$ que tiene los coeficientes de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos es cero.

$$f(x_0, \ldots, x_{H-1}) = 0 \leftrightarrow \vec{w} \cdot \vec{v} = 0$$

Por ejemplo, un polinomio $f(x) = \theta_0 \cdot x^0 + \theta_1 \cdot x + \ldots + \theta_{n-1} \cdot x^{n-1}$ expresado con un elemento indeterminado x se puede expresar por el producto interior de dos vectores n dimensionales como sigue.

$$\vec{w} = (w_1, \ldots, w_n) = (\theta_0, \ldots, \theta_{n-1}) \quad (65)$$

$$\vec{v} = (v_1, \ldots, v_n) = (x^0, \ldots, x^{n-1}) \quad (66)$$

$$f(x) = \vec{w} \cdot \vec{v} \quad (67)$$

En otras palabras, si el polinomio f(x) que indica una fórmula lógica es cero es equivalente a si el producto interior en la Expresión (67) es cero.

$$f(x) = 0 \leftrightarrow \vec{w} \cdot \vec{v} = 0 \quad (68)$$

Cuando un vector que tiene los elementos indeterminados de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos se expresa por

$$\vec{w} = (w_1, \ldots, w_n)$$

y un vector que tiene los coeficientes de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos se expresa por

$$\vec{v} = (v_1, \ldots, v_n)$$

si el polinomio $f(x_0, \ldots, x_{H-1})$ que indica una fórmula lógica es cero es equivalente a si el producto interior del vector $\vec{w}$ y el vector $\vec{v}$ es cero.

Por ejemplo, cuando se usan las siguientes expresiones en lugar de las expresiones (65) y (66),

$$\vec{w} = (w_1, \ldots, w_n) = (x^0, \ldots, x^{n-1}) \quad (69)$$

$$\vec{v} = (v_1, \ldots, v_n) = (\theta_0, \ldots, \theta_{n-1}) \quad (70)$$

si el polinomio f(x) que indica una fórmula lógica es cero es equivalente a si el producto interior en la Expresión (67) es cero.

En el cifrado de predicado del producto interior, uno de los vectores $\vec{v} = (v_0, \ldots, v_{n-1})$ y $\vec{w} = (w_0, \ldots, w_{n-1})$ se usa como la información de atributo y el otro se usa como la información de predicado. Una de la información de atributo y la información de predicado se incorpora en el texto cifrado y la otra se incorpora en la información de clave. Por ejemplo, se usa un vector n dimensional $(\theta_0, \ldots, \theta_{n-1})$ como información de predicado, otro vector n dimensional $(x^0, \ldots, x^{n-1})$ se usa como información de atributo, una de la información de atributo y la información de predicado se incorpora en el texto cifrado y la otra se incorpora en la información de clave. Se supone en la siguiente descripción que un vector n dimensional incorporado en la información de clave es $\vec{w} = (w_1, \ldots, w_n)$ y otro vector n dimensional incorporado en el texto cifrado es $\vec{v} = (v_1, \ldots, v_n)$. Por ejemplo,

Información de predicado: $\vec{w} = (w_1, \ldots, w_n) = (\theta_0, \ldots, \theta_{n-1})$
Información de atributo: $\vec{v} = (v_1, \ldots, v_n) = (x^0, \ldots, x^{n-1})$

Alternativamente,

Información de predicado: $\vec{v} = (v_1, \ldots, v_n) = (\theta_0, \ldots, \theta_{n-1})$
Información de atributo: $\vec{w} = (w_1, \ldots, w_n) = (x^0, \ldots, x^{n-1})$

[Esquema básico del cifrado de predicado del producto interior]
Un ejemplo de esquema básico de un mecanismo de encapsulación de claves (KEM) que usa el cifrado de predicado del producto interior se describirá más adelante. Este esquema incluye Setup(1^k), GenKey(MSK, $\vec{w}$), Enc(PA, $\vec{v}$) y Dec(SKw, C_2).

Configuración de Setup(1^k):

Entrada: Parámetro de seguridad k
Salida: Información de clave maestra MSK, parámetro público PK

En un ejemplo de Setup(1^k), se usa el parámetro de seguridad k como n y se seleccionan la matriz de (n + ζ) filas por (n + ζ) columnas A que tiene los vectores de base (n + ζ) dimensionales a_i (i = 1, ..., n + ζ) como elementos, la matriz de (n + ζ) filas por (n + ζ) columnas A* que tiene el vector de base a_i* (i = 1, ..., n + ζ) como elementos y las matrices de (n + ζ) filas por (n + ζ) columnas X y X* usadas para transformación de coordenadas. Entonces, el vector de base (n + ζ) dimensional b_i (i = 1, ..., n + ζ) se calcula a través de transformación de coordenadas por la Expresión (52) y los vectores de base (n + ζ) dimensional b_i* (i = 1, ..., n + ζ) se calculan a través de transformación de coordenadas por la Expresión (54). Entonces, la matriz de (n + ζ) filas por (n + ζ) columnas B* que tiene los vectores de base b_i* (i = 1, ..., n + ζ) como elementos se saca como la información de clave maestra MSK; y los espacios de vector V y V*, la matriz de (n + ζ) filas por (n + ζ) columnas B que tiene los vectores de base b_i (i = 1, ..., n + ζ) como elementos, el parámetro de seguridad k, el campo finito F_q, la curva elíptica E, los grupos cíclicos G_1, G_2 y G_T, los generadores g_1, g_2 y g_T, la función bilineal e y otros se sacan como el parámetro público PK.

Generación de información de clave GenKey(MSK, $\vec{w}$):

Entrada: Información de clave maestra MSK, vector $\vec{w}$

Salida: Información de clave D* que corresponde al vector $\vec{w}$

En un ejemplo de GenKey(MSK, $\vec{w}$), un elemento $\alpha \in F_q$ se selecciona a partir del campo finito F_q. Entonces, la matriz B*, la cual es la información de clave maestra MSK, se usa para generar y sacar una información de clave D* que corresponde al vector $\vec{w}$ de la siguiente manera.

$$D^* = \alpha \cdot (\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + b_{n+1}^* \in G_2^{n+1} \qquad (71)$$

Si es difícil resolver un problema logarítmico discreto en el grupo cíclico G_2, es difícil separar y extraer el componente de b_μ* de la información de clave D*.

Cifrado Enc(PA, $\vec{v}$):

Entrada: Parámetro público PK, vector $\vec{v}$
Salida: Texto cifrado C_2, clave común K

En un ejemplo de Enc(PA, $\vec{v}$), se generan la clave común K y un número aleatorio υ_0, que es un elemento del campo finito F_q. Entonces, el parámetro público PK, tal como la matriz B, los elementos υ_1, ..., υ_ζ del campo finito F_q, el vector $\vec{v}$ y el número aleatorio υ_0 se usan para generar el texto cifrado C_2 de la siguiente forma.

$$C_2 = \upsilon_0 \cdot (\sum_{\mu=1}^{n} v_\mu \cdot b_\mu) + \sum_{\mu=n+1}^{n+\zeta} \upsilon_{\mu-n} \cdot b_\mu \in G_1^{n+\zeta} \qquad (72)$$

Se sacan el texto cifrado C_2 y la clave común K. Un ejemplo de la clave común K es $g_T^{\tau\upsilon 1} \in G_T$, donde $\upsilon 1$ significa υ_1. Un ejemplo de τ es 1_F, como se describió anteriormente. Si es difícil resolver un problema logarítmico discreto en el grupo cíclico G_1, es difícil separar y extraer el componente b_μ del texto cifrado C_2.

Descifrado y compartición de clave Dec(SKw, C_2):

Entrada: Información de clave D_1* que corresponde al vector $\vec{w}$, texto cifrado C_2
Salida: Clave común K

En un ejemplo de Dec(SKw, C_2), el texto cifrado C_2 y la información de clave D_1* se introducen a la función bilineal e de la Expresión (32). Entonces, a partir de las características de las Expresiones (33) y (56), se satisface lo siguiente.

$$
\begin{aligned}
e(C_2, D^*) &= e(\upsilon_0 \cdot (\textstyle\sum_{\mu=1}^{n} v_\mu \cdot b_\mu) + \sum_{\mu=n+1}^{n+\zeta} \upsilon_{\mu-n} \cdot b_\mu, \sigma \cdot (\textstyle\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^{\,*}) + b_{n+1}^{\,*}) \\
&= e(\upsilon_0 \cdot v_1 \cdot b_1, \sigma \cdot w_1 \cdot b_1^{\,*}) \cdot \ldots \cdot e(\upsilon_0 \cdot v_n \cdot b_n, \sigma \cdot w_n \cdot b_n^{\,*}) \\
&\quad \times e(\upsilon_1 \cdot b_{n+1}, b_{n+1}^{\,*}) \cdot e(\upsilon_2 \cdot b_{n+2}, 0) \cdot \ldots \cdot e(\upsilon_\zeta \cdot b_{n+\zeta}, 0) \\
&= e(b_1, b_1^{\,*})^{\upsilon_0 \cdot v_1 \cdot \sigma \cdot w_1} \cdot \ldots \cdot e(b_n, b_n^{\,*})^{\upsilon_0 \cdot v_n \cdot \sigma \cdot w_n} \cdot e(b_{n+1}, b_{n+1}^{\,*})^{\upsilon_1} \\
&= g_T^{\tau \cdot \upsilon_0 \cdot v_1 \cdot \sigma \cdot w_1} \cdot \ldots \cdot g_T^{\tau \cdot \upsilon_0 \cdot v_n \cdot \sigma \cdot w_n} \cdot g_T^{\tau \cdot \upsilon_1} \\
&= g_T^{\tau \cdot \upsilon_0 \cdot \sigma \cdot \vec{v} \cdot \vec{w}} \cdot g_T^{\tau \cdot \upsilon_1}
\end{aligned}
\qquad (73)
$$

Cuando el producto interior $\vec{w} \cdot \vec{v}$ es cero, la Expresión (73) se puede deformar a la siguiente forma.

$$
\begin{aligned}
e(C_2, D^*) &= g_T^{\tau \cdot \upsilon_0 \cdot \sigma \cdot 0} \cdot g_T^{\tau \cdot \upsilon_1} \\
&= g_T^{\tau \cdot \upsilon_1}
\end{aligned}
\qquad \cdots (74)
$$

A partir de este resultado, se genera y se saca la clave común K. Un ejemplo de la clave común K es $g_T^{\tau \upsilon 1} \in G_T$.

[Estructura general]
La Figura 15 es un diagrama de bloques que ilustra la estructura de un aparato de compartición 810 según la segunda realización. La Figura 16 es un diagrama de bloques que ilustra la estructura de aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) según la segunda realización. La Figura 17 es un diagrama de bloques que ilustra la estructura de un aparato de adquisición 830 según la segunda realización. La Figura 18 es un diagrama de bloques que ilustra la estructura de una unidad de composición 835 en la Figura 17. En esas figuras, a componentes idénticos a aquellos en la primera realización se dan los mismos números de referencia que en la primera realización en aras de la simplicidad.

Un sistema de compartición de secretos según esta realización se obtiene sustituyendo el aparato de compartición 110 en la Figura 1 con el aparato de compartición 810, sustituyendo los aparatos de gestión de partes [PA(α, h(α))] 120-α-h(α) con los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) y sustituyendo el aparato de adquisición 130 con el aparato de adquisición 830.

[Aparato de compartición 810]
Como se muestra en la Figura 15, el aparato de compartición 810 en esta realización incluye un almacenamiento temporal 111, un almacenamiento 112, un controlador 113, unidades de compartición de secretos 814-α (α = 1 a L) y un transmisor 115. El aparato de compartición 810 en esta realización se implementa ejecutando un programa predeterminado leído en un ordenador conocido dotado con una CPU, una RAM, una ROM y similares, por ejemplo.

[Aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α)]

Como se ilustra en la Figura 16, cada uno de los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) en esta realización incluye un almacenamiento temporal 121-α-h(α), un almacenamiento 122-α-h(α), un controlador 123-α-h(α), un generador de valores de secretos compartidos 824-α-h(α), un transmisor 125-α-h(α) y un receptor 126-α-h(α). Cada uno de los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) en esta realización se implementa ejecutando un programa predeterminado leído en un ordenador conocido dotado con una CPU, una RAM, una ROM y similares, por ejemplo.

[Generador de valor común 140-α]
El generador de valor común 140-α es el mismo que en la primera realización.

[Aparato de adquisición 830]
Como se ilustra en la Figura 17, el aparato de adquisición 830 en esta realización incluye un almacenamiento temporal 131, un almacenamiento 132, un controlador 133, unidades de reconstrucción 834-α (α = 1 a L), una unidad de composición 835, un transmisor 135 y un receptor 136. Como se muestra en la Figura 18, la unidad de composición 835 incluye una primera unidad de operación 835a y una segunda unidad de operación 835b. El aparato de adquisición 830 en esta realización se implementa ejecutando un programa predeterminado leído en un

ordenador conocido dotado con una CPU, una RAM, una ROM y similares, por ejemplo.

[Procesamiento de compartición de secretos]
El procesamiento de compartición de secretos en esta realización se describirá a continuación.

Esta realización es una aplicación de la primera realización: Una matriz B* (Expresión (59)), que es la información de clave maestra MSK del cifrado de predicado del producto interior, se comparte con un esquema de compartición de secretos y se reconstruye la información de claves D*, como se da por la Expresión (71). En la descripción dada más adelante, la información de claves D* de la Expresión (71) se generaliza a la información de generación dada por

$$SK = \sigma(\alpha) \cdot \{\Sigma_{\mu=1}^{n} w_\mu \cdot b_\mu^*\} + \Sigma_{\mu=n+1}^{n+\zeta} b_\mu^* \in G^{n+\zeta} \qquad (75)$$

La Expresión (71) es un ejemplo cuando ζ = 1.

Los elementos

$$\chi_{i,\beta} \cdot \kappa_2 \cdot g_2 \in G_2 \ (i = 1, \ldots, n + \zeta, \beta = 1, \ldots, n + \zeta) \quad (76)$$

de la matriz B* dada por la Expresión (55) se expresan como

$$\theta(i,\beta) \cdot g_2 \in G_2 \qquad (77)$$

$$\theta(i,\beta) = \chi_{i,\beta} \cdot \kappa_2 \in F_q \qquad (78)$$

Cuando el vector de base b_i^* de la Expresión (55) se expresa como

$$b_i^* = (\theta(i, 1) \cdot g_2, \ldots, \theta(i, n + \zeta) \cdot g_2) \in G_2^{n+\zeta} \qquad (79)$$

Esta indica que la compartición de secretos de la matriz B* y la reconstrucción de la información de generación SK se pueden ejecutar extendiendo la primera realización o sus modificaciones a múltiples dimensiones.

La diferencia de la primera realización y sus modificaciones se describirá principalmente más adelante. Las partes en común a ellas no se describirán.

[Procesamiento preparatorio]
En el procesamiento preparatorio para el procesamiento de compartición de secretos en esta realización, la información $\theta(i,\beta) \in F_q$ para identificar la información secreta $\theta(i,\beta) \cdot g_2 \in G_2$ (i = 1 a n + ζ, β = 1 a n + ζ) cada parte de la cual es un elemento del vector de base b_i^*, se almacena en el almacenamiento 112 del aparato de compartición 810.

[Procesamiento de compartición de secretos entero]
La Figura 19 es una vista que ilustra el procesamiento de compartición de secretos entero en la segunda realización. El procesamiento de compartición de secretos entero en esta realización se describirá a continuación con referencia a la Figura 19.

En esta realización, el aparato de compartición 810 (Figura 15) genera las partes SH(i, β, α, h (α)) compartiendo la información secreta $\theta(i,\beta) \cdot g_2 \in G_2$, cada parte de la cual es un elemento de los vectores de base b_i^*, para cada uno de los subconjuntos SUB(α) separadamente y saca las partes SH(i, β, α, h (α)) (paso S81). El esquema de compartición de secretos específicos es el mismo que en la primera realización. Un conjunto de partes SH(i, β, α, h (α)) $\in G_2$ (i = 1 a n + ζ, β = 1 a n + ζ) se llama una parte SH(α, h (α)). Las partes SH(α, h (α)) se envían a través de la red 150 a los aparatos de gestión de partes correspondientes [PA(α, h(α))] 820-α-h(α).

Cada uno de los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) al cual se envió cada una de las partes SH(α, h (α)) genera un valor de secreto compartido DSH(α, h (α)) usando las partes SH(i, β, α, h (α)) que forman cada una de las partes SH(α, h (α)), un valor común σ (α) usado en cada uno de los subconjuntos SUB(α) y un vector n dimensional $\vec{w}$ = (w_1, …, w_n) que tiene elementos de un campo finito F_q como elementos w_μ (μ = 1 a n) (paso S82). El valor de secreto compartido DSH(α, h (α)) en esta realización es

$$DSH(\alpha,h(\alpha)) = \sigma(\alpha) \cdot \{\Sigma_{\mu=1}{}^{n} w_\mu \cdot SHb_\mu{}^{*}(\alpha, h(\alpha))\} + \Sigma_{\mu=n+1}{}^{n+\zeta} SHb_\mu{}^{*}(\alpha, h(\alpha)) \in G^{n+\zeta} \quad (81)$$

donde $SHb_i{}^{*}$ (α, h (α)) está siguiendo el vector de base compartido (n + ζ) dimensional, que tiene (n + ζ) partes SH(i, 1, α, h (α)) a SH(i, n + ζ, α, h (α)) como elementos.

$$SHb_i{}^{*}(\alpha, h(\alpha)) = (SH(i, 1, \alpha, h(\alpha)), ..., SH(i, n + \zeta, \alpha, h(\alpha)) \in G^{n+\zeta} \quad (80)$$

En esta realización, los valores comunes (σ (α)) de diferentes subconjuntos SUB(α) son independientes unos de otros.

Los valores de secretos compartidos DSH(α, h(α)) sacados de los aparatos de gestión de partes [PA(α, h(α))] 820-α -h(α) se envían separadamente a través de la red 150 al aparato de adquisición 830. Usando la pluralidad de valores de secretos compartidos DSH(α, h(α)) que corresponden al mismo subconjunto SUB(α), el aparato de adquisición 830 genera un valor de secreto reconstruido SUBSK(α) expresado como sigue por el procesamiento de reconstrucción para cada subconjunto SUB(α) (paso S83).

$$SUBSK(\alpha) = \sigma(\alpha) \cdot \{\Sigma_{\mu=1}{}^{n} w_\mu \cdot b_\mu{}^{*}\} + \Sigma_{\mu=n+1}{}^{n+\zeta} b_\mu{}^{*} \in G^{n+\zeta} \quad (82)$$

Este procesamiento se puede implementar ejecutando el procesamiento de reconstrucción en la primera realización o sus modificaciones para cada dimensión μ de los valores de secretos compartidos DSH(α, h(α)).

El aparato de adquisición 830 entonces genera información de generación SK usando los valores de secretos reconstruidos SUBSK(α) generados para los subconjuntos correspondientes SUB(α) y saca la información de generación SK (paso S84).

En esta realización, el aparato de adquisición 830 genera la información de generación SK realizando una combinación lineal de los valores de secretos reconstruidos SUBSK(α). Un ejemplo de la información de generación se expresa como sigue.

$$SK = \{(\sigma(1) + ... + \sigma(L))/L\} \cdot \{\Sigma_{\mu=1}{}^{n} w_\mu \cdot b_\mu{}^{*}\} + \Sigma_{\mu=n+1}{}^{n+\zeta} b_\mu{}^{*} \in G^{n+\zeta} \quad (83)$$

[Procesamiento (en el paso S81) en el aparato de compartición]
La Figura 20 es una vista que ilustra un ejemplo de procesamiento en el aparato de compartición en la segunda realización. El procesamiento en el aparato de compartición 810 se describirá a continuación en detalle con referencia a esta figura.

El controlador 113 del aparato de compartición 810 (Figura 15) especifica α = 1 y β = 1 y almacena los ajustes en el almacenamiento temporal 111 (paso S811). El controlador 113 del aparato de compartición 810 entonces especifica i = 1 y almacena el ajuste en el almacenamiento temporal 111 (paso S812).

La información $\theta(i,\beta) \in F_q$ para identificar la información secreta $\theta(i,\beta) \cdot g_2 \in G_2$ (i = 1 a n + ζ, β = 1 a n + ζ) se lee del almacenamiento 112 e introduce a la unidad de compartición de secretos 814-α. La unidad de compartición de secretos 814-α genera H(α) partes

$$SH(i, \beta, \alpha, 1), ..., SH(i, \beta, \alpha, H(\alpha)) \quad (84)$$

para un subconjunto SUB(α) compartiendo la información secreta $\theta(i,\beta) \cdot g_2$ usando la información $\theta(i,\beta) \in F_q$ y las saca (paso S813). Este procesamiento se puede ejecutar por el mismo método que en el paso S112 de la primera realización o sus modificaciones.

El controlador 113 entonces juzga si β almacenado en el almacenamiento temporal 111 es n + ζ (paso S814). Si no se juzga que β = n + ζ, el controlador 113 especifica β + 1 como un nuevo valor de β, almacena el ajuste en el almacenamiento temporal 111 (paso S815) y hace que el procesamiento del paso S813 sea ejecutado con este nuevo valor de β.

Si se juzga en el paso S814 que β = n + ζ, el controlador 113 especifica β = 1 y almacena el ajuste en el almacenamiento temporal 111 (paso S816). Entonces, el controlador 113 juzga si i almacenado en el almacenamiento temporal 111 es n + ζ (paso S817). Si no se juzga que i = n + ζ el controlador 113 especifica i + 1 como un nuevo valor de i, almacena el ajuste en el almacenamiento temporal 111 (paso S818) y hace que el procesamiento del paso S813 sea ejecutado con el nuevo valor de i.

Si se juzga en el paso S817 que i = n + ζ, el controlador 113 juzga si α almacenada en el almacenamiento temporal 111 es L (paso S113). Si no se juzga que α = L, el controlador 113 especifica α + 1 como un nuevo valor de α, almacena el ajuste en el almacenamiento temporal 111 (paso S114) y hace que el procesamiento del paso S812 sea ejecutado con el nuevo valor de α.

Si se juzga en el paso S113 que α = L, las partes SH(α, h (α))sacadas de las unidades de compartición de secretos 814-α se envían al transmisor 115. El transmisor 115 envía conjuntos de (n + ζ)^2 partes

$$SH(i, \beta, \alpha, h(\alpha)) \ (i = 1, ..., n + \zeta, \beta = 1, ..., n + \zeta) \qquad (85)$$

a los aparatos de gestión de partes correspondientes [PA(α, h(α))] 820-α-h(α) a través de la red 150 (paso S819). La parte SH(1, 1) formada de (n + ζ)^2 partes SH(i, β, 1, 1) (i = 1 a n + ζ, β = 1 a n + ζ) se envía al aparato de gestión de partes [PA(1, 1)] 820-1-1; la parte SH(1, 2) formada de (n + ζ)^2 partes SH(i, β, 1, 2) (i = 1 a n + ζ, β = 1 a n + ζ) se envía al aparato de gestión de partes [PA(1, 2)] 820-1-2; ...; y la parte SH(L, H(L)) formada de (n + ζ)^2 partes SH(i, β, L, H(L)) (i = 1 a n + ζ, β = 1 a n + ζ) se envía al aparato de gestión de partes [PA(L, H(L))] 820-L-H(L).

[Procesamiento en generador de valor común]
Cada uno de los generadores de valores comunes 140-α (Figura 3B) genera un valor común σ(α) a ser compartido por los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) incluidos en el subconjunto SUB(α) que corresponde al generador de valor común 140-α. En esta realización, se usa un número aleatorio generado por el generador de números aleatorios 141-α como el valor común σ(α) y el transmisor 142-α envía el valor común σ(α) a los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) incluidos en el subconjunto SUB(α).

[Procesamiento (en el paso S82) de los aparatos de gestión de partes]
La Figura 21 es una vista que ilustra un ejemplo de procesamiento en los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) en la segunda realización. El procesamiento en los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) en esta realización se describirá a continuación con referencia a esta figura.

Cada uno de los receptores 126-α-h(α) de los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) recibe la parte SH(α-h(α)) formada de las (n + ζ)^2 partes enviadas SH(i, β, α, h(α)) (i = 1 a n + ζ, β = 1 a n + ζ) y la almacena en el almacenamiento 122-α-h(α) (paso S821). Si el procesamiento en el paso S821 se ejecutó antes y si la parte SH(α-h(α)) ya ha sido almacenada en el almacenamiento 122-α-h(α) del aparato de gestión de partes [PA(α, h(α))] 820-α-h(α), se puede omitir el procesamiento del paso S821.

Cada uno de los receptores 126-α-h(α) de los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) recibe cada uno de los valores comunes σ(α) enviados desde los generadores de valores comunes 140-α y los almacena en cada uno de los almacenamientos 122-α-h(α) (paso S122).

En esta realización, un vector n dimensional $\vec{w}$ = (w_1, ..., w_n), que es la información proporcionada leída desde el almacenamiento 132 del aparato de adquisición 830 (Figura 17), se envía desde el transmisor 135 a través de la red 150 a los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α). El vector n dimensional $\vec{w}$ = (w_1, ..., w_n) es común a todos los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α). El vector n dimensional $\vec{w}$ = (w_1,

..., w_n) se recibe por cada uno de los receptores 126-α-h(α) de los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) (Figura 16) y se almacena en cada uno de los almacenamientos 122-α-h(α) (paso S823).

Cada uno de los generadores de valores de secretos 824-α-h(α) lee la parte SH(α, h(α)), el valor común $\sigma(\alpha)$ y el vector n dimensional $\vec{w}$ = (w_1, ..., w_n) desde cada uno de los almacenamientos 122-α-h(α). Cada uno de los generadores de valores de secretos 824-α-h(α) genera un valor de secreto compartido DSH(α, h(α)) dado por la Expresión (81), usando la parte SH(α, h(α)) y la información común que contiene el valor común $\sigma(\alpha)$ y $\vec{w}$ = (w_1 a w_n) y saca el valor de secreto compartido DSH(α, h(α)) (paso S824).

Cada uno de los valores de secretos compartidos generados DSH(α, h(α)) se envía a cada uno de los transmisores 125-α-h(α). Los transmisores 125-α-h(α) envían los valores de secretos compartidos DSH(α, h(α)) a través de la red 150 al aparato de adquisición 830 (paso S125).

[Procesamiento (en los pasos S83 y S84) en el aparato de adquisición]
La Figura 22 es una vista que ilustra un ejemplo de procesamiento en el aparato de adquisición en la segunda realización.

Los valores de secretos compartidos DSH(α, h(α)) enviados desde los aparatos de gestión de partes [PA(α, h(α))] 820-α-h(α) se reciben por el receptor 136 del aparato de adquisición 830 (Figura 17) y se almacenan en el almacenamiento 132 (paso S131).

Entonces, el controlador 133 juzga si el número de valores de secretos compartidos DSH(α, h(α)) almacenados en el almacenamiento 132 es mayor o igual al número requerido (paso S132). Si no se juzga aquí que los valores de secretos compartidos DSH(α, h(α)) del número requerido o mayor se almacenan en el almacenamiento 132, el procesamiento vuelve al paso S131.

Si se juzga que el número de valores de secretos compartidos DSH(α, h(α)) almacenados en el almacenamiento 132 es mayor o igual que el número requerido, el controlador 133 especifica α = 1 y almacena el ajuste en el almacenamiento temporal 131 (paso S133). Entonces, el número requerido de valores de secretos compartidos DSH(α, h(α)) que corresponden al subconjunto SUB(α) se leen desde el almacenamiento 132 e introducen a la unidad de reconstrucción 834-α. La unidad de reconstrucción 834-α genera un valor de secreto reconstruido SUBSK(α) dado por la Expresión (82), por el procesamiento de reconstrucción para el subconjunto SUB(α), usando los valores de secretos compartidos de entrada DSH(α, h(α)) y saca el valor de secreto reconstruido SUBSK(α) del subconjunto SUB(α) (paso S834).

El controlador 133 a continuación juzga si α almacenado en el almacenamiento temporal 131 es L (paso S135). Si no se juzga aquí que α = L, el controlador 133 especifica α + 1 como un nuevo valor de α, almacena el ajuste en el almacenamiento temporal 131 (paso S136) y hace que el procesamiento en el paso S834 sea ejecutado con el nuevo valor de α.

Si se juzga en el paso S135 que α = L, los valores de secretos reconstruidos SUBSK(α) sacados de las unidades de reconstrucción correspondientes 134-α se envían a la unidad de composición 835. La primera unidad de operación 835a (Figura 18) de la unidad de composición 835 genera la siguiente combinación lineal y la saca (paso S841).

$$\begin{aligned} &SUBSK(1) + \ldots + SUBSK(L) \\ &= (\sigma(1) + \ldots + \sigma(L)) \cdot \{\Sigma_{\mu=1}^{n} w_\mu \cdot b_\mu^*\} \\ &\quad + L \cdot \Sigma_{\mu=n+1}^{n+\zeta} b_\mu^* \in G^{n+\zeta} \end{aligned} \qquad (86)$$

La combinación lineal SUBSK(1) + ... + SUBSK(L) se introduce a la segunda unidad de operación 835b. La segunda unidad de operación 835b genera la siguiente información de generación y saca la información de generación SK (paso S842).

$$\begin{aligned} SK &= \{(\sigma(1) + \ldots + \sigma(L))/L\} \cdot \{\Sigma_{\mu=1}^{n} w_\mu \cdot b_\mu^*\} \\ &\quad + \Sigma_{\mu=n+1}^{n+\zeta} b_\mu^* \in G^{n+\zeta} \end{aligned} \qquad (87)$$

[Modificación de la segunda realización]
Las modificaciones de la primera realización se pueden aplicar a esta realización, también.

[Otras modificaciones y otros]
La presente invención no está limitada a las realizaciones descritas anteriormente. Por ejemplo, cada operación definida en el campo finito F_q se puede sustituir con una operación definida en un anillo finito Z_q cuyo orden es q. Un método de sustitución de la operación definida en el campo finito F_q con la operación definida en el anillo finito Z_q es para permitir un q distinto de números primos y sus potencias.

En lugar de la Expresión (71), se puede usar la siguiente Expresión:

$$D^* = \sigma \cdot (\Sigma_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + \Sigma_{\iota=n+1}^{n+\zeta} \upsilon_\iota \cdot b_\iota^* \in G_2^{n+\zeta}$$

donde υ_ι es una constante o una variable (tal como un número aleatorio). El procesamiento descrito anteriormente se puede ejecutar en el orden en el que se describe aquí o se puede ejecutar en paralelo o independientemente, según las capacidades de procesamiento de las unidades que ejecutan el procesamiento o como se necesite. Son posibles otras modificaciones dentro del alcance de la presente invención.

Cuando la estructura descrita anteriormente se implementa por un ordenador, los detalles de procesamiento de las funciones que se deberían proporcionar por cada aparato se describen en un programa. Cuando el programa se ejecuta por un ordenador, las funciones de procesamiento descritas anteriormente se implementan en el ordenador.

El programa que contiene los detalles de procesamiento se puede grabar en un medio de almacenamiento legible por ordenador. El medio de almacenamiento legible por ordenador puede ser cualquier tipo de medio, tal como un dispositivo de almacenamiento magnético, un disco óptico, un medio de almacenamiento magneto óptico y una memoria de semiconductores.

El programa se distribuye por venta, transferencia o préstamo de un medio de grabación portátil tal como un DVD o un CD-ROM con el programa grabado en él, por ejemplo. El programa también se puede distribuir almacenando el programa en una unidad de almacenamiento de un ordenador servidor y transfiriendo el programa desde el ordenador servidor a otro ordenador a través de la red.

Un ordenador que ejecuta este tipo de programa primero almacena el programa grabado en el medio de grabación portátil o el programa transferido desde el ordenador servidor en su unidad de almacenamiento. Entonces, el ordenador lee el programa almacenado en su unidad de almacenamiento y ejecuta el procesamiento según el programa leído. En una forma de ejecución de programa diferente, el ordenador puede leer el programa directamente desde el medio de grabación portátil y ejecutar un procesamiento según el programa o el ordenador puede ejecutar un procesamiento según el programa cada vez que el ordenador recibe el programa transferido desde el ordenador servidor. Alternativamente, el procesamiento se puede ejecutar por un denominado servicio de proveedor de servicios de aplicaciones (ASP), en el que la función de procesamiento se implementa solo dando una instrucción de ejecución de programa y obteniendo los resultados sin transferir el programa desde el ordenador servidor al ordenador. El programa de esta realización incluye información que se proporciona para uso en el procesamiento por un ordenador y se trata por consiguiente como un programa (algo que no es una instrucción directa al ordenador pero son datos o similares que tienen características que determinan el procesamiento ejecutado por el ordenador).

En esta realización, los aparatos se implementan ejecutando el programa predeterminado en el ordenador, pero al menos una parte del procesamiento se puede implementar por hardware.

DESCRIPCIÓN DE LOS NÚMEROS DE REFERENCIA

1:	Sistema de compartición de secretos
110, 810:	Aparatos de compartición
120, 820:	Aparatos de gestión de partes
130, 830:	Aparatos de adquisición
140:	Generador de valor común

REIVINDICACIONES

1. Un sistema de compartición de secretos **caracterizado por que** comprende

un aparato de compartición (110); $\sum_{\alpha=1}^{L} h(\alpha)$ aparatos de gestión de partes PA(α, h(α)) donde α = 1, …, L, L ≥ 2, h(α) = 1, …, H(α), H(α) ≥ 2; y
un aparato de adquisición (130); en donde
el aparato de compartición (110) incluye unidades de compartición de secretos (114-α) adaptadas para generar partes SH(α, h(α)) compartiendo secretos de información secreta con un esquema de compartición de secretos separadamente para subconjuntos respectivos SUB(α) cada uno de los cuales está formado de H(α) aparatos de gestión de partes PA(α, 1), …, PA (α, H(α)) y para sacar las partes SH (α, h(α));
los aparatos de gestión de partes PA (α, h(α)) incluyen generadores de valores de secretos compartidos (124-α-h(α)) adaptados para generar valores de secretos compartidos DSH(α, h(α)) y sacar los valores de secretos compartidos DSH(α, h(α)) respectivamente, cada uno de los valores de secretos compartidos DSH(α, h(α)) que se genera realizando una operación común a una de las partes SH(α, h(α)) y la información común que contiene uno de los valores comunes σ(α), cada uno de los valores comunes σ(α) que está compartido en cada uno de los subconjuntos SUB(α), la información común usada por los aparatos de gestión de partes PA(α, h(α)) que pertenecen al mismo de los subconjuntos SUB(α) que es el mismo y los aparatos de gestión de partes PA(α, h(α)) que pertenecen al mismo de los subconjuntos SUB(α) que realizan la misma operación común;
el aparato de adquisición (130) incluye:

unidades de reconstrucción (134-α) adaptados para generar valores de secretos reconstruidos SUBSK(α) que corresponden a los subconjuntos SUB(α) respectivamente, cada uno de los valores de secretos reconstruidos SUBSK(α) que se genera realizando un procesamiento de reconstrucción con el esquema de compartición de secretos para cada uno de los subconjuntos SUB(α), usando una pluralidad de los valores de secretos compartidos DSH(α, h(α)) que corresponde al mismo de los subconjuntos SUB(α); y
una unidad de composición (137) adaptada para generar información de generación SK usando los valores de secretos reconstruidos SUBSK(α) y para sacar la información de generación SK.

2. El sistema de compartición de secretos según la Reivindicación 1, en donde los valores comunes σ(α) compartidos en diferentes subconjuntos SUB(α) son independientes unos de otros.

3. El sistema de compartición de secretos según la Reivindicación 1 ó 2, en donde los generadores de valores de secretos compartidos (124-α-h(α)) de los aparatos de gestión de partes PA(α, h(α)), donde α = 1, …, L, realizan la misma operación común.

4. El sistema de compartición de secretos según la Reivindicación 3, en donde la operación común es lineal; y
la unidad de composición (137) está adaptada para generar la información de generación SK realizando una combinación lineal de los valores de secretos reconstruidos SUBSK(α).

5. El sistema de compartición de secretos según la Reivindicación 1, en donde la información común contiene el uno de los valores comunes σ(α) y la información común proporcionada a todos los aparatos de gestión de partes PA(α, h(α)), proporcionados por el aparato de adquisición (130).

6. El sistema de compartición de secretos según la Reivindicación 1, en donde la unidad de composición (137) está adaptada para generar la información de generación SK realizando una combinación lineal de los valores de secretos reconstruidos SUBSK(α).

7. El sistema de compartición de secretos según la Reivindicación 1, en donde la operación común es lineal.

8. El sistema de compartición de secretos según la Reivindicación 1, en donde cada una de las unidades de compartición de secretos (114-α) está adaptada para generar las partes SH(α, h(α)) por compartición de secretos de la información secreta usando un esquema de compartición de secretos de umbral (R(α), H(α)), donde 2 ≤ R(α) < H(α), con respecto a al menos una parte de los subconjuntos SUB(α); y
las unidades de reconstrucción (134-α) están adaptadas para generar los valores de secretos reconstruidos SUBSK(α) que corresponden a los subconjuntos SUB(α) respectivamente, cada uno de los valores de secretos reconstruidos SUBSK(α) que se genera usando R(α) o más valores de secretos compartidos DSH(α, h(α))

que corresponden al mismo de los subconjuntos SUB(α).

9. El sistema de compartición de secretos según la Reivindicación 8, en donde la información secreta contiene un elemento $\theta \cdot g \in G$ de un grupo cíclico G, donde g es un generador del grupo cíclico G y θ es un elemento del campo finito F_q;
el elemento $\theta \in F_q$ identifica la información secreta; y
cada una de las partes SH(α, h(α)) generada usando el esquema de compartición de secretos de umbral (R(α), H(α)) incluye un elemento f(α, ϕ(h(α)))·g $\in$ G del grupo cíclico G, donde x representa una variable que es un elemento del campo finito F_q, f(α, x)$\in F_q$ representa un polinomio de grado de orden (R(α) – 1) que satisface f(α, ω) = θ con respecto a un elemento predeterminado $\omega \in F_q$ del campo finito F_q y ϕ(h(α)) representa un índice que corresponde a h(α).

10. El sistema de compartición de secretos según la Reivindicación 8, en donde la información secreta contiene un elemento θ de un campo finito F_q; y
cada una de las partes SH(α, h(α)) generada usando el esquema de compartición de secretos de umbral (R(α), H(α)) incluye un elemento f(α, ϕ(h(α))) $\in F_q$ del campo finito F_q, donde x representa una variable que es un elemento del campo finito F_q, f(α, x)$\in F_q$ representa un polinomio de grado de orden (R(α) – 1) que satisface f(α, ω) = θ con respecto a un elemento predeterminado $\omega \in F_q$ del campo finito F_q y ϕ(h(α)) representa un índice que corresponde a h(α).

11. El sistema de compartición de secretos según la Reivindicación 1, en donde cada una de las unidades de compartición de secretos (114-α) está adaptada para generar las partes SH(α, h(α)) de la información secreta usando un esquema de compartición de secretos de umbral (H(α), H(α)) con respecto a al menos una parte de los subconjuntos SUB(α); y
las unidades de reconstrucción (134-α) están adaptadas para generar los valores de secretos reconstruidos SUBSK(α) que corresponden a los subconjuntos SUB(α) respectivamente, cada uno de los valores de secretos reconstruidos SUBSK(α) que se genera usando H(α) valores de secretos compartidos DSH(α, h(α)) que corresponden al mismo de los subconjuntos SUB(α).

12. El sistema de compartición de secretos según la Reivindicación 11, en donde la información secreta contiene un elemento $\theta \cdot g \in G$ de un grupo cíclico G, donde g es un generador del grupo cíclico G y θ es un elemento de un campo finito F_q; y
las partes SH(α, h(α)) generadas usando el esquema de compartición de secretos de umbral (H(α), H(α)) son elementos del grupo cíclico G, que satisfacen SH(α, 1) + SH(α, 2) + … + SH(α, H(α)) = $\theta \cdot g \in G$.

13. El sistema de compartición de secretos según la Reivindicación 11, en donde la información secreta contiene un elemento θ de un campo finito F_q; y
las partes SH(α, h(α)) generadas usando el esquema de compartición de secretos de umbral (H(α), H(α)) son elementos del campo finito F_q, que satisfacen SH(α, 1) + SH(α, 2) + … + SH(α, H(α)) = $\theta \in F_q$.

14. El sistema de compartición de secretos según cualquiera de las Reivindicaciones 5 a 13, en donde la información secreta es un conjunto de vectores de base b_i* que son b_1*, …, $b_{n+\zeta}$*, donde g es un generador de un grupo cíclico G, θ (i, β) es un elemento de un campo finito F_q, i = 1, …, n + ζ, β = 1, …, n + ζ, n $\geq$ 1, $\zeta \geq 1$ y b_i* = (θ (i, 1)·g, …, θ (i, n + ζ)·g) $\in G^{n+\zeta}$ es un vector de base (n + ζ) dimensional que tiene (n + ζ) elementos del grupo cíclico G como elementos;
cada una de las unidades de compartición de secretos (814-α) está adaptada para generar las partes SH(i, β, α, h (α))$\in$ G por compartición de secretos de los elementos θ (i, β)·g $\in$ G de los vectores de base b_i* separadamente para los subconjuntos respectivos SUB(α) y cada una de las partes SH(α, h(α)) es un conjunto de las partes SH(i, β, α, h (α))$\in$ G donde i = 1, …, n + ζ, β = 1, …, n + ζ;
un vector n dimensional $\vec{w}$ = (w_1, …, w_n) que tiene elementos del campo finito F_q como elementos w_μ, donde se proporciona μ = 1, …, n;
cada uno de los generadores de valores de secretos compartidos (824-α-h(α) genera cada uno de los valores de secretos compartidos DSH(α, h(α)) usando las partes SH(i, β, α, h(α)) donde i = 1, …, n + ζ, β = 1, …, n

+ ζ ; el uno de los valores comunes $\sigma(\alpha)$ y el vector n dimensional $\vec{w}$ y cada uno de los valores de secretos compartidos DSH(α, h(α)) es DSH(α, h(α)) = $\sigma(\alpha)\cdot\{\sum_{\mu=1}^{n} w_\mu \cdot SHb_\mu^*(\alpha, h(\alpha))\} + \sum_{\mu=n+1}^{n+\zeta} SHb_\mu^*(\alpha, h(\alpha)) \in G^{n+\zeta}$ con respecto a un vector de base de partes (n + ζ) dimensional $SHb_i^*(\alpha, h(\alpha))$ = SH(i, 1, α, h(α)), ..., SH(i, n + ζ , α, h(α)) $\in G^{n+\zeta}$ formado de (n + ζ) partes SH(i, 1, α, h(α)), ..., SH(i, n + ζ , α, h(α)); y

cada uno de los valores de secretos reconstruidos SUBSK(α) es SUBSK(α) = $\sigma(\alpha)\cdot\{\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*\} + \sum_{\mu=n+1}^{n+\zeta} b_\mu^* \in G^{n+\zeta}$.

15. El sistema de compartición de secretos según la Reivindicación 14, en donde la unidad de composición (835) está adaptada para calcular la información de generación SK = $\{(\sigma(1) + \ldots + \sigma(L))/L\}\cdot\{\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*\} + \sum_{\mu=n+1}^{n+\zeta} b_\mu^*$.

16. Un aparato de compartición que comprende unidades de compartición de secretos (114-α) adaptado para recibir información secreta, para generar partes SH(α, h(α))) por compartición de secretos de la información secreta separadamente para los subconjuntos SUB(α) respectivos, cada uno de los subconjuntos SUB(α) que está formado de H(α) aparatos de gestión de partes PA(α, 1), ..., PA(α, H(α)), α = 1, ..., L, L $\geq$ 2, h(α) = 1, ..., H(α), H(α) $\geq$ 2 y para sacar las partes SH(α, h(α)),
el aparato de compartición **caracterizado por que** la información secreta es un conjunto de vectores de base bi* que son b_1^*, ..., $b_{n+\zeta}^*$ de SUBSK(α) = $\sigma(\alpha)\cdot\{\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*\} + \sum_{\mu=n+1}^{n+\zeta} b_\mu^* \in G^{n+\zeta}$, donde g es un generador de un grupo cíclico G, θ (i, β) es un elemento de un campo finito F_q, i = 1, ..., n + ζ , β = 1, ..., n + ζ , n $\geq$ 1, $\zeta \geq 1$ y b_i^* = (θ (i, 1)·g, ..., θ (i, n + ζ)·g) $\in G^{n+\zeta}$ es un vector de base (n + ζ) dimensional que tiene (n + ζ) elementos del grupo cíclico G como elementos, $\vec{w}$ es un vector n dimensional $\vec{w}$ = (w_1, ..., w_n) que tiene elementos del campo finito F_q como elementos w_μ, μ = 1, ..., n y $\sigma(\alpha)$ es un valor común $\sigma(\alpha)$ compartido en cada uno de los subconjuntos SUB(α); y
cada una de las unidades de compartición de secretos (814-α) está adaptada para generar partes SH(i, β, α, h(α)) $\in$ G por compartición de secretos de los elementos $\theta(i, \beta)\cdot g \in$ G de los vectores de base b_i^* separadamente para los subconjuntos SUB(α) respectivos y cada una de las partes SH(α, h(α)) es un conjunto de las partes SH(i, β, α, h(α))$\in$ G donde i = 1, ..., n + ζ , β = 1, ..., n + ζ .

17. Un aparato de gestión de partes **caracterizado por que** comprende:

un generador de valores de secretos compartidos (124-α, h(α)) adaptado para generar un valor de secreto compartido DSH(α, h(α)) realizando una operación común a una de las partes SH(α, h(α)) obtenida por compartición de secretos de la información secreta separadamente para cada uno de los subconjuntos SUB(α) y la información común que contiene uno de los valores comunes $\sigma(\alpha)$, cada uno de los valores comunes $\sigma(\alpha)$ que está compartido en cada uno de los subconjuntos SUB(α), el uno de los valores comunes $\sigma(\alpha)$ que está compartido en uno de los subconjuntos SUB(α), cada uno de los subconjuntos SUB(α) que está formado de H(α) aparatos de gestión de partes PA(α, 1), ..., PA(α, H(α)) y para sacar el valor de secreto compartido DSH(α, h(α)), donde α = 1, ..., L, L $\geq$ 2, h(α) = 1, ..., H(α), H(α) $\geq$ 2;
la información común se comparte con los aparatos de gestión de partes PA(α, h(α)) que pertenecen al mismo de los subconjuntos SUB(α); y
la operación común se realiza por los aparatos de gestión de partes PA(α, h(α)) que pertenecen al mismo de los subconjuntos SUB(α).

18. El aparato de gestión de partes según la Reivindicación 17, en donde los valores comunes $\sigma(\alpha)$ compartidos en diferentes subconjuntos SUB(α) son independientes unos de otros.

19. El aparato de gestión de partes según una de las Reivindicaciones 17 y 18, en donde la operación común se

realiza por todos los generadores de valores de secretos compartidos (124-α-h(α)) de los aparatos de gestión de partes PA(α, h(α)) donde α = 1, …, L.

20. El aparato de gestión de partes según la Reivindicación 17, en donde la información común contiene el uno de los valores comunes $\sigma(\alpha)$ y la información común proporcionada a todos los aparatos de gestión de partes PA(α, h(α)), proporcionada por el aparato de adquisición (130).

21. El aparato de gestión de partes según la Reivindicación 20, en donde la información proporcionada es un vector n dimensional $\vec{w}$ = (w_1, …, w_n) que tiene elementos de un campo finito F_q como elementos w_μ (μ =1, …, n); y
el generador de valores de secretos compartidos (824-α-h(α)) genera el valor de secreto compartido DSH(α, h(α)) usando las partes SH(i, β, α, h(α)), el uno del valor común $\sigma(\alpha)$ y el vector n dimensional $\vec{w}$; y
el valor de secreto compartido DSH(α, h(α)) es
DSH(α, h (α)) = $\sigma(\alpha)\cdot\{\sum_{\mu=1}^{n} w_\mu \cdot SHb_\mu^*(\alpha, h(\alpha))\} + \sum_{\mu=n+1}^{n+\zeta} SHb_\mu^*(\alpha, h(\alpha)) \in G^{n+\zeta}$ con respecto a un vector de base de parte (n + ζ) dimensional $SHb_i^*(\alpha, h(\alpha))$ = (SH(i, 1, α, h(α)), …, SH(i, n + ζ, α, h(α)) $\in$ $G^{n+\zeta}$ formado de (n + ζ) partes SH(i, 1, α, h(α)), …, SH(i, n + ζ, α, h(α)) donde $\zeta \geq 1$.

22. Un aparato de adquisición que comprende:

unidades de reconstrucción (134-α) adaptadas para generar valores de secretos reconstruidos SUBSK(α) que corresponden a subconjuntos SUB(α) respectivamente, cada uno de los subconjuntos SUB(α) que están formados de H(α) aparatos de gestión de partes PA(α, 1), …, PA(α, H(α)), cada uno de los valores de secretos reconstruidos SUBSK(α) que se genera por procesamiento de reconstrucción con un esquema de compartición de secretos para cada uno de los subconjuntos SUB(α) usando una pluralidad de valores de secretos compartidos DSH(α, h(α)) que corresponde al mismo de los subconjuntos SUB(α), α = 1, …, L, L $\geq$ 2, h(α) = 1, …, H(α), H(α) $\geq$ 2; y
una unidad de composición (137) adaptada para generar información de generación SK usando los valores de secretos reconstruidos SUBSK(α) y para sacar la información de generación SK,
el aparato de adquisición **caracterizado por que** además comprende:

una unidad de salida (135) para sacar un vector n dimensional $\vec{w}$ = (w_1, …, w_n) que tiene elementos de un campo finito F_q como elementos w_μ donde μ = 1, …, n); en donde
cada uno de los valores de secretos reconstruidos SUBSK(α) es SUBSK(α) = $\sigma(\alpha)\cdot\{\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*\} + \sum_{\mu=n+1}^{n+\zeta} b_\mu^* \in G^{n+\zeta}$, donde $\sigma(\alpha)$ es un valor común compartido de cada uno de los subconjuntos SUB(α), g es un generador de un grupo cíclico G, θ (i, β) es un elemento del campo finito F_q, i = 1, …, n + ζ, β = 1, …, n + ζ, n $\geq$ 1, $\zeta \geq 1$ y b_i^* = (θ (i, 1)·g, …, θ (i, n + ζ)·g) $\in$ $G^{n+\zeta}$ es un vector de base (n + ζ) dimensional que tiene (n + ζ) elementos del grupo cíclico G como elementos.

23. El aparato de adquisición según la Reivindicación 22, en donde la unidad de composición (835) está adaptada para calcular la información de generación SK = $\{(\sigma(1) + \ldots + \sigma(L))/L\}\cdot\{\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*\} + \sum_{\mu=n+1}^{n+\zeta} b_\mu^*$.

24. Un método de compartición de secretos **caracterizado por que** comprende los pasos de:

(a) generar en un aparato de compartición (110), partes SH(α, h(α)) por compartición de secretos de información secreta con un esquema de compartición de secretos separadamente para subconjuntos SUB(α) respectivos, donde α = 1, …, L, L $\geq$ 2, cada uno de los subconjuntos SUB(α) que está formado de H(α) aparatos de gestión de partes PA(α, 1), …, PA(α, H(α)) que pertenecen a un conjunto formado de $\sum_{\alpha=1}^{L}$ h(α) aparatos de gestión de partes PA(α, h(α)), donde h(α) = 1, …, H(α), H(α) $\geq$ 2 y que saca las partes SH(α, h(α));
(b) generar, en cada uno de los aparatos de gestión de partes PA(α, h(α)), un valor de secreto compartido DSH(α, h(α)) realizando una operación común a una de las partes SH(α, h(α)) e información común que contiene uno de los valores comunes $\sigma(\alpha)$, cada uno de los valores comunes $\sigma(\alpha)$ que está compartido en cada uno de los subconjuntos SUB(α) y que saca el valor de secreto compartido DSH(α,

h(α));
(c) generar, en un aparato de adquisición (130), valores de secretos compartidos SUBSK(α) que corresponden a los subconjuntos SUB(α) respectivamente, cada uno de los valores de secretos reconstruidos SUBSK(α) que se genera por procesamiento de reconstrucción con el esquema de compartición de secretos para cada uno de los subconjuntos SUB(α), usando una pluralidad de valores de secretos compartidos DSH(α, h(α)) que corresponden al mismo de los subconjuntos SUB(α); y
(d) generar, en un aparato de adquisición (130), información de generación SK usando los valores de secretos reconstruidos SUBSK(α) y sacando la información de generación SK;
en el paso (b), la información común usada por los aparatos de gestión de partes PA(α, h(α)) que pertenecen al mismo de los subconjuntos SUB(α) que son el mismo y los aparatos de gestión de partes PA(α, h(α)) que pertenecen al mismo de los subconjuntos SUB(α) que realizan la misma operación común.

25. Un método de procesamiento para un aparato de compartición, el método de procesamiento que comprende los pasos de:

introducir información secreta al aparato de compartición (110);
generar partes SH(α, h(α)) por compartición de secretos de la información secreta separadamente para subconjuntos SUB(α) respectivos, cada uno de los subconjuntos SUB(α) que está formado de H(α) aparatos de gestión de partes PA(α, 1), …, PA(α, H(α)), donde α = 1, …, L, L $\geq$ 2, h(α) = 1, …, H(α), H(α) $\geq$ 2, en los primeros medios del aparato de compartición (110); y
sacar las partes SH(α, h(α)), en los segundos medios del aparato de compartición (110),
el método de procesamiento **caracterizado por que** la información secreta es un conjunto de vectores de base b_i* que son b_1*, …, $b_{n+\zeta}$* de SUBSK(α) = $\sigma(\alpha)\cdot\{\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*\} + \sum_{\mu=n+1}^{n+\zeta} b_\mu^* \in G^{n+\zeta}$, donde g es un generador de un grupo cíclico G, θ (i, β) es un elemento de un campo finito F_q, i = 1, …, n + ζ, β = 1, …, n + ζ, n $\geq$ 1, $\zeta \geq 1$ y $b_i^* = (\theta(i, 1)\cdot g, \ldots, \theta(i, n+\zeta)\cdot g) \in G^{n+\zeta}$ es un vector de base (n + ζ) dimensional que tiene (n + ζ) elementos del grupo cíclico G como elementos, $\vec{w}$ es un vector n dimensional $\vec{w} = (w_1, \ldots, w_n)$ que tiene elementos del campo finito F_q como elementos w_μ, μ = 1, …, n y $\sigma(\alpha)$ es un valor común $\sigma(\alpha)$ compartido en cada uno de los subconjuntos SUB(α); y
cada una de las unidades de compartición de secretos (814-α) está adaptada para generar partes SH(i, β, α, h(α))$\in$ G por compartición de secretos de los elementos $\theta(i,\beta)\cdot g \in G$ de los vectores de base b_i* separadamente para subconjuntos SUB(α) respectivos y cada una de las partes SH(α, h(α)) es un conjunto de las partes SH(i, β, α, h(α))$\in$ G donde i = 1, …, n + ζ, β = 1, …, n + ζ.

26. Un método de procesamiento para un aparato de gestión de partes, **caracterizado por que** el método de procesamiento comprende los pasos de:

generar un valor de secreto compartido DSH(α, h(α)) realizando una operación común a una de las partes SH(α, h(α)) obtenida compartiendo secretos de información secreta separadamente para cada uno de los subconjuntos SUB(α) y la información común que contiene uno de los valores comunes $\sigma(\alpha)$, cada uno de los valores comunes $\sigma(\alpha)$ que está compartido en cada uno de los subconjuntos SUB(α), el uno de los valores comunes $\sigma(\alpha)$ que está compartido en uno de los subconjuntos SUB(α), cada uno de los subconjuntos SUB(α) que está formado de H(α) aparatos de gestión de partes PA(α, 1), …, PA(α, H(α)), donde α = 1, …, L, L $\geq$ 2, h(α) = 1, …, H(α), H(α) $\geq$ 2, en los primeros medios del aparato de gestión de partes; y
sacar el valor de secreto compartido DSH(α, h(α)), en los segundos medios del aparato de gestión de partes;
la información común está compartida con los aparatos de gestión de partes PA(α, h(α)) que pertenecen al mismo de los subconjuntos SUB(α) y la operación común se realiza por los aparatos de gestión de partes PA(α, h(α)) que pertenecen al mismo de los subconjuntos SUB(α).

27. Un método de procesamiento para un aparato de adquisición, **caracterizado por que** el método de procesamiento comprende los pasos de:

generar, en los primeros medios del aparato de adquisición (130), valores de secretos reconstruidos SUBSK(α) que corresponden a subconjuntos SUB(α) respectivamente, cada uno de los subconjuntos SUB(α) que está formado de H(α) aparatos de gestión de partes PA(α, 1), …, PA(α, H(α)), cada uno

de los valores de secretos reconstruidos SUBSK(α) que se genera por procesamiento de reconstrucción con un esquema de compartición de secretos para cada uno de los subconjuntos SUB(α), usando una pluralidad de valores de secretos compartidos DSH(α, h(α)) que corresponden al mismo de los subconjuntos SUB(α), donde cada uno de los subconjuntos SUB(α) es un subconjunto formado de H(α) aparatos de gestión de partes PA(α, 1), …, PA(α, H(α)), α = 1, …, L, L $\geq$ 2, h(α) = 1, …, H(α), H(α) $\geq$ 2; y
generar, en los segundos medios del aparato de adquisición (130), información de generación SK usando los valores de secretos reconstruidos SUBSK(α) y sacar la información de generación SK,
el método de procesamiento **caracterizado por que** además comprende un paso de sacar, desde una unidad de salida (135), un vector n dimensional $\vec{w}$ = (w_1, …, w_n) que tiene elementos de un campo finito F_q como elementos w_μ, μ = 1, …, n, en donde

cada uno de los valores de secretos reconstruidos SUBSK(α) es SUBSK(α) = $\sigma(\alpha)\cdot\{\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*\} + \sum_{\mu=n+1}^{n+\zeta} b_\mu^* \in G^{n+\zeta}$, donde $\sigma(\alpha)$ es un valor común compartido en cada uno de los subconjuntos SUB(α), g es un generador de un grupo cíclico G, θ (i, β) es un elemento del campo finito F_q, i = 1, …, n + ζ, β = 1, …, n + ζ, n $\geq$ 1, $\zeta \geq 1$ y $b_i^* = (\theta(i, 1)\cdot g, \ldots, \theta(i, n + \zeta)\cdot g) \in G^{n+\zeta}$ es un vector de base (n + ζ) dimensional que tiene (n + ζ) elementos del grupo cíclico G como elementos.

28. El método de procesamiento según la Reivindicación 27, en donde la información de generación SK es SK = $\{(\sigma(1) + \ldots + \sigma(L))/L\}\cdot\{\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*\} + \sum_{\mu=n+1}^{n+\zeta} b_\mu^*$.

29. Un programa para hacer a un ordenador funcionar como el aparato de compartición según la Reivindicación 16.

30. Un programa para hacer a un ordenador funcionar como el aparato de gestión de partes según una de las Reivindicaciones 17 a 21.

31. Un programa para hacer a un ordenador funcionar como el aparato de adquisición según la Reivindicación 22 ó 23.

32. Un medio de grabación legible por ordenador que tiene almacenado en el mismo un programa para hacer a un ordenador funcionar como el aparato de compartición según la Reivindicación 16.

33. Un medio de grabación legible por ordenador que tiene almacenado en el mismo un programa para hacer a un ordenador funcionar como el aparato de gestión de partes según una de las Reivindicaciones 17 a 21.

34. Un medio de grabación legible por ordenador que tiene almacenado en el mismo un programa para hacer a un ordenador funcionar como el aparato de adquisición según la Reivindicación 22 ó 23.

FIG.1

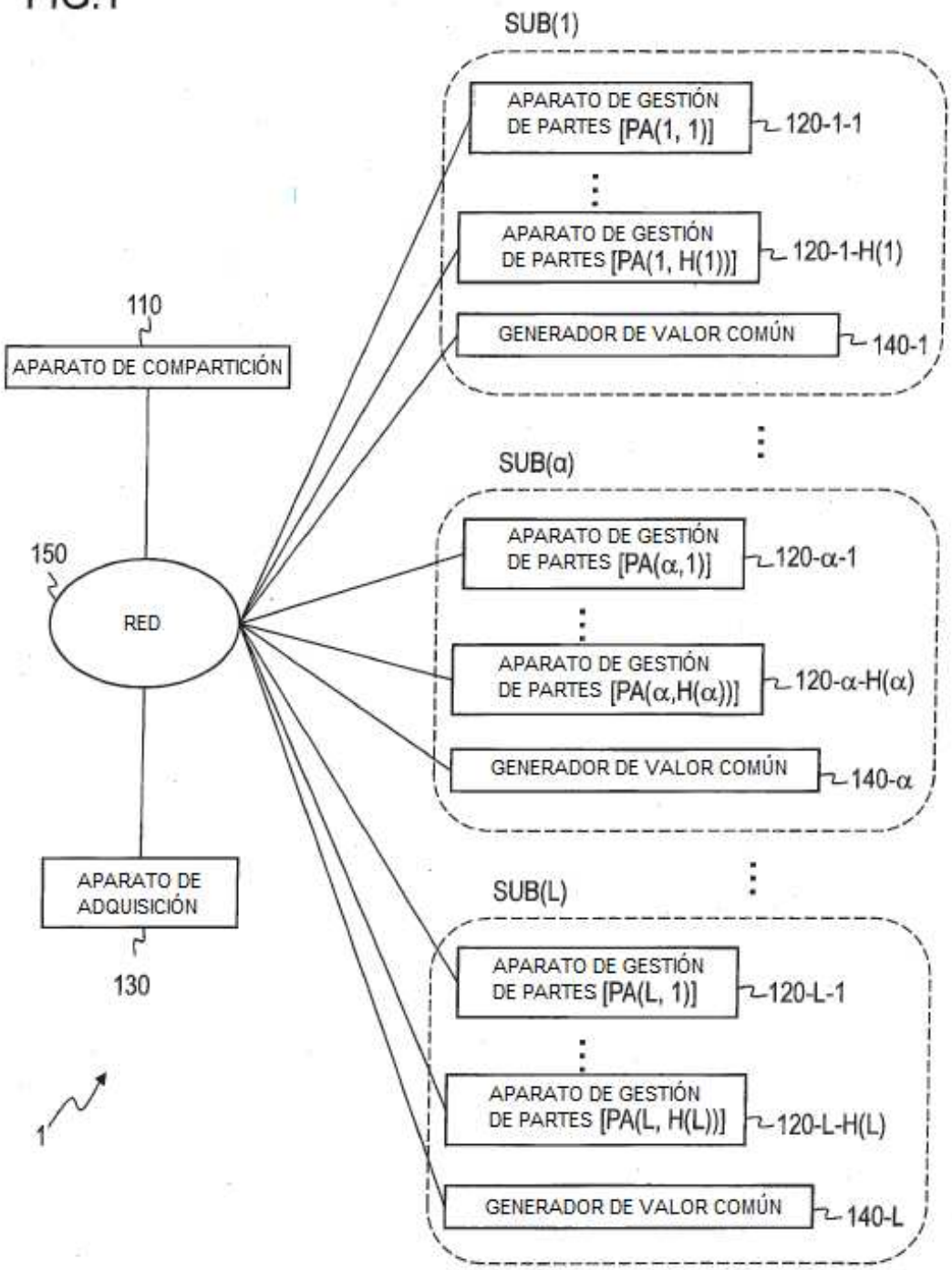

SUB(1)
APARATO DE GESTIÓN DE PARTES [PA(1, 1)]
120-1-1
APARATO DE GESTIÓN DE PARTES [PA(1, H(1))]
120-1-H(1)
GENERADOR DE VALOR COMÚN
140-1
SUB(α)
APARATO DE GESTIÓN DE PARTES [PA(α,1)]
120-α-1
APARATO DE GESTIÓN DE PARTES [PA(α,H(α))]
120-α-H(α)
GENERADOR DE VALOR COMÚN
140-α
SUB(L)
APARATO DE GESTIÓN DE PARTES [PA(L, 1)]
120-L-1
APARATO DE GESTIÓN DE PARTES [PA(L, H(L))]
120-L-H(L)
GENERADOR DE VALOR COMÚN
140-L
110
APARATO DE COMPARTICIÓN
150
RED
APARATO DE ADQUISICIÓN
130
1

FIG.2

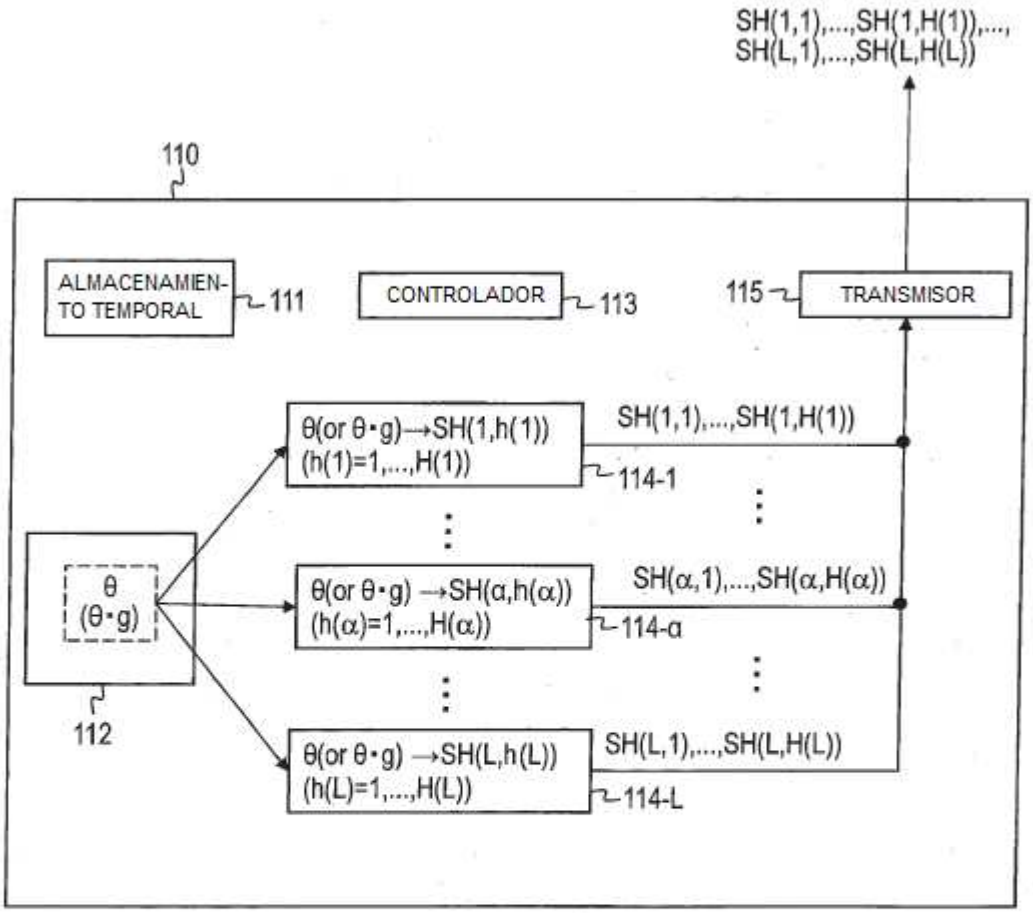

SH(1,1),...,SH(1,H(1)),...,
SH(L,1),...,SH(L,H(L))
110
ALMACENAMIEN-
TO TEMPORAL
111
CONTROLADOR
113
115
TRANSMISOR
θ(or θ•g)→SH(1,h(1))
(h(1)=1,...,H(1))
SH(1,1),...,SH(1,H(1))
114-1
θ
(θ•g)
θ(or θ•g) →SH(α,h(α))
(h(α)=1,...,H(α))
SH(α,1),...,SH(α,H(α))
114-α
112
θ(or θ•g) →SH(L,h(L))
(h(L)=1,...,H(L))
SH(L,1),...,SH(L,H(L))
114-L

FIG.3A

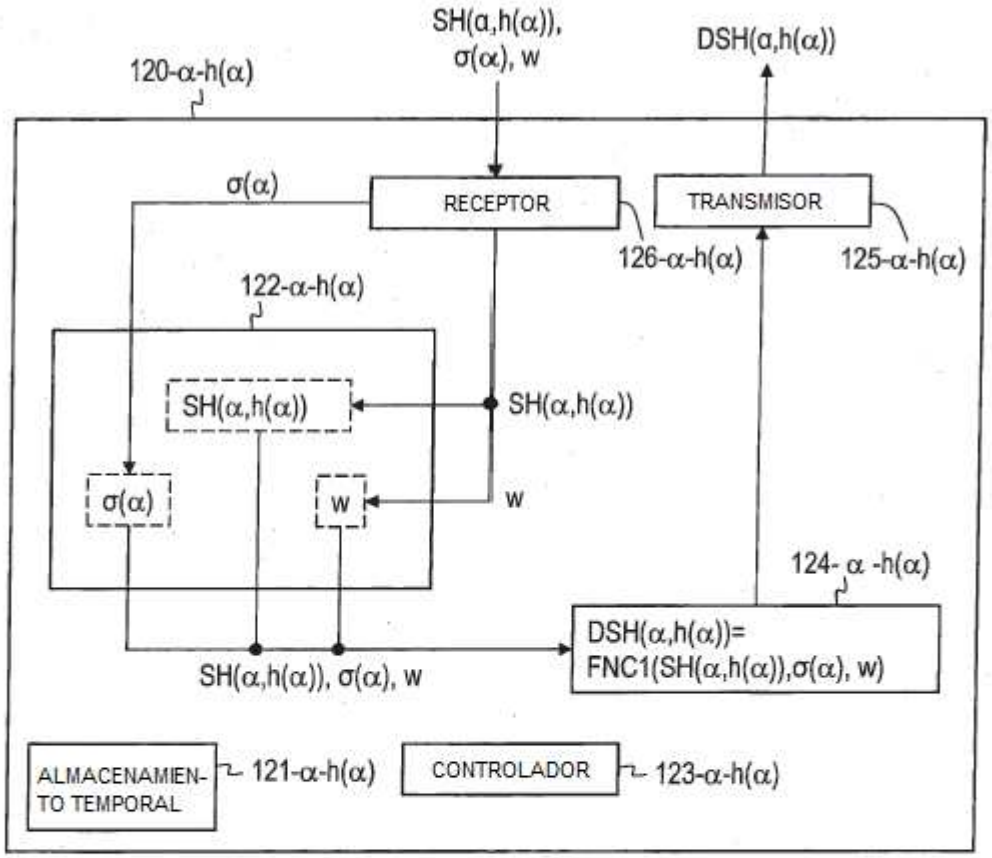

SH(α,h(α)),
σ(α), w
DSH(α,h(α))
120-α-h(α)
σ(α)
RECEPTOR
TRANSMISOR
126-α-h(α)
125-α-h(α)
122-α-h(α)
SH(α,h(α))
SH(α,h(α))
σ(α)
w
w
124- α -h(α)
DSH(α,h(α))=
FNC1(SH(α,h(α)),σ(α), w)
SH(α,h(α)), σ(α), w
ALMACENAMIEN-
TO TEMPORAL
121-α-h(α)
CONTROLADOR
123-α-h(α)

FIG.3B

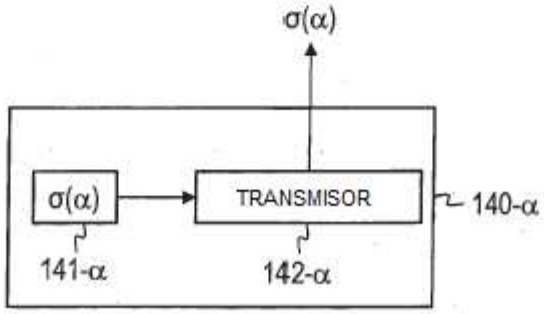

σ(α)
σ(α)
TRANSMISOR
140-α
141-α
142-α

FIG.4

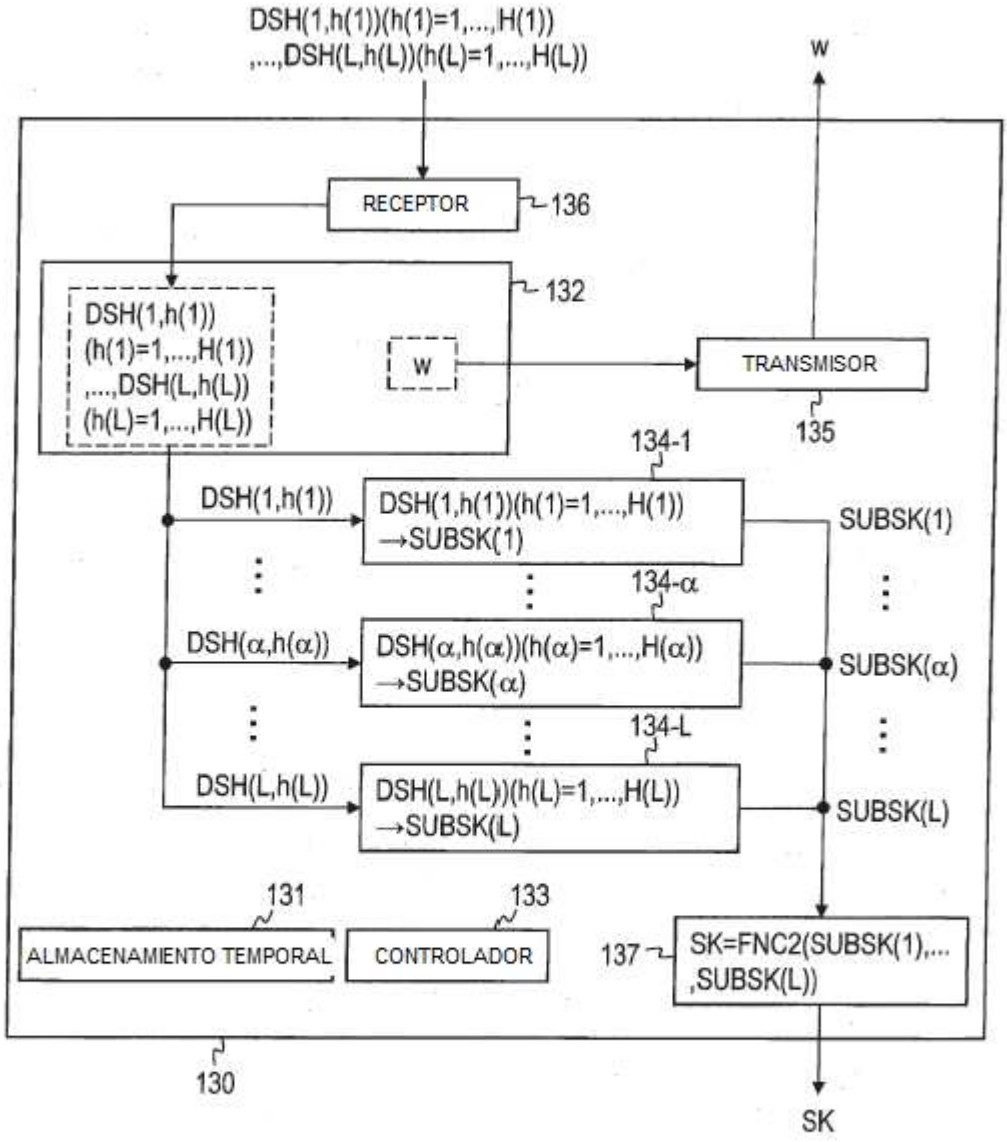

DSH(1,h(1))(h(1)=1,...,H(1))
,...,DSH(L,h(L))(h(L)=1,...,H(L))
W
RECEPTOR
136
132
DSH(1,h(1))
(h(1)=1,...,H(1))
,...,DSH(L,h(L))
(h(L)=1,...,H(L))
W
TRANSMISOR
135
134-1
DSH(1,h(1))
DSH(1,h(1))(h(1)=1,...,H(1))
→SUBSK(1)
SUBSK(1)
134-α
DSH(α,h(α))
DSH(α,h(α))(h(α)=1,...,H(α))
→SUBSK(α)
SUBSK(α)
134-L
DSH(L,h(L))
DSH(L,h(L))(h(L)=1,...,H(L))
→SUBSK(L)
SUBSK(L)
131
ALMACENAMIENTO TEMPORAL
133
CONTROLADOR
137
SK=FNC2(SUBSK(1),...
,SUBSK(L))
130
SK

FIG.5A

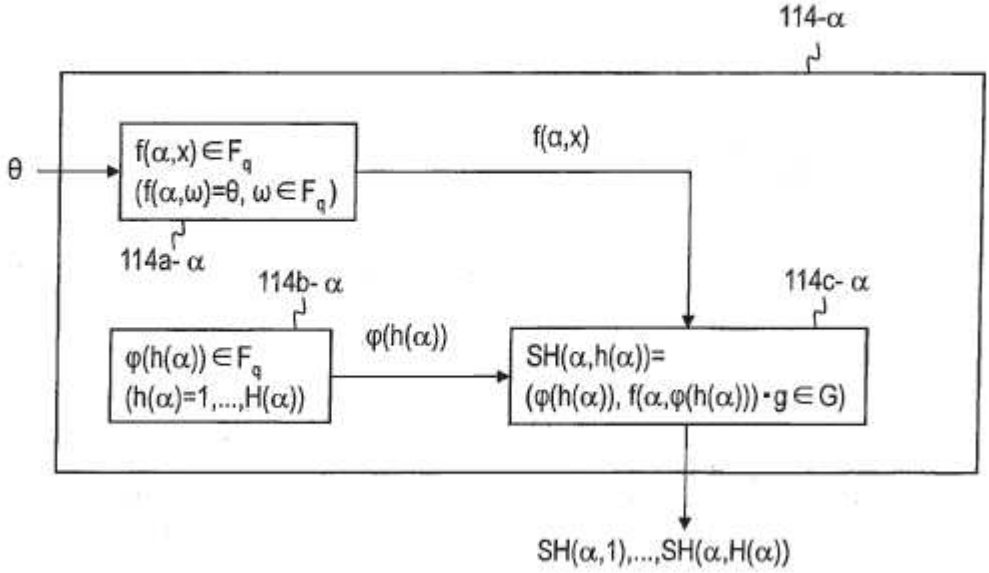

114-α
θ
f(α,x)∈F_q
(f(α,ω)=θ, ω∈F_q)
f(α,x)
114a-α
114b-α
114c-α
φ(h(α))∈F_q
(h(α)=1,...,H(α))
φ(h(α))
SH(α,h(α))=
(φ(h(α)), f(α,φ(h(α)))·g∈G)
SH(α,1),...,SH(α,H(α))

FIG.5B

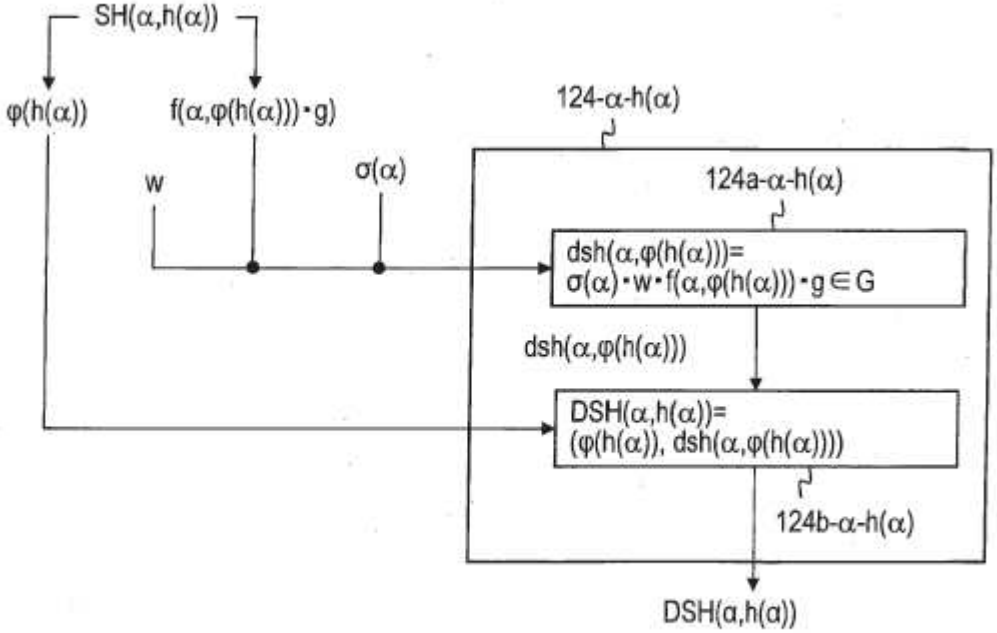

SH(α,h(α))
φ(h(α))
f(α,φ(h(α)))·g)
124-α-h(α)
w
σ(α)
124a-α-h(α)
dsh(α,φ(h(α)))=
σ(α)·w·f(α,φ(h(α)))·g∈G
dsh(α,φ(h(α)))
DSH(α,h(α))=
(φ(h(α)), dsh(α,φ(h(α))))
124b-α-h(α)
DSH(α,h(α))

FIG.6

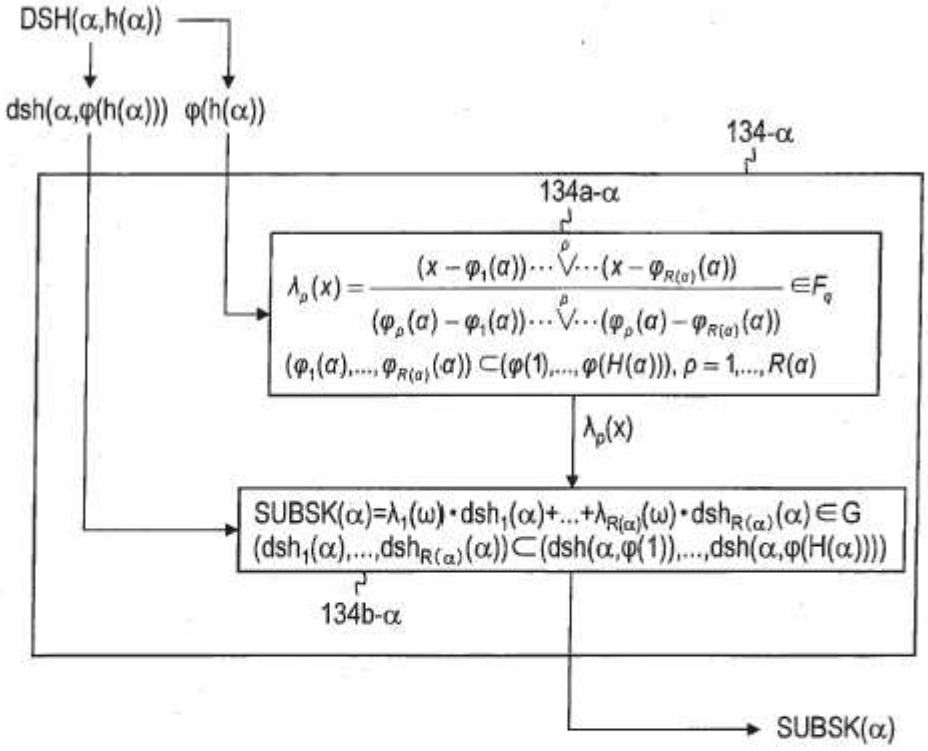

DSH(α,h(α))
dsh(α,φ(h(α)))
φ(h(α))
134-α
134a-α
$\lambda_\rho(x)=\frac{(x-\varphi_1(\alpha))\cdots\overset{\rho}{\vee}\cdots(x-\varphi_{R(\alpha)}(\alpha))}{(\varphi_\rho(\alpha)-\varphi_1(\alpha))\cdots\overset{\rho}{\vee}\cdots(\varphi_\rho(\alpha)-\varphi_{R(\alpha)}(\alpha))}\in F_q$
$(\varphi_1(\alpha),\ldots,\varphi_{R(\alpha)}(\alpha))\subset(\varphi(1),\ldots,\varphi(H(\alpha))),\ \rho=1,\ldots,R(\alpha)$
$\lambda_\rho(x)$
$SUBSK(\alpha)=\lambda_1(\omega)\cdot dsh_1(\alpha)+\ldots+\lambda_{R(\alpha)}(\omega)\cdot dsh_{R(\alpha)}(\alpha)\in G$
$(dsh_1(\alpha),\ldots,dsh_{R(\alpha)}(\alpha))\subset(dsh(\alpha,\varphi(1)),\ldots,dsh(\alpha,\varphi(H(\alpha))))$
134b-α
SUBSK(α)

FIG.7

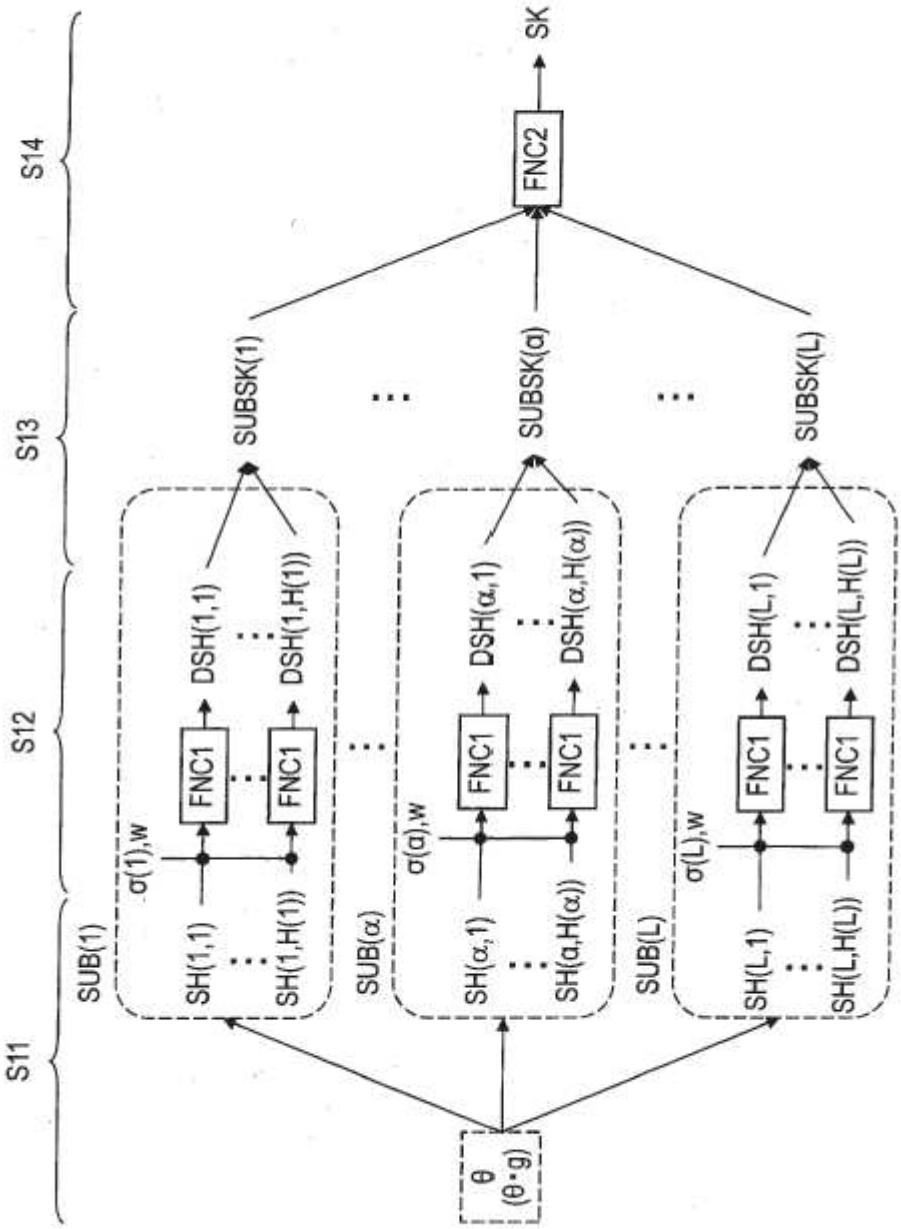

S11
S12
S13
S14
SUB(1)
SUB(α)
SUB(L)
SH(1,1)
SH(1,H(1))
SH(α,1)
SH(α,H(α))
SH(L,1)
SH(L,H(L))
σ(1),w
σ(α),w
σ(L),w
FNC1
DSH(1,1)
DSH(1,H(1))
DSH(α,1)
DSH(α,H(α))
DSH(L,1)
DSH(L,H(L))
SUBSK(1)
SUBSK(α)
SUBSK(L)
FNC2
SK
θ
(θ·g)

FIG.8A

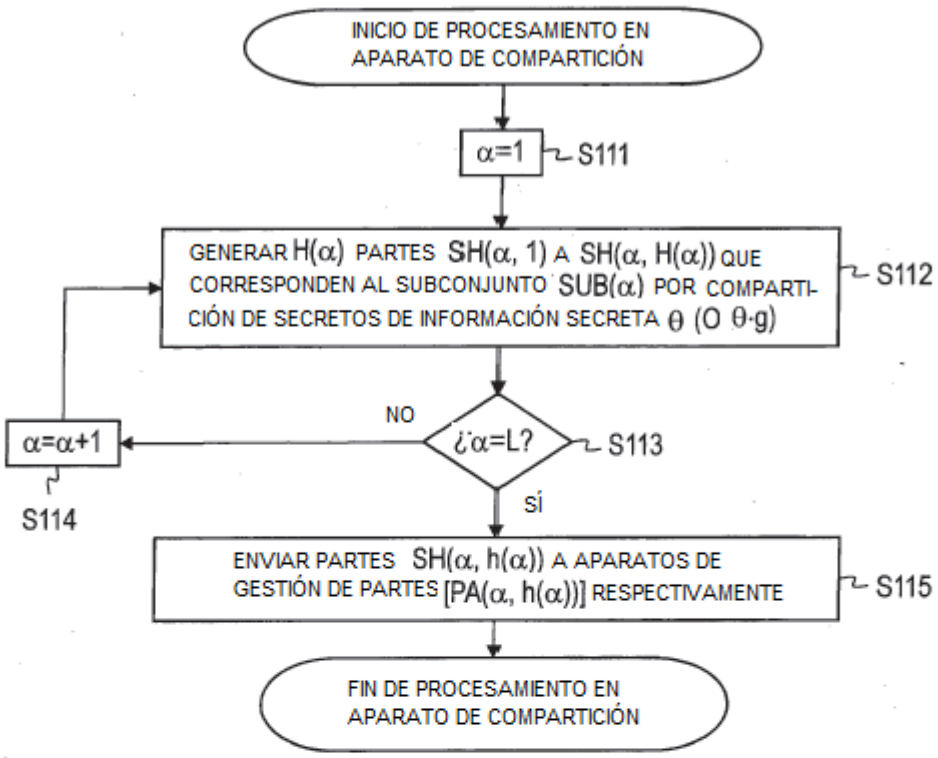

INICIO DE PROCESAMIENTO EN APARATO DE COMPARTICIÓN
α=1
S111
GENERAR H(α) PARTES SH(α, 1) A SH(α, H(α)) QUE CORRESPONDEN AL SUBCONJUNTO SUB(α) POR COMPARTICIÓN DE SECRETOS DE INFORMACIÓN SECRETA θ (O θ·g)
S112
NO
¿α=L?
S113
α=α+1
S114
SÍ
ENVIAR PARTES SH(α, h(α)) A APARATOS DE GESTIÓN DE PARTES [PA(α, h(α))] RESPECTIVAMENTE
S115
FIN DE PROCESAMIENTO EN APARATO DE COMPARTICIÓN

FIG.8B

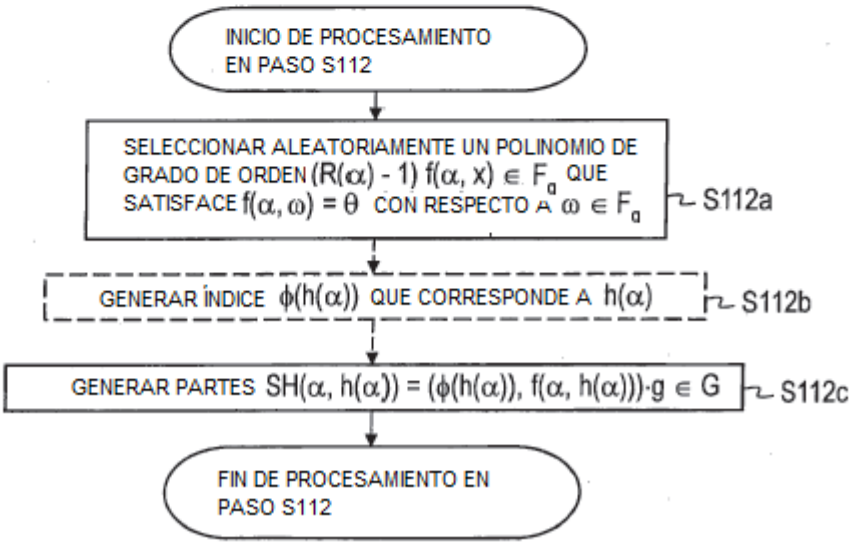

INICIO DE PROCESAMIENTO EN PASO S112
SELECCIONAR ALEATORIAMENTE UN POLINOMIO DE GRADO DE ORDEN (R(α) - 1) f(α, x) ∈ Fq QUE SATISFACE f(α, ω) = θ CON RESPECTO A ω ∈ Fq
S112a
GENERAR ÍNDICE ϕ(h(α)) QUE CORRESPONDE A h(α)
S112b
GENERAR PARTES SH(α, h(α)) = (ϕ(h(α)), f(α, h(α)))·g ∈ G
S112c
FIN DE PROCESAMIENTO EN PASO S112

FIG.9A

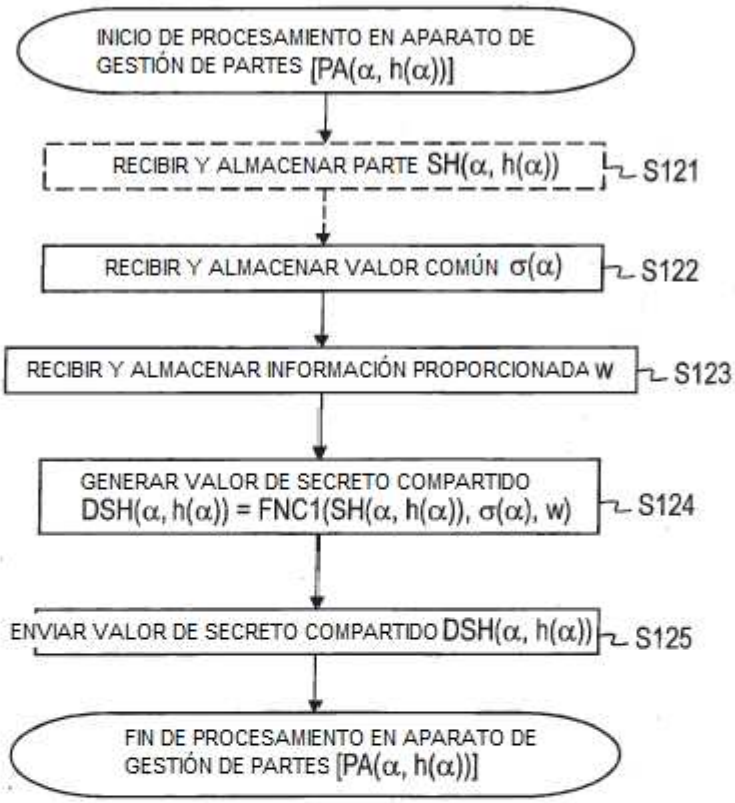

INICIO DE PROCESAMIENTO EN APARATO DE GESTIÓN DE PARTES [PA(α, h(α))]
RECIBIR Y ALMACENAR PARTE SH(α, h(α))
S121
RECIBIR Y ALMACENAR VALOR COMÚN σ(α)
S122
RECIBIR Y ALMACENAR INFORMACIÓN PROPORCIONADA w
S123
GENERAR VALOR DE SECRETO COMPARTIDO DSH(α, h(α)) = FNC1(SH(α, h(α)), σ(α), w)
S124
ENVIAR VALOR DE SECRETO COMPARTIDO DSH(α, h(α))
S125
FIN DE PROCESAMIENTO EN APARATO DE GESTIÓN DE PARTES [PA(α, h(α))]

FIG.9B

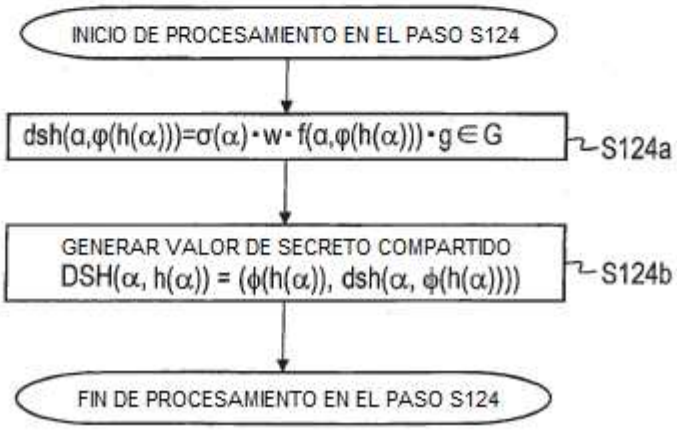

INICIO DE PROCESAMIENTO EN EL PASO S124
dsh(α,φ(h(α)))=σ(α)・w・f(α,φ(h(α)))・g∈G
S124a
GENERAR VALOR DE SECRETO COMPARTIDO DSH(α, h(α)) = (ϕ(h(α)), dsh(α, ϕ(h(α))))
S124b
FIN DE PROCESAMIENTO EN EL PASO S124

FIG.10A

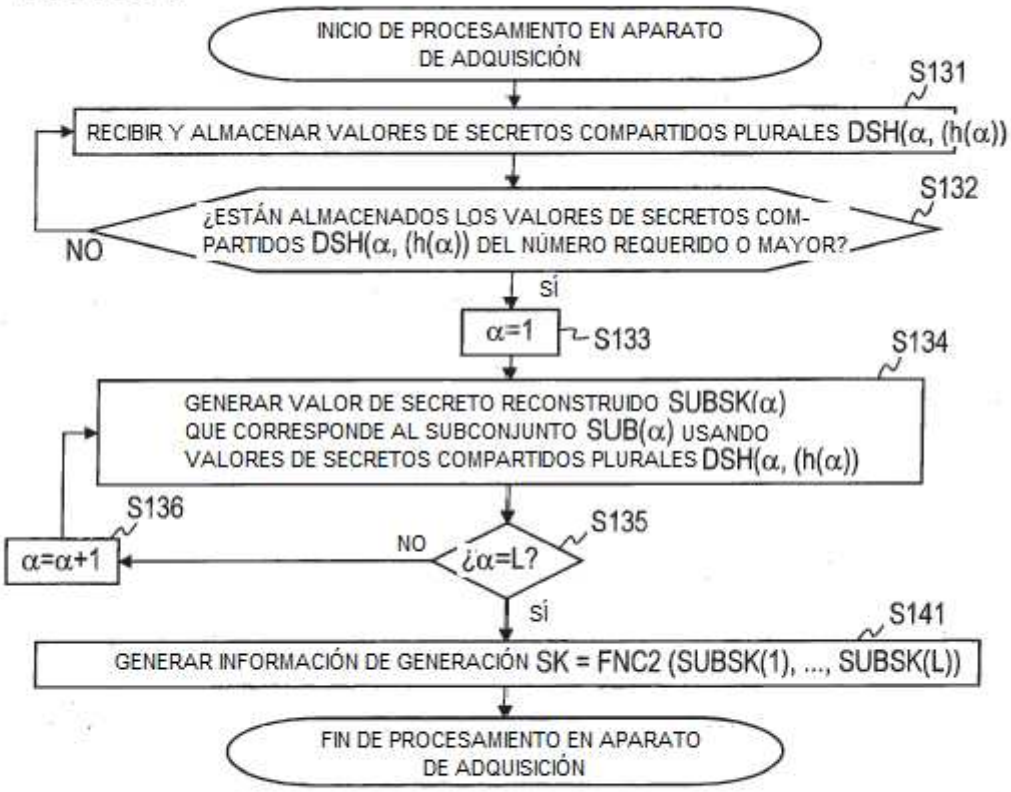


FIG.10B

FIG.11A

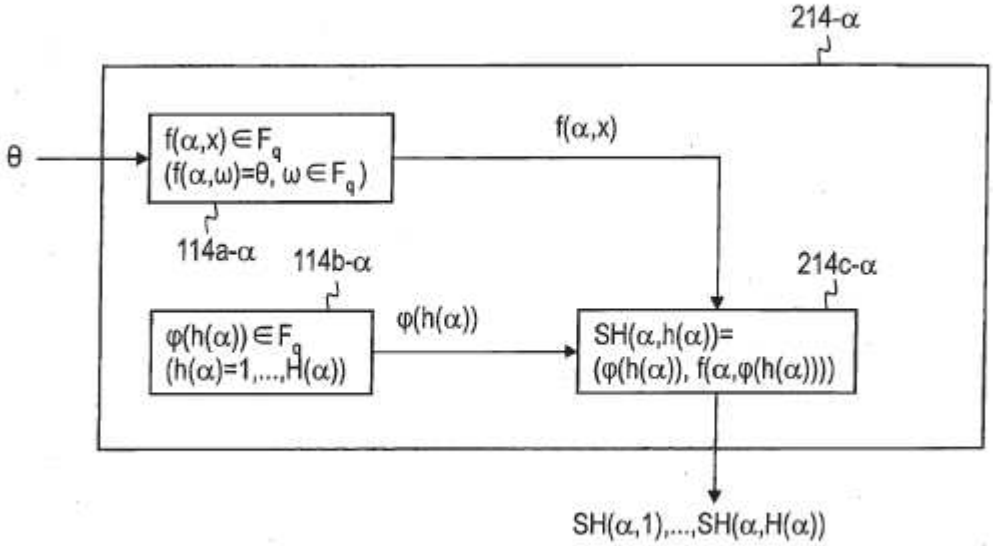


FIG.11B

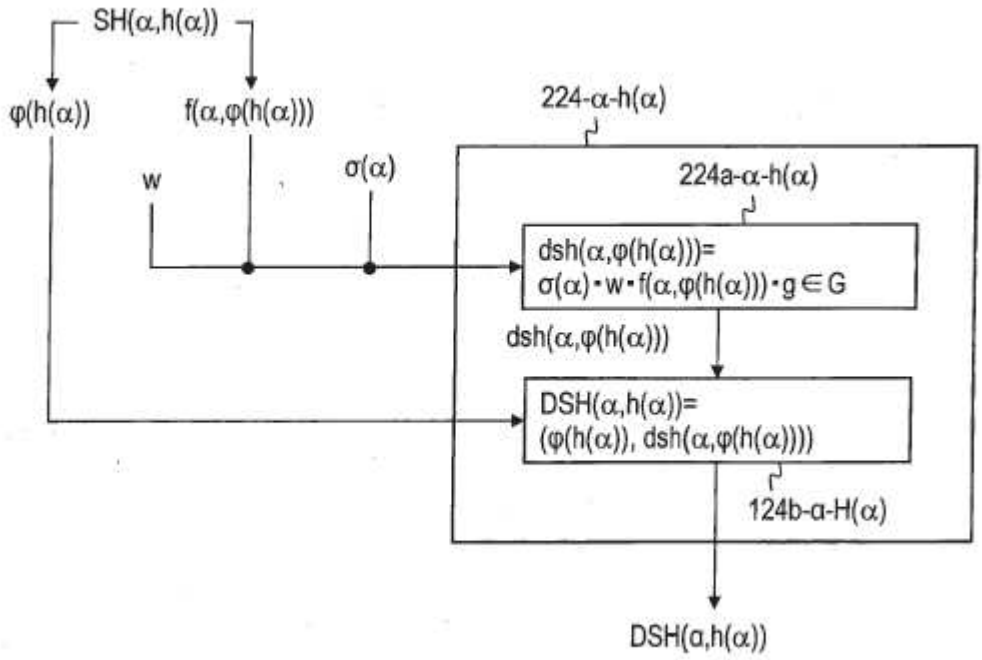


FIG.12A

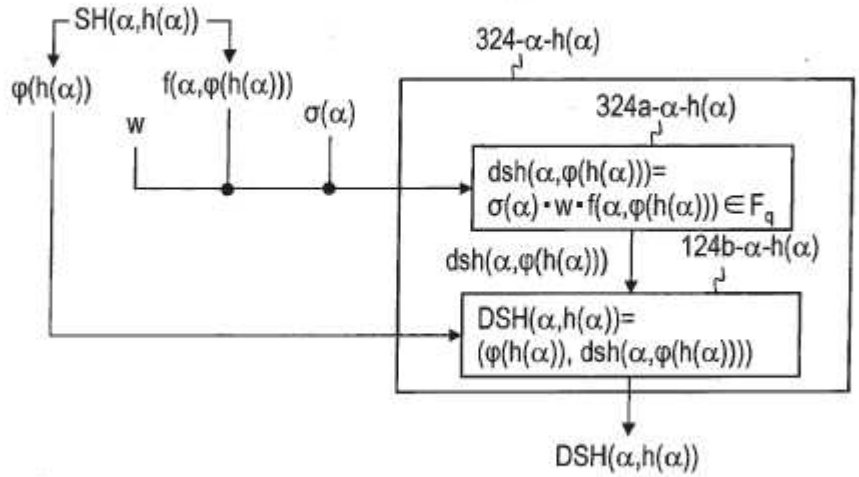


FIG.12B

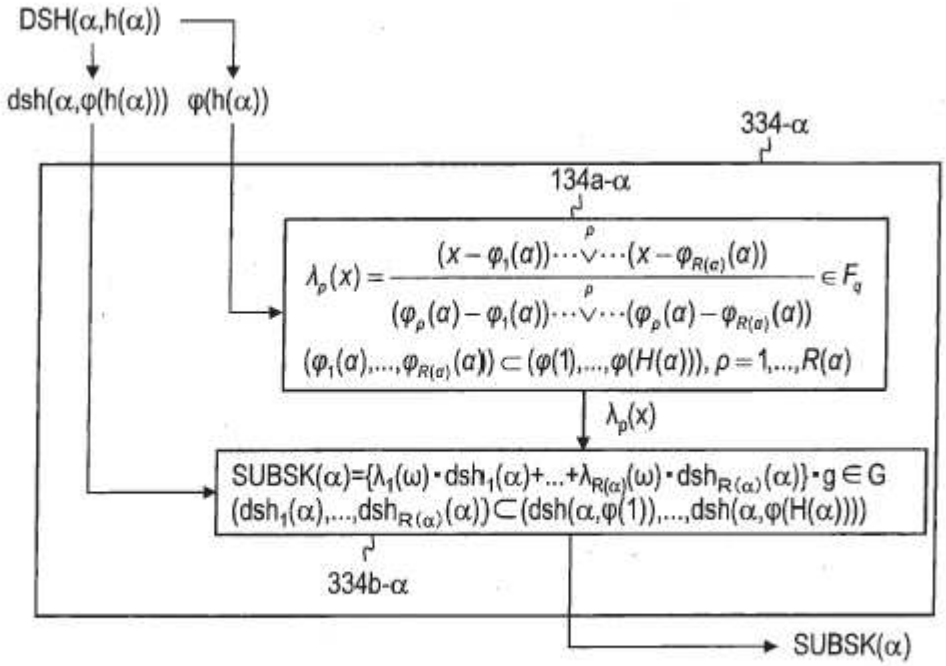


FIG.13A

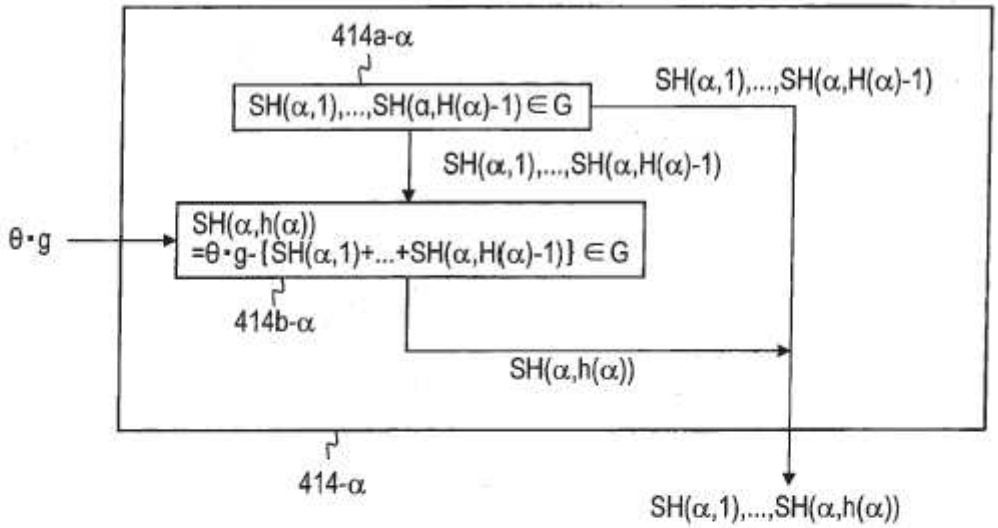


FIG.13B

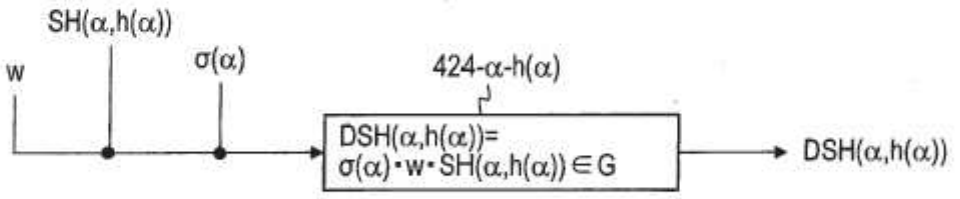


FIG.13C

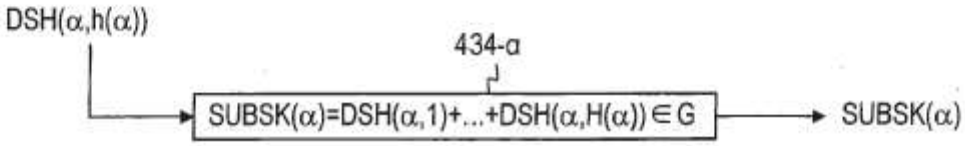


FIG.14A

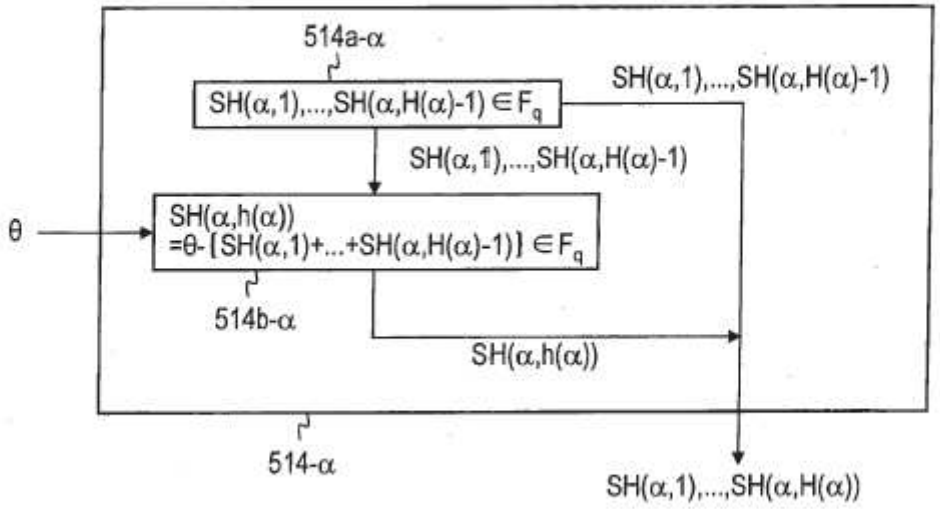


FIG.14B

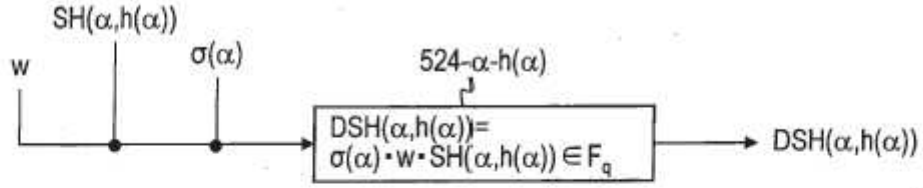


FIG.14C

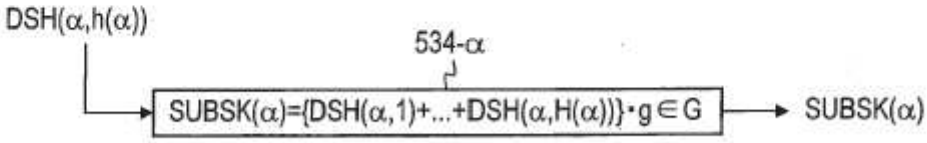


FIG.15

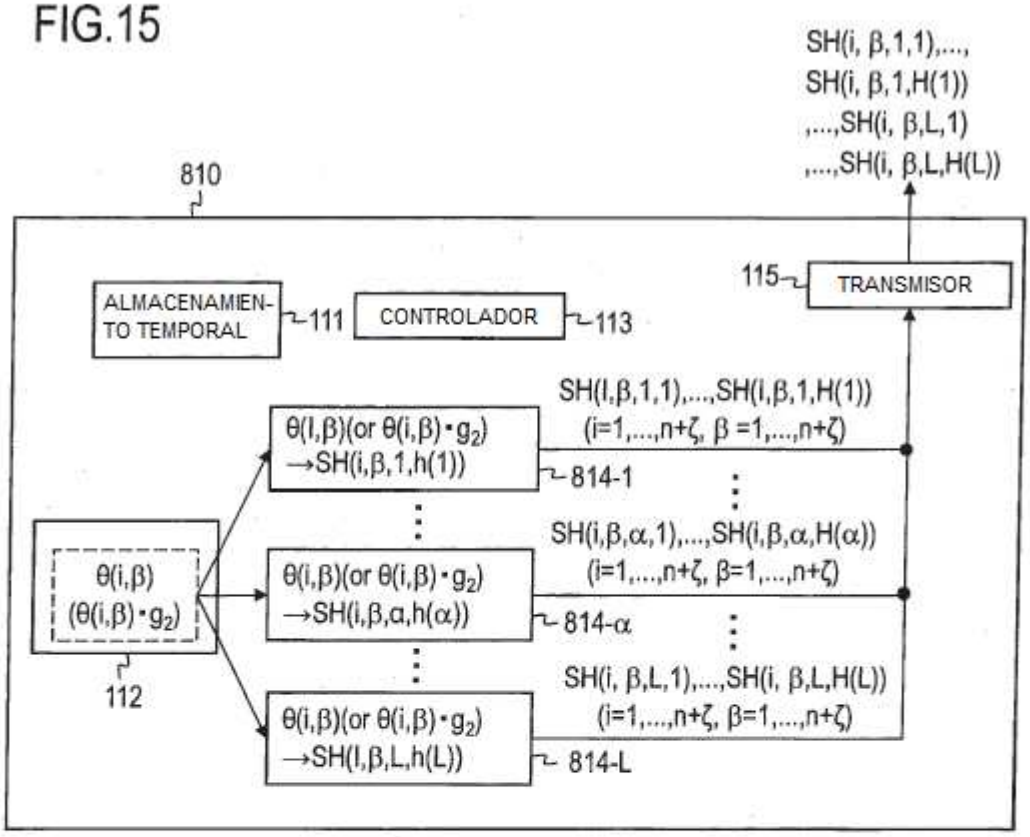

SH(i, β,1,1),...,
SH(i, β,1,H(1))
,...,SH(i, β,L,1)
,...,SH(i, β,L,H(L))
810
115
TRANSMISOR
ALMACENAMIEN-
TO TEMPORAL
111
CONTROLADOR
113
θ(i,β)
(θ(i,β)·g2)
112
θ(I,β)(or θ(i,β)·g2)
→SH(i,β,1,h(1))
SH(I,β,1,1),...,SH(i,β,1,H(1))
(i=1,...,n+ζ, β =1,...,n+ζ)
814-1
θ(i,β)(or θ(i,β)·g2)
→SH(i,β,α,h(α))
SH(i,β,α,1),...,SH(i,β,α,H(α))
(i=1,...,n+ζ, β=1,...,n+ζ)
814-α
θ(i,β)(or θ(i,β)·g2)
→SH(I,β,L,h(L))
SH(i, β,L,1),...,SH(i, β,L,H(L))
(i=1,...,n+ζ, β=1,...,n+ζ)
814-L

FIG.16

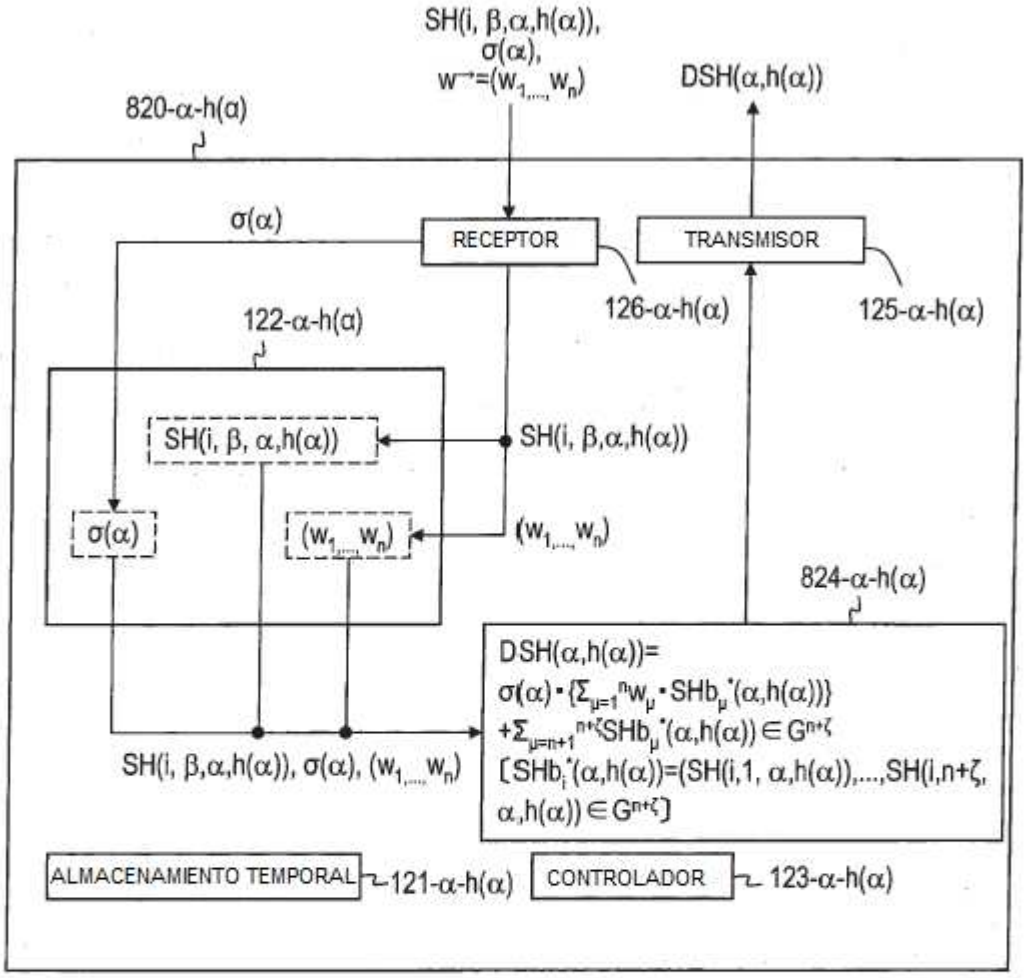

SH(i, β,α,h(α)),
σ(α),
w→=(w1,..., wn)
DSH(α,h(α))
820-α-h(α)
σ(α)
RECEPTOR
TRANSMISOR
126-α-h(α)
125-α-h(α)
122-α-h(α)
SH(i, β, α,h(α))
SH(i, β,α,h(α))
σ(α)
(w1,..., wn)
(w1,..., wn)
824-α-h(α)
DSH(α,h(α))=
σ(α)·{Σμ=1n wμ·SHbμ*(α,h(α))}
+Σμ=n+1n+ζ SHbμ*(α,h(α))∈Gn+ζ
[SHbi*(α,h(α))=(SH(i,1, α,h(α)),...,SH(i,n+ζ,
α,h(α))∈Gn+ζ]
SH(i, β,α,h(α)), σ(α), (w1,..., wn)
ALMACENAMIENTO TEMPORAL
121-α-h(α)
CONTROLADOR
123-α-h(α)

FIG.17

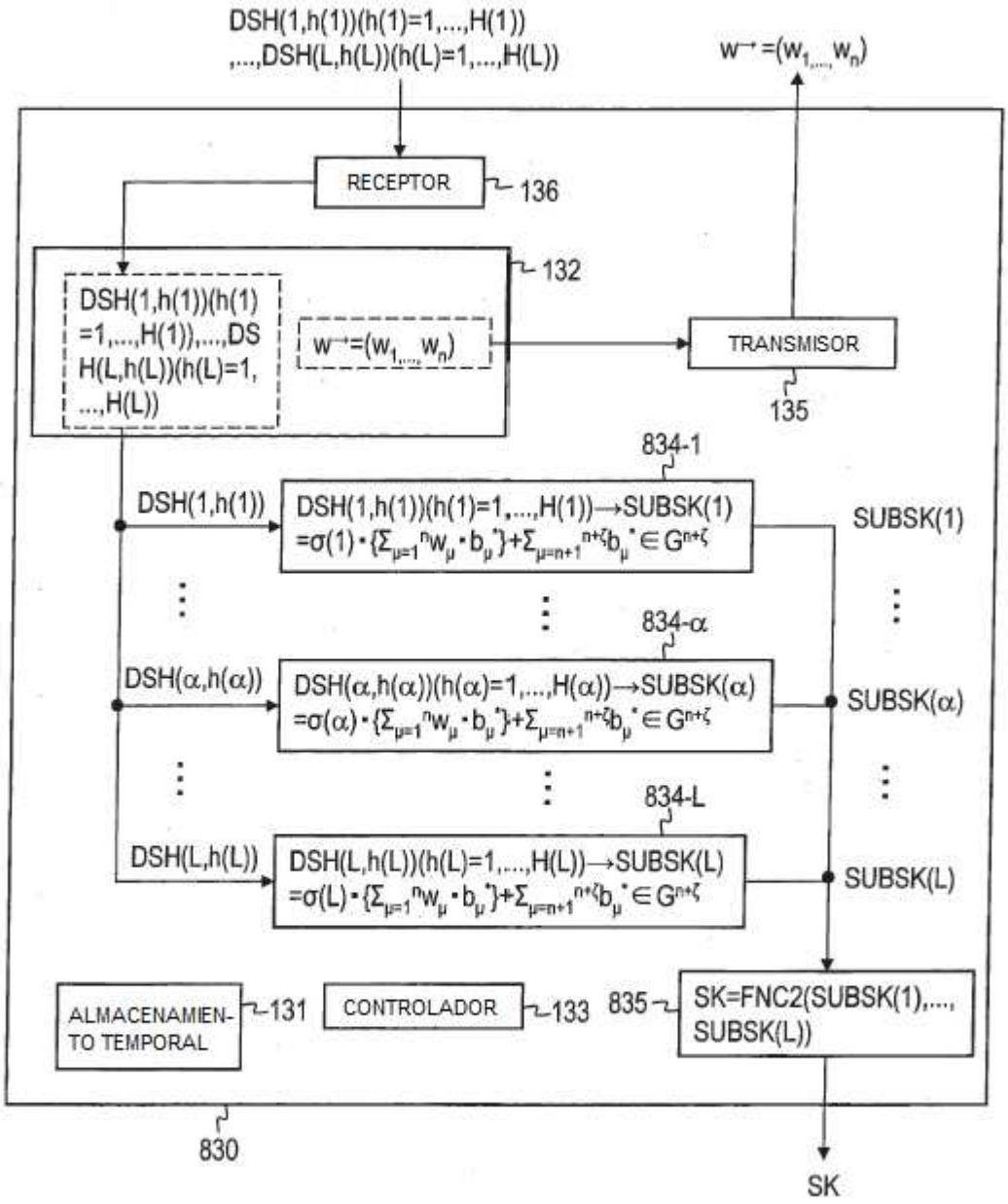

DSH(1,h(1))(h(1)=1,...,H(1))
,...,DSH(L,h(L))(h(L)=1,...,H(L))
w→=(w1,...,wn)
RECEPTOR
136
132
DSH(1,h(1))(h(1)=1,...,H(1)),...,DSH(L,h(L))(h(L)=1,...,H(L))
w→=(w1,...,wn)
TRANSMISOR
135
834-1
DSH(1,h(1))
DSH(1,h(1))(h(1)=1,...,H(1))→SUBSK(1)
=σ(1)·{Σμ=1^n wμ·bμ*}+Σμ=n+1^n+ζ bμ*∈G^n+ζ
SUBSK(1)
834-α
DSH(α,h(α))
DSH(α,h(α))(h(α)=1,...,H(α))→SUBSK(α)
=σ(α)·{Σμ=1^n wμ·bμ*}+Σμ=n+1^n+ζ bμ*∈G^n+ζ
SUBSK(α)
834-L
DSH(L,h(L))
DSH(L,h(L))(h(L)=1,...,H(L))→SUBSK(L)
=σ(L)·{Σμ=1^n wμ·bμ*}+Σμ=n+1^n+ζ bμ*∈G^n+ζ
SUBSK(L)
ALMACENAMIENTO TEMPORAL
131
CONTROLADOR
133
835
SK=FNC2(SUBSK(1),...,SUBSK(L))
830
SK

FIG.18

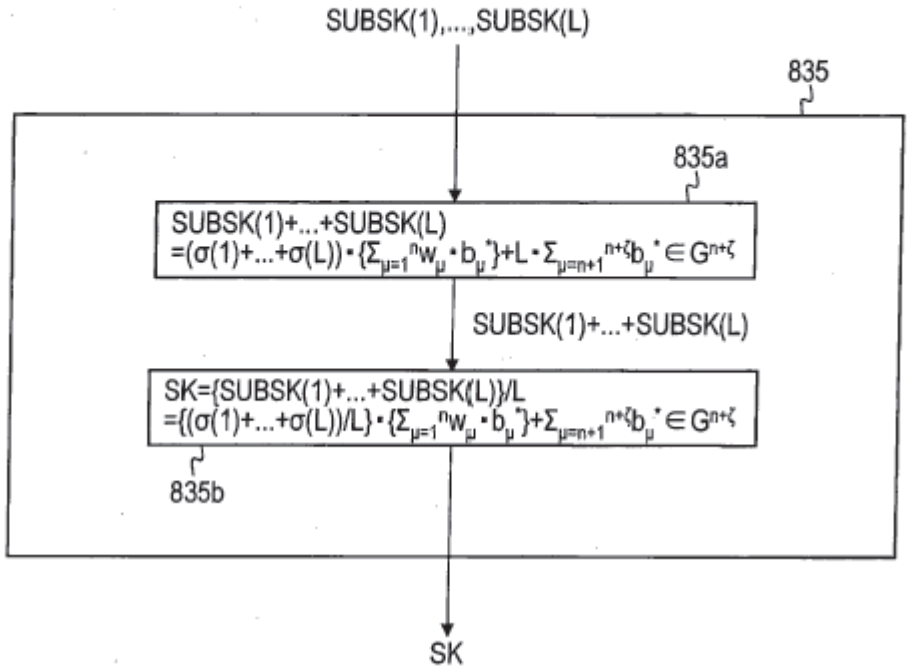

SUBSK(1),...,SUBSK(L)
835
835a
SUBSK(1)+...+SUBSK(L)
=(σ(1)+...+σ(L))・{Σμ=1nwμ・bμ*}+L・Σμ=n+1n+ζbμ*∈Gn+ζ
SUBSK(1)+...+SUBSK(L)
SK={SUBSK(1)+...+SUBSK(L)}/L
={(σ(1)+...+σ(L))/L}・{Σμ=1nwμ・bμ*}+Σμ=n+1n+ζbμ*∈Gn+ζ
835b
SK

FIG.19

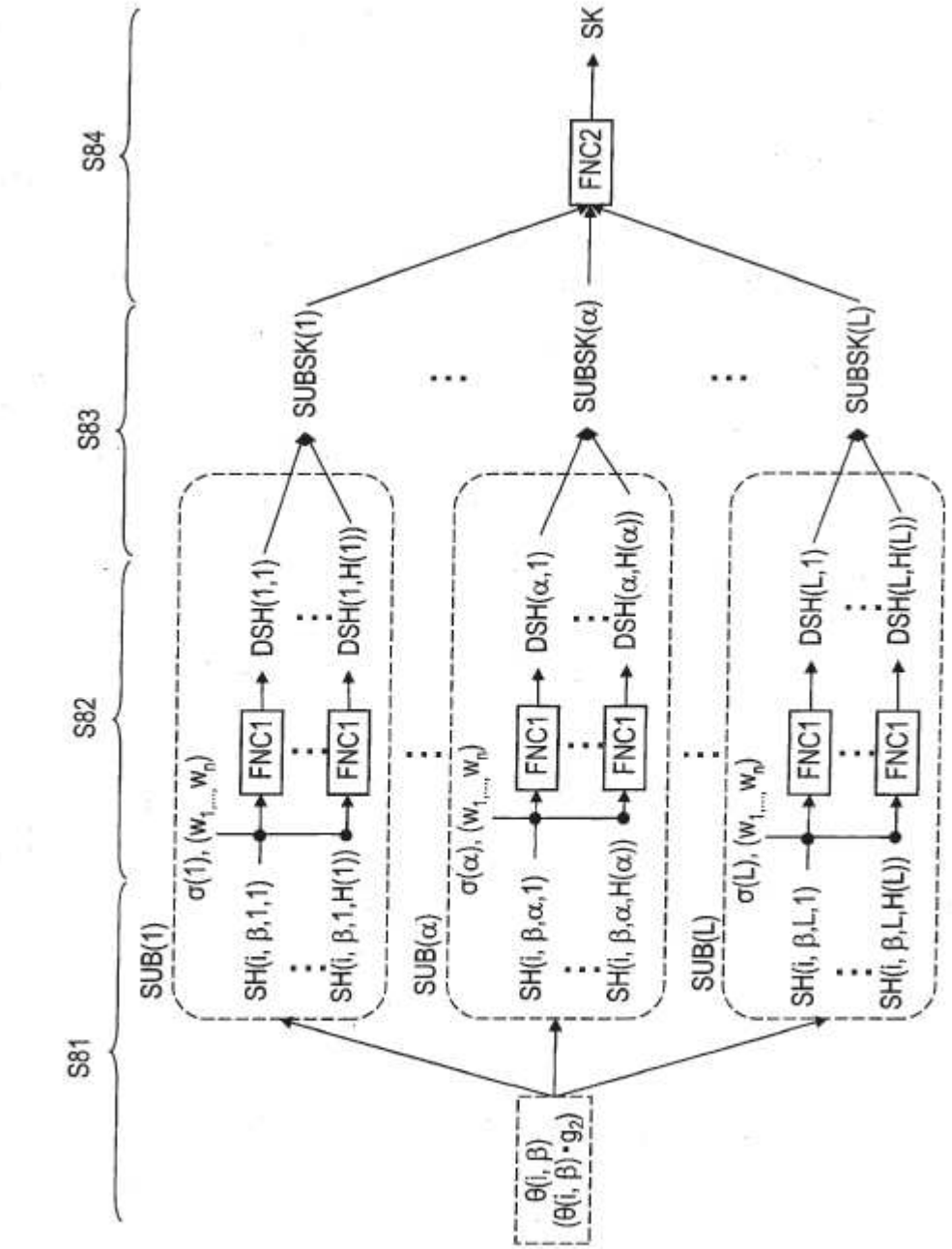

S81
S82
S83
S84
SUB(1)
SUB(α)
SUB(L)
σ(1), (w1,..., wn)
σ(α), (w1,..., wn)
σ(L), (w1,..., wn)
SH(i, β,1,1)
SH(i, β,1,H(1))
SH(i, β,α,1)
SH(i, β,α,H(α))
SH(i, β,L,1)
SH(i, β,L,H(L))
FNC1
DSH(1,1)
DSH(1,H(1))
DSH(α,1)
DSH(α,H(α))
DSH(L,1)
DSH(L,H(L))
SUBSK(1)
SUBSK(α)
SUBSK(L)
FNC2
SK
θ(i, β)
(θ(i, β)·g2)

FIG.20

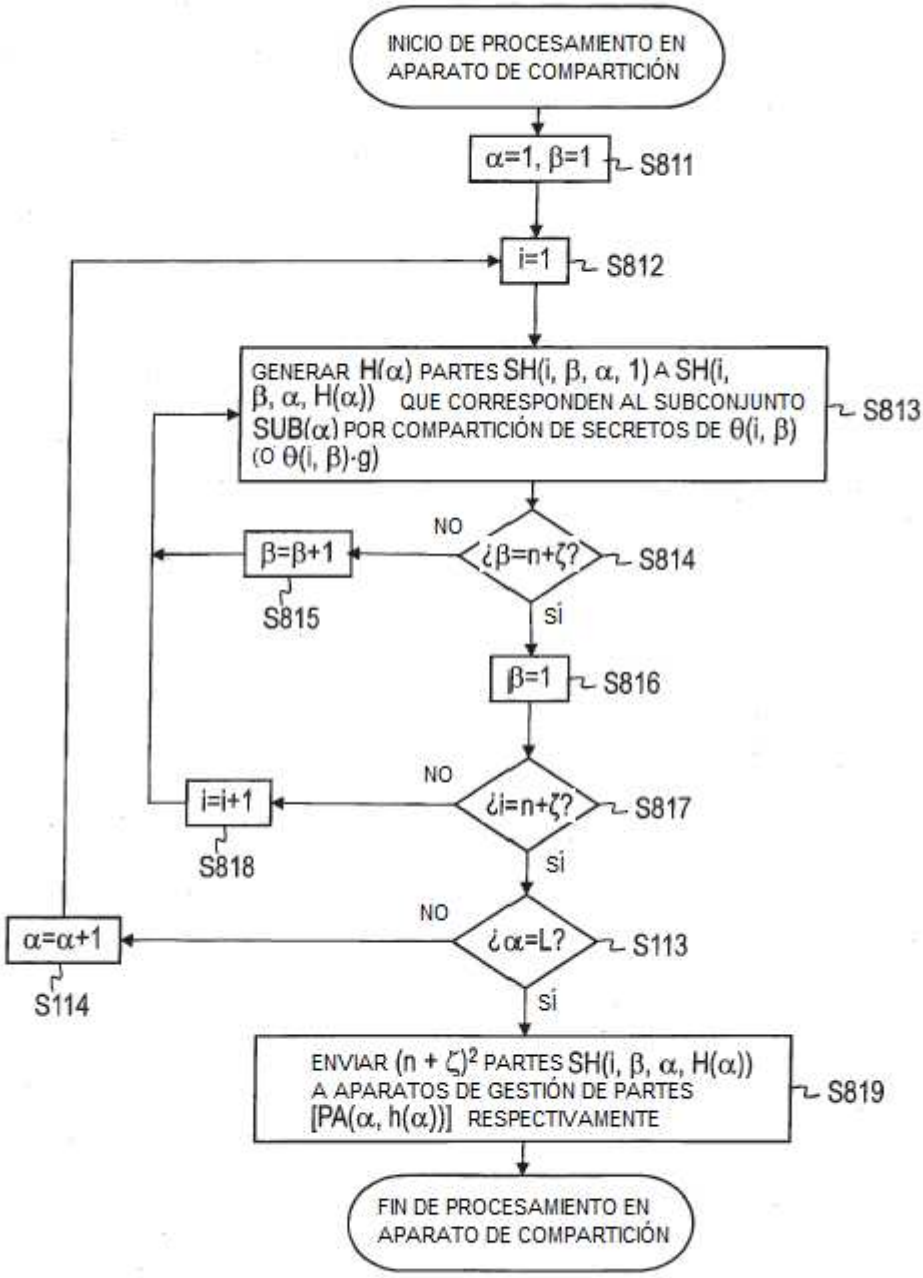

INICIO DE PROCESAMIENTO EN APARATO DE COMPARTICIÓN
α=1, β=1
S811
i=1
S812
GENERAR H(α) PARTES SH(i, β, α, 1) A SH(i, β, α, H(α)) QUE CORRESPONDEN AL SUBCONJUNTO SUB(α) POR COMPARTICIÓN DE SECRETOS DE θ(i, β) (O θ(i, β)·g)
S813
NO
¿β=n+ζ?
S814
β=β+1
S815
SÍ
β=1
S816
NO
¿i=n+ζ?
S817
i=i+1
S818
SÍ
NO
¿α=L?
S113
α=α+1
S114
SÍ
ENVIAR (n + ζ)² PARTES SH(i, β, α, H(α)) A APARATOS DE GESTIÓN DE PARTES [PA(α, h(α))] RESPECTIVAMENTE
S819
FIN DE PROCESAMIENTO EN APARATO DE COMPARTICIÓN

FIG.21

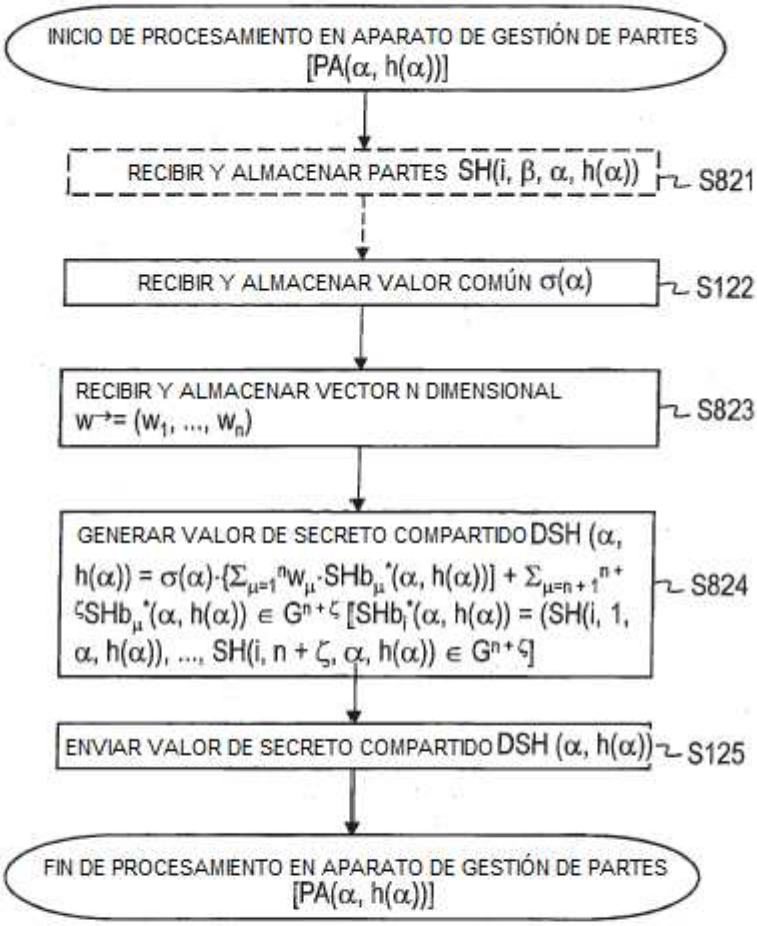
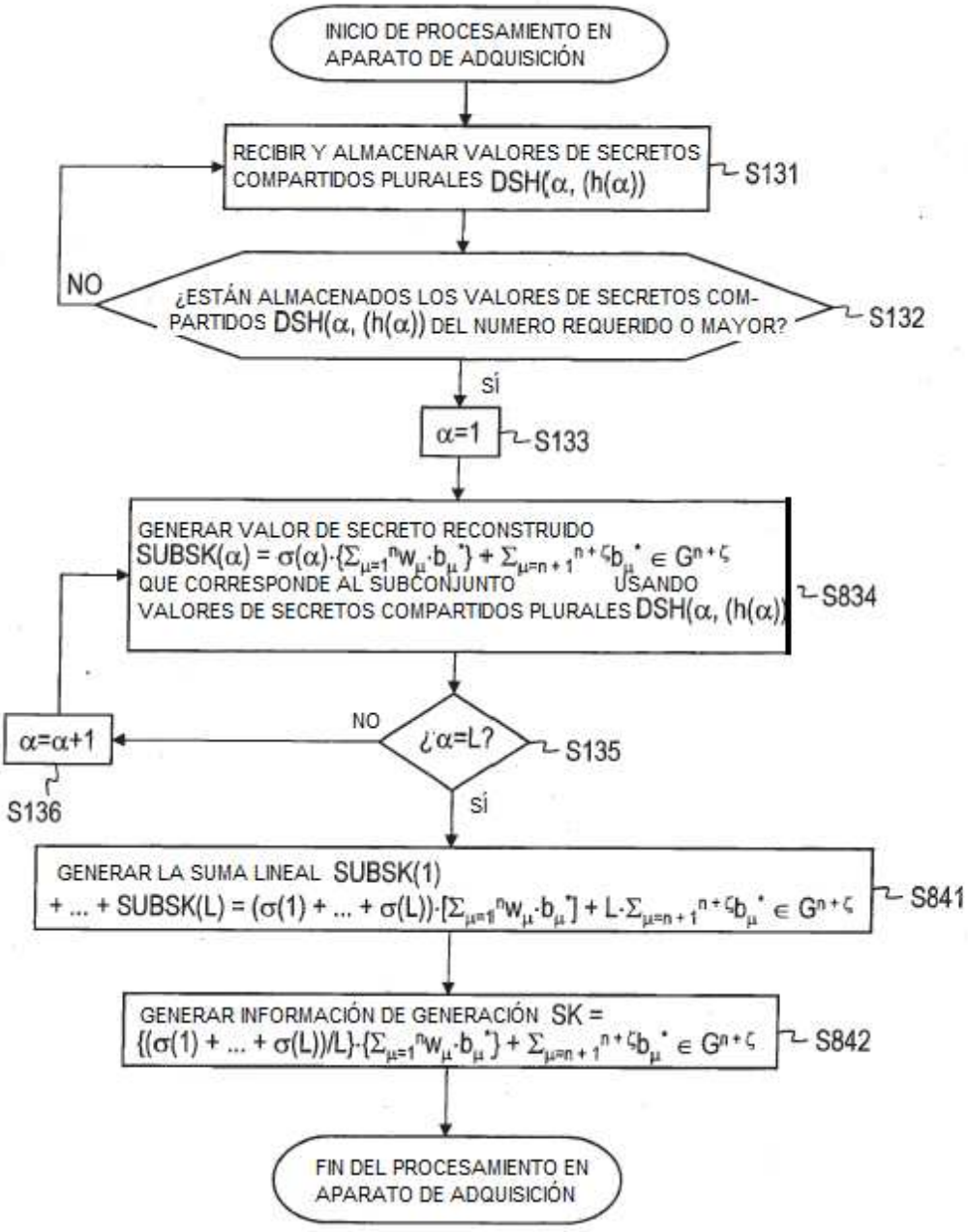

INICIO DE PROCESAMIENTO EN APARATO DE GESTIÓN DE PARTES
[PA(α, h(α))]
RECIBIR Y ALMACENAR PARTES SH(i, β, α, h(α))
S821
RECIBIR Y ALMACENAR VALOR COMÚN σ(α)
S122
RECIBIR Y ALMACENAR VECTOR N DIMENSIONAL
w→= (w1, ..., wn)
S823
GENERAR VALOR DE SECRETO COMPARTIDO DSH (α, h(α)) = σ(α)·{Σμ=1n wμ·SHbμ*(α, h(α))] + Σμ=n+1n+ζ SHbμ*(α, h(α)) ∈ Gn+ζ [SHbi*(α, h(α)) = (SH(i, 1, α, h(α)), ..., SH(i, n + ζ, α, h(α)) ∈ Gn+ζ]
S824
ENVIAR VALOR DE SECRETO COMPARTIDO DSH (α, h(α))
S125
FIN DE PROCESAMIENTO EN APARATO DE GESTIÓN DE PARTES
[PA(α, h(α))]

FIG.22


INICIO DE PROCESAMIENTO EN APARATO DE ADQUISICIÓN
RECIBIR Y ALMACENAR VALORES DE SECRETOS COMPARTIDOS PLURALES DSH(α, (h(α))
S131
NO
¿ESTÁN ALMACENADOS LOS VALORES DE SECRETOS COMPARTIDOS DSH(α, (h(α)) DEL NUMERO REQUERIDO O MAYOR?
S132
SÍ
α=1
S133
GENERAR VALOR DE SECRETO RECONSTRUIDO SUBSK(α) = σ(α)·{Σμ=1n wμ·bμ*} + Σμ=n+1n+ζ bμ* ∈ Gn+ζ QUE CORRESPONDE AL SUBCONJUNTO USANDO VALORES DE SECRETOS COMPARTIDOS PLURALES DSH(α, (h(α))
S834
NO
¿α=L?
S135
α=α+1
S136
SÍ
GENERAR LA SUMA LINEAL SUBSK(1) + ... + SUBSK(L) = (σ(1) + ... + σ(L))·[Σμ=1n wμ·bμ*] + L·Σμ=n+1n+ζ bμ* ∈ Gn+ζ
S841
GENERAR INFORMACIÓN DE GENERACIÓN SK = {(σ(1) + ... + σ(L))/L}·{Σμ=1n wμ·bμ*} + Σμ=n+1n+ζ bμ* ∈ Gn+ζ
S842
FIN DEL PROCESAMIENTO EN APARATO DE ADQUISICIÓN