(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 602 052**

(51) Int. CI.:

H04L 9/30 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.11.2010 PCT/JP2010/070280**

(87) Fecha y número de publicación internacional: **26.05.2011 WO11062136**

(96) Fecha de presentación y número de la solicitud europea: **15.11.2010 E 10831530 (0)**

(97) Fecha y número de publicación de la concesión europea: **05.10.2016 EP 2503533**

(54) Título: **Sistema de procesamiento criptográfico, dispositivo de generación de clave, dispositivo de delegación de clave, dispositivo de cifrado, dispositivo de descifrado, método de procesamiento criptográfico y programa de procesamiento criptográfico**

(30) Prioridad:

20.11.2009 JP 2009264454

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.02.2017

(73) Titular/es:

MITSUBISHI ELECTRIC CORPORATION (50.0%)
7-3, Marunouchi 2-chome, Chiyoda-ku
Tokyo 100-8310, JP y
NIPPON TELEGRAPH AND TELEPHONE CORPORATION (50.0%)

(72) Inventor/es:

TAKASHIMA, KATSUYUKI y
OKAMOTO, TATSUAKI

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema de procesamiento criptográfico, dispositivo de generación de clave, dispositivo de delegación de clave, dispositivo de cifrado, dispositivo de descifrado, método de procesamiento criptográfico y programa de procesamiento criptográfico

Campo técnico

Esta invención se refiere a un esquema de mecanismo de encapsulación de clave de predicado jerárquico (HPKEM) y un esquema de cifrado de predicado jerárquico (HPE).

Antecedentes de la técnica

La Literatura no de Patente 18 trata la implementación de esquemas HPKEM y HPE en espacios duales emparejados a través de una operación de emparejamiento.

Lista de referencias

Literatura no de Patente

Literatura no de Patente 1: Bethencourt, J., Sahai, A., Waters, B.: Ciphertex-policy attribute-based encryption. En: 2007 IEEE Symposium on Security and Privacy, páginas 321-334. IEEE Press (2007)

Literatura no de Patente 2: Boneh, D., Boyen, X.: Efficient selective-ID secure identity based encryption without random oracles. En: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, páginas 223-238. Springer Heidelberg (2004)

Literatura no de Patente 3: Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. En: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, páginas 443-459. Springer Heidelberg (2004)

Literatura no de Patente 4: Boneh, D., Boyen, X., Goh, E.: Hierarchical identity based encryption with constant size ciphertext. En: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, páginas 440-456. Springer Heidelberg (2005)

Literatura no de Patente 5: Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. En: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, páginas. 213-229. Springer Heidelberg (2001)

Literatura no de Patente 6: Boneh, D., Hamburg, M.: Generalized identity based and broadcast encryption scheme. En: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, páginas 455-470. Springer Heidelberg (2008)

Literatura no de Patente 7: Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. En: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, páginas 535-554. Springer Heidelberg (2007)

Literatura no de Patente 8: Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). En: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, páginas 290-307. Springer Heidelberg (2006)

Literatura no de Patente 9: Cocks, C.: An identity based encryption scheme based on quadratic residues. En: Honary, B. (ed.) IMA Int. Conf. LNCS, vol. 2260, páginas 360-363. Springer Heidelberg (2001)

Literatura no de Patente 10: Gentry, C.: Practical identity-based encryption without random oracles. En: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, páginas 445-464. Springer Heidelberg (2006)

Literatura no de Patente 11: Gentry, C., Halevi, S.: Hierarchical identity-based encryption with polynomially many levels. En: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, páginas 437-456. Springer Heidelberg (2009)

Literatura no de Patente 12: Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. En: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, páginas 548-566. Springer Heidelberg (2002)

Literatura no de Patente 13: Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. En: ACM Conference on Computer and Communication Security 2006, páginas 89-98, ACM (2006)

Literatura no de Patente 14: Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. En: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, páginas 415-432. Springer Heidelberg (2008)

Literatura no de Patente 15: Horwitz, J., Lynn, B.: Towards hierarchical identity-based encryption. En: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, páginas 466-481. Springer Heidelberg (2002)

Literatura no de Patente 16: Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynominal equations and inner products. En: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, páginas 146-162. Springer Heidelberg (2008)

Literatura no de Patente 17: Okamoto, T., Takashima, K.: Homomorphic encryption and signatures from vector decomposition. En: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, páginas 57-74. Springer Heidelberg (2008)

Literatura no de Patente 18: Okamoto, T., Takashima, K.: A geometric approach on pairing and hierarchical predicate encryption. En: Poster session, EUROCRYPT 2009. (2009)

Literatura no de Patente 19: Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. En: ACM Conference on Computer and Communication Security 2007, páginas 195-203, ACM, (2007)

Literatura no de Patente 20: Pirretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure attribute-based systems. En: ACM Conference on Computer and Communication Security 2006, páginas 99-112, ACM, (2006)

Literatura no de Patente 21: Sahai, A., Waters, B.: Fuzzy identity-based encryption. En: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, páginas 457-473. Springer Heidelberg (2005)

Literatura no de Patente 22: Shi, E., Waters, B.: Delegating capability in predicate encryption systems. En: Aceto, L., Damgard, I., Goldberg, L.A., Halldorsson, M.M., Ingolfsdottir, A., Walukiewicz, I. (eds.) ICALP (2) 2008. LNCS, vol. 5126, páginas 560-578. Springer Heidelberg (2008)

Literatura no de Patente 23: Takashima, K.: Efficiently computable distortion maps for supersingular curves. En: van der Poorten, A.J., Stein, A. (eds.) ANTS VIII, LNCS, vol. 5011, páginas 88-101. Springer Heidelberg (2008)

Literatura no de Patente 24: Waters, B: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. ePrint, IACR, http://eprint.iacr.org/2008/290

Descripción de la invención

Problema técnico

En los esquemas HPKEM y HPE propuestos en la Literatura no de Patente 18, se da una prueba de seguridad en un modelo idealizado (genérico). No obstante, en los esquemas HPKEM y HPE propuestos en la Literatura no de Patente 18, no se da una prueba de seguridad en un modelo estándar.

Es un objeto de esta invención proporcionar un esquema de cifrado de predicado (PE) y un esquema de mecanismo de encapsulación de clave de predicado (PKEM) con seguridad mejorada. En particular, es un objetivo de esta invención proporcionar un esquema PE y un esquema PKEM con capacidad de delegación.

Solución al problema

Un sistema de procesamiento criptográfico según esta invención, por ejemplo, realiza un proceso de cifrado de predicado usando espacios de vectores duales de un espacio V y un espacio V* emparejado a través de una operación de emparejamiento mostrada en la Fórmula 1 y el sistema de procesamiento criptográfico comprende:

un dispositivo de cifrado que, usando un dispositivo de procesamiento, genera como un vector de cifrado c_1 un vector de una base B^, la base B^ que tiene, de entre los vectores de base b_i (i = 1, …, n, …, N) (N que es un número entero de 3 o mayor y n que es un número entero de 1 a N-2) que constituyen una base B predeterminada del espacio V, los vectores de base b_i (i = 1, …, n) y un vector de base d_{n+1} que es una suma de dos o más vectores de base b_i (i = n+1, …, m) de entre los vectores de base b_i (i = n+1, …, N), el vector de cifrado c_1 que es el vector en el cual la información de atributo se incrusta como coeficientes de uno o más vectores de base de entre los vectores de base b_i (i = 1, …, n) y la información predeterminada se incrusta como un coeficiente del vector de base d_{n+1} ; y

un dispositivo de descifrado que, usando el dispositivo de procesamiento, realiza la operación de emparejamiento e (c_1, $k^*_{L,dec}$) mostrada en la Fórmula 1 sobre el vector de cifrado c_1 generado por el dispositivo de cifrado y un vector de clave $k^*_{L,dec}$ para descifrar el vector de cifrado c_1 y para extraer un valor que concierne a la información predeterminada, el vector de clave $k^*_{L,dec}$ que es un vector de una base B* del espacio V* y construido de manera que la información predicado se incrusta como coeficientes de uno o más vectores de base de los vectores de base b^*_i (i = 1, …, n) de entre los vectores de base b^*_i (i = 1, …, n, …, N) que constituyen la base B* y coeficientes de los vectores de base b^*_i (i = n+1, …, m) de la base B* se incrustan de manera que una suma de los coeficientes de los vectores de base b^*_i (i = n+1, …, m) es 1.

[Formula 1]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

donde

$$p := \sum_{i=1}^{N} \chi_i b_i ,$$

$$q := \sum_{i=1}^{N} \eta_i b_i^* ,$$

χ_i, η_i: valores predeterminados.

Efectos ventajosos de la invención

Un sistema criptográfico según esta invención puede implementar un esquema de cifrado de predicado (PE) y un esquema de mecanismo de encapsulación de clave de predicado (PKEM) con seguridad mejorada.

Breve descripción de los dibujos

La Fig. 1 es un diagrama para explicar una noción de “delegación (delegación jerárquica)”;

La Fig. 2 es un diagrama para explicar salto de delegación sobre un nivel;

La Fig. 3 es un diagrama que muestra estructuras jerárquicas de información de atributo e información de predicado;

La Fig. 4 es un diagrama que muestra un ejemplo de un esquema de cifrado basado en identidad jerárquica (HIBE) que es un ejemplo de aplicación de un esquema de cifrado de predicado jerárquico (HPE) para predicados de producto interior;

La Fig. 5 es un diagrama para explicar una base y un vector de base;

La Fig. 6 es un diagrama para explicar un ejemplo de un método para implementar una estructura jerárquica en un espacio de vector;

La Fig. 7 es un diagrama de configuración de un sistema de procesamiento criptográfico 10;

La Fig. 8 es un diagrama de flujo que muestra operaciones de un dispositivo de generación de clave 100, un dispositivo de cifrado de nivel de orden L 200 y un dispositivo de descifrado de nivel de orden L 300 del sistema de procesamiento criptográfico 10;

La Fig. 9 es un diagrama de flujo que muestra operaciones de un dispositivo de delegación de clave de nivel de orden L 400, un dispositivo de cifrado de nivel de orden (L+1) 200 y un dispositivo de descifrado de nivel de orden (L+1) 300 del sistema de procesamiento criptográfico 10;

La Fig. 10 es un diagrama para explicar un método de cambio de base;

La Fig. 11 es un diagrama de bloques funcional que muestra funciones del sistema de procesamiento criptográfico 10 que implementa un esquema HPE según una segunda realización;

La Fig. 12 es un diagrama de flujo que muestra operaciones del dispositivo de generación de clave 100 según la segunda realización;

La Fig. 13 es un diagrama de flujo que muestra operaciones del dispositivo de cifrado 200 según la segunda realización;

La Fig. 14 es un diagrama de flujo que muestra operaciones del dispositivo de descifrado 300 según la segunda realización;

La Fig. 15 es un diagrama de flujo que muestra operaciones del dispositivo de delegación de clave 400 según la segunda realización;

La Fig. 16 es un diagrama conceptual que muestra una estructura sobre una base de espacios de vectores de emparejamiento duales según la segunda realización;

La Fig. 17 es un diagrama de bloques funcional que muestra funciones del sistema de procesamiento criptográfico 10 que implementa un esquema de mecanismo de encapsulación de clave de predicado jerárquico (HPKEM) según la segunda realización;

La Fig. 18 es un diagrama de flujo que muestra operaciones del dispositivo de cifrado 200 según la segunda realización;

La Fig. 19 es un diagrama de flujo que muestra operaciones del dispositivo de descifrado 300 según la segunda realización;

La Fig. 20 es un diagrama de bloques funcional que muestra funciones del sistema de procesamiento criptográfico 10 que implementa un esquema de cifrado de predicado (PE) con capacidad de delegación según una tercera realización; y

La Fig. 21 es un diagrama que muestra un ejemplo de una configuración hardware del dispositivo de generación de clave 100, el dispositivo de cifrado 200, el dispositivo de descifrado 300 y el dispositivo de delegación de clave 400.

Descripción de las realizaciones preferidas

Las realizaciones de la invención se describirán ahora con referencia a los dibujos.

En la siguiente descripción, un dispositivo de procesamiento es una CPU 911 o similar que se describe más tarde. Un dispositivo de almacenamiento es una ROM 913, una RAM 914, un disco magnético 920 o similares que se describe más tarde. Un dispositivo de comunicación es una placa de comunicación 915 o similar que se describe más tarde. Un dispositivo de entrada es un teclado 902, la placa de comunicación 915 o similar que se describe más tarde. Un dispositivo de salida es la RAM 914, el disco magnético 920, la placa de comunicación 915, un LCD 901 o similar que se describe más tarde. Es decir, el dispositivo de procesamiento, el dispositivo de almacenamiento, el dispositivo de comunicación, el dispositivo de entrada y el dispositivo de salida son hardware.

Se describirán notaciones que se usan en la siguiente descripción.

Cuando A es una variable o distribución aleatoria, la Fórmula 101 indica que y se selecciona aleatoriamente a partir de A según la distribución de A. Es decir, y es un número aleatorio en la Fórmula 101.

[Fórmula 101]

$$y \xleftarrow{R} A$$

Cuando A es un conjunto, la Fórmula 102 indica que y se selecciona uniformemente a partir de A. Es decir, y es un número aleatorio uniforme en la Fórmula 102.

[Fórmula 102]

$$y \xleftarrow{U} A$$

La Fórmula 103 indica que y es fijo, definido o sustituido por z.

[Fórmula 103]

$$y := z$$

Cuando a es un valor fijo, la Fórmula 104 indica que una máquina (algoritmo) A saca a en una entrada x.

[Fórmula 104]

$$A(x) \rightarrow a$$

Por ejemplo,

$$A(x) \rightarrow 1$$

Un símbolo de vector indica una representación de vector sobre un campo finito F_q, es decir, la Fórmula 105.

[Fórmula 105]

$\vec{x}$ indica

$$(x_1, \ldots, x_n) \in \mathbb{F}_q.$$

La Fórmula 106 indica el producto interior de dos vectores $\vec{x}$ y $\vec{v}$ mostrados en la Fórmula 107 y la Fórmula 108 muestra este producto interior.

[Fórmula 106]

$$\vec{x} \cdot \vec{v}$$

[Fórmula 107]

$$\vec{x} = (x_1, \ldots, x_n)$$
$$\vec{v} = (v_1, \ldots, v_n)$$

[Fórmula 108]

$$\sum_{i=1}^{n} x_i v_i$$

X^T indica la traspuesta de una matriz X.

En la siguiente descripción, un proceso criptográfico incluirá un proceso de cifrado, un proceso de descifrado y un proceso de generación de clave y también incluirá un proceso de encapsulación de clave.

Primera realización

En esta realización, se describirán conceptos básicos para implementar un “esquema de cifrado de predicado (PE) con delegación” y un “esquema de mecanismo de encapsulación de clave de predicado (PKEM) con delegación” que se trata en realizaciones posteriores, junto con constricciones básicas del esquema PE (PKEM) con delegación.

En primer lugar, se describirá una noción de un “esquema PE (PKEM) con delegación para predicados de producto interior”, que es un tipo de esquema PE (PKEM) con delegación. Los esquemas PE (PKEM) con delegación que se tratan en las realizaciones posteriores son esquemas PE (PKEM) con delegación para predicados de producto interior. Para describir la noción del esquema PE con delegación para predicados de producto interior, se describirá primero una noción de “delegación”, junto con una noción de “delegación jerárquica”. Entonces, se describirá el “esquema PE para predicados de producto interior”. Entonces, se describirá un “esquema PE jerárquico (HPE) para predicados de producto interior (esquema PKEM jerárquico (HPKEM) para predicados de producto interior), que es un tipo de esquema PE para predicados de producto interior con la noción de delegación jerárquica. Además, para reforzar la comprensión del esquema HPE para predicados de producto interior, se describirá un ejemplo de aplicación del esquema HPE para predicados de producto interior.

En segundo lugar, se describirá el esquema HPE para predicados de producto interior en espacios de vectores. En ésta y posteriores realizaciones, los esquemas HPE y HPKEM para predicados de producto interior se implementan en espacios de vectores. Una “base” y un “vector de base” se describirán primero. Entonces, se describirá el “esquema PE para predicados de producto interior en espacios de vectores”. Entonces, se describirá un “método para implementar una estructura jerárquica en un espacio de vector”. Además, para reforzar la comprensión, se describirá un ejemplo de implementación de la estructura jerárquica.

En tercer lugar, se describirán construcciones básicas de los “esquemas HPE y HPKEM” según ésta y posteriores realizaciones. También se describirá un “sistema de procesamiento criptográfico 10” que implementa los esquemas HPE y HPKEM.

En cuarto lugar, se describirán conceptos para implementar los esquemas HPKEM y HPE. Se describirán “grupos de emparejamiento bilineal”, “espacios de vectores V y V*”, “bases duales canónicas A y A*”, “operación de emparejamiento”, “cambio de base” y “mapas de distorsión”.

En quinto lugar, se describirán “espacios de vectores de emparejamiento duales (DPVS)” que tienen estructuras matemáticas ricas para implementar los esquemas HPKEM y HPE.

En sexto lugar, en base a las descripciones anteriores, se describirá brevemente un método para implementar los esquemas HPE y HPKEM que se tratan en detalle en las realizaciones posteriores.

<1. Esquema HPE para predicados de producto interior>

<1.1 Noción de delegación (delegación jerárquica)>

La Fig. 1 es un diagrama para explicar la noción de "delegación (delegación jerárquica)".

Delegación significa que un usuario que tiene una clave de nivel más alto genera una clave de nivel más bajo que tiene capacidades más limitadas que la clave (de nivel más alto) del usuario.

En la Fig. 1, una raíz (dispositivo de generación de clave) genera claves secretas para usuarios de primer nivel (nivel 1) usando una clave secreta maestra. Es decir, la raíz genera las claves 1, 2 y 3 para usuarios de primer nivel 1, 2, y 3 respectivamente. Entonces, usando la clave 1, por ejemplo, el usuario 1 puede generar las claves 11, 12 y 13 para los usuarios 11, 12 y 13, respectivamente, quienes son usuarios de nivel más bajo (segundo) del usuario 1. Las claves 11, 12 y 13 poseídas por los usuarios 11, 12 y 13 tienen capacidades más limitadas que la clave 1 poseída por el usuario 1. Las capacidades limitadas significan que los textos cifrados que se pueden descifrar por esa clave secreta son limitados. Es decir, una clave secreta de nivel más bajo solamente puede descifrar algunos de los textos cifrados que se pueden descifrar por una clave secreta de nivel más alto. Esto significa que las claves 11, 12 y 13 poseídas por los usuarios 11, 12 y 13 solamente pueden descifrar algunos de los textos cifrados que se pueden descifrar por la clave 1 poseída por el usuario 1. Normalmente, las claves 11, 12 y 13 pueden descifrar respectivamente diferentes textos cifrados. Por otra parte, un texto cifrado que se puede descifrar por las claves 11, 12 o 13 se puede descifrar por la clave 1.

Como se muestra en la Fig. 1, cada clave secreta se proporciona para un nivel específico. Esto se describe como “jerárquico”. Es decir, como se muestra en la Fig. 1, una generación jerárquica de claves de nivel más bajo se llama “delegación jerárquica”.

En la Fig. 1, se ha descrito que la raíz genera las claves secretas para los usuarios de primer nivel, los usuarios de primer nivel generan las claves secretas para los usuarios de segundo nivel y los usuarios de segundo nivel generan las claves secretas para los usuarios de tercer nivel. No obstante, como se muestra en la Fig. 2, la raíz puede generar no solamente las claves secretas para los usuarios de primer nivel, sino también las claves secretas para los usuarios de segundo nivel o más bajo. Del mismo modo, los usuarios de primer nivel pueden generar no solamente las claves secretas para los usuarios de segundo nivel, sino también las claves secretas para los usuarios de tercer nivel o más bajo. Es decir, la raíz o cada usuario puede generar las claves secretas para niveles más bajos que el nivel de su propia clave secreta.

<1-2. Esquema PE para predicados de producto interior>

A continuación, se describirá el “esquema PE para predicados de producto interior”.

El esquema PE es un esquema criptográfico en el que un texto cifrado se puede descifrar si un resultado de la introducción de información de atributo x a información de predicado f_v es 1 (verdadero) ($f_v(x) = 1$). Normalmente, la información de atributo x está incrustada en un texto cifrado y la información de predicado f_v está incrustada en una clave secreta. Es decir, en el esquema PE, un texto cifrado c cifrado en base a la información de atributo x se descifra por una clave secreta SK_f generada en base a la información de predicado f_v. El esquema PE se puede describir como un esquema criptográfico en el que, por ejemplo, la información de predicado f_v es una expresión condicional y la información de atributo x es información que se introduce a la expresión condicional y un texto cifrado se puede descifrar si la información de entrada (información de atributo x) satisface la expresión condicional (información de predicado f_v) ($f_v(x) = 1$).

El esquema PE se trata en detalle en la Literatura no de Patente 16.

El esquema PE para predicados de producto interior es un tipo de esquema PE en el cual $f_v(x) = 1$ si el producto interior de la información de atributo x y la información de predicado f_v es un valor predeterminado. Es decir, un texto cifrado c cifrado por la información de atributo x se puede descifrar por una clave secreta SK_f generada en base a la información de predicado f_v si y solamente si el producto interior de la información de atributo x y la información de predicado f_v es un valor predeterminado. En la siguiente descripción, se supone que $f_v(x) = 1$ si el producto interior de la información de atributo x y la información de predicado f_v es 0.

<1-3. Esquema HPE para predicados de producto interior>

El esquema HPE (HPKEM) para predicados de producto interior es un tipo de “esquema PE para predicados de producto interior” con la noción descrita anteriormente de “delegación jerárquica”.

En el esquema HPE para predicados de producto interior, la información de atributo y la información de predicado tienen estructuras jerárquicas, a fin de añadir un sistema de delegación jerárquica al esquema PE para predicados de producto interior.

La Fig. 3 es un diagrama que muestra estructuras jerárquicas de información de atributo e información de predicado.

En la Fig. 3, información de atributo e información de predicado con los mismos números de referencia corresponden una a la otra (es decir, su producto interior es 0). Es decir, el producto interior de un atributo 1 y un predicado 1 es 0, el producto interior de un atributo 11 y un predicado 11 es 0, el producto interior de un atributo 12 y un predicado 12 es 0 y el producto interior de un atributo 13 y un predicado 13 es 0. Esto significa que un texto cifrado c1 cifrado por el atributo 1 se puede descifrar por una clave secreta k1 generada en base al predicado 1. Un texto cifrado c11 cifrado por el atributo 11 se puede descifrar por una clave secreta k11 generada en base al predicado 11. Lo mismo se puede decir del atributo 12 y el predicado 12 también como del atributo 13 y el predicado 13.

Como se describió anteriormente, el esquema HPE para predicados de producto interior tiene el sistema de delegación jerárquica. De esta manera, la clave secreta k11 se puede generar en base al predicado 11 y la clave secreta k1 generar en base al predicado 1. Es decir, un usuario que tiene la clave secreta de nivel más alto k1 puede genera su clave secreta de nivel más bajo k11 a partir de la clave secreta k1 y el predicado de nivel más bajo 11. Del mismo modo, la clave secreta k12 se puede generar a partir de la clave secreta k1 y el predicado 12 y la clave secreta k13 se puede generar a partir de la clave secreta k1 y el predicado 13.

Un texto cifrado cifrado por una clave (clave pública) que corresponde a una clave secreta de nivel más bajo se puede descifrar por una clave secreta de nivel más alto. Por otra parte, un texto cifrado cifrado por una clave (clave pública) que corresponde a una clave secreta de nivel más alto no se puede descifrar por una clave secreta de nivel más bajo. Es decir, los textos cifrados c11, c12 y c13 cifrados por los atributos 11, 12 y 13, respectivamente, se pueden descifrar por la clave secreta k1 generada en base al predicado 1. Por otra parte, el texto cifrado c1 cifrado por el atributo 1 no se puede descifrar por las claves secretas k11, k12 y k13 generadas en base a los predicados 11, 12 y 13, respectivamente. Es decir, el producto interior del atributo 11, 12 o 13 y el predicado 1 es 0. Por otra parte, el producto interior del atributo 1 y el predicado 11, 12 o 13 no es 0.

<1-4. Ejemplo de aplicación del esquema HPE para predicados de producto interior>

La Fig. 4 es un diagrama que muestra un ejemplo de un esquema de cifrado basado en identidad jerárquica (HIBE), que es un ejemplo de aplicación del esquema HPE para predicados de producto interior que se describen más tarde. El esquema HIBE es un proceso criptográfico en el que la noción de jerarquía se aplica a un esquema de cifrado basado en identidad (IBE). El esquema IBE es un tipo de esquema PE, esto es, un esquema PE concordante, que permite a un texto cifrado ser descifrado si un ID incluido en el texto cifrado concuerda con un ID incluido en una clave secreta.

En el ejemplo mostrado en la Fig. 4, en base a una clave secreta maestra sk y un ID “A” de Empresa A, una raíz (dispositivo de generación de clave) genera una clave secreta (clave A) que corresponde al ID “A”. Por ejemplo, en base a la clave A y el ID de cada división, un administrador de seguridad de la Empresa A genera una clave secreta que corresponde a ese ID. Por ejemplo, el administrador de seguridad genera una clave secreta (clave 1) que corresponde a un ID “A-1” de una división de ventas. Entonces, en base a la clave secreta de cada división y el ID de cada unidad que pertenece a esa división, por ejemplo, un administrador de cada división genera una clave secreta que corresponde a ese ID. Por ejemplo, un administrador de la división de ventas genera una clave secreta (clave 11) que corresponde a un ID “A-11” de una unidad de ventas 1.

En este caso, un texto cifrado cifrado por el ID “A-11” de la unidad de ventas 1 se puede descifrar por la clave 11 que es la clave secreta que corresponde al ID “A-11” de la unidad de ventas 1. No obstante, un texto cifrado cifrado por el ID de una unidad de ventas 2 o una unidad de ventas 3 no se puede descifrar por la clave 11. También, un texto cifrado cifrado por el ID de la división de ventas no se puede descifrar por la clave 11.

Un texto cifrado cifrado por el ID “A-1” de la división de ventas no se puede descifrar por la clave 1 que es la clave secreta que corresponde al ID “A-1” de la división de ventas. También, un texto cifrado cifrado por el ID de una unidad que pertenece a la división de ventas se puede descifrar por la clave 1. Es decir, un texto cifrado cifrado por el ID de la unidad de ventas 1, 2 o 3 se puede descifrar por la clave 1. No obstante, un texto cifrado cifrado por el ID de una división de fabricación (ID: A-2) o una división de personal (ID: A-3) no se puede descifrar por la clave 1. También, un texto cifrado cifrado por el ID de una Empresa A no se puede descifrar por la clave 1.

Un texto cifrado cifrado por el ID “A” de la Empresa A se puede descifrar por la clave A que es la clave secreta que corresponde al ID “A” de la Empresa A. También, un texto cifrado cifrado por el ID de cada división que pertenece a la Empresa A o el ID de una unidad que pertenece a cada división se puede descifrar por la clave A.

El esquema HPE para predicados de producto interior se puede adaptar a diversas aplicaciones distintas del esquema IBE. En particular, los procesos criptográficos que se describen más tarde no están limitados a una clase de pruebas de igualdad, de modo que se pueden aplicar a un vasto número de aplicaciones. Por ejemplo, los procesos criptográficos también se pueden adaptar para otros tipos de esquema PE para predicados de producto interior tales como un esquema de cifrado investigable, haciendo posible implementar aplicaciones que no son posibles con un esquema PE de la técnica anterior con el sistema de delegación, tal como limitar un intervalo investigable en cada nivel usando una expresión condicional tal como AND u OR.

Es decir, los esquemas HPKEM y HPE que se describen en las realizaciones posteriores se pueden aplicar a una amplia variedad de aplicaciones tales como los esquemas IBE y de cifrado investigable.

<2. Esquema HPE para predicados de producto interior en espacios de vectores>

Los esquemas HPKEM y HPE se implementan en espacios de vectores dimensionales altos llamados espacios de vectores de emparejamiento duales (DPVS) que se describen más tarde. De esta manera, se describirá el esquema HPE para predicados de producto interior en espacios de vectores.

<2-1. Base y vector de base>

En primer lugar, se explicarán brevemente una “base” y un “vector de base” que se usan para explicar un espacio de vector.

La Fig. 5 es un diagrama para explicar la base y el vector de base.

La Fig. 5 muestra un vector v de un espacio de vector bidimensional. El vector v es $c_1a_1 + c_2a_2$. Además, el vector v es $y_1b_1 + y_2b_2$. Aquí a_1 y a_2 se llaman vectores de base en una base A y se representan como base A: = (a_1, a_2). b_1 y b_2 se llaman vectores de base en una base B y se representan como base B: = (b_1, b_2). c_1, c_2, y_1 e y_2 son los coeficientes de vectores de base respectivos. La Fig. 5 muestra un espacio de vector bidimensional, de modo que hay dos vectores de base en cada base. En un espacio de vector N dimensional, hay un número N de vectores de base en cada base.

<2-2. Esquema PE para predicados de producto interior en espacios de vectores>

Se describirá ahora el esquema PE para predicados de producto interior en espacios de vectores.

Como se describió anteriormente, el esquema PE para predicados de producto interior es un tipo de esquema PE en el que $f_v(x) = 1$ si el producto interior de la información de atributo x y la información de predicado f_v es un valor predeterminado (0 en este caso). Cuando la información de atributo x y la información de predicado f_v son vectores, esto es, un vector de atributo $\vec{x}$ y un vector de predicado $\vec{v}$, su predicado de producto interior se define como se muestra en la Fórmula 109.

[Fórmula 109]

Si $\vec{x} \cdot \vec{v} = \sum_{i=1}^{n} x_i v_i = 0$, entonces $f_{\vec{v}}(\vec{x}) = 1$ y

si $\vec{x} \cdot \vec{v} = \sum_{i=1}^{n} x_i v_i \neq 0$, entonces $f_{\vec{v}}(\vec{x}) = 0$,

donde

$$\vec{x} = (x_1, \ldots, x_n) ,$$
$$\vec{v} = (v_1, \ldots, v_n) .$$

Es decir, es un tipo de esquema PE en el que un resultado de la introducción de la información de atributo x a la información de predicado f_v es 1 (verdadero) si el producto interior del vector de atributo $\vec{x}$ y el vector de predicado $\vec{v}$ (es decir, la suma de productos interiores en forma de elemento) es 0 y un resultado de la introducción de la información de atributo x a la información de predicado f_v es 0 (falsa) si el producto interior del vector de atributo $\vec{x}$ y el vector de predicado $\vec{v}$ no es 0.

<2-3. Método para implementar una estructura jerárquica en un espacio de vector>

Se describirá ahora un método para implementar una estructura jerárquica en un espacio de vector.

La Fig. 6 es un diagrama para explicar un ejemplo del método para implementar una estructura jerárquica en un espacio de vector.

El espacio de vector aquí se supone que es un espacio de vector dimensional alto (N dimensional). Es decir, existe un número N de vectores de base c_i (i = 1, …, N) en una base C predeterminada del espacio de vector.

Un número n de vectores de base (vectores de base c_i (i = 1, …, n)) de entre el número N de vectores de base se usan para representar la estructura jerárquica. Los vectores de base c_i (i = 1, …, n) se dividen en un número d de grupos, esto es, vectores de base c_i (i = 1, …, μ_1), vectores de base c_i (i = μ_1+1, …, μ_2), … y vectores de base c_i (i = μ_{d-1}+1, …, n), donde d indica una profundidad de jerarquía.

Entonces, un número μ_1 de vectores de base c_1 (i = 1, …, μ_1) se asignan para representar información de atributo e información de predicado del primer nivel. Un número (μ_2-μ_1) de vectores de base c_i (i = μ_1+1, …, μ_2) se asignan para representar información de atributo e información de predicado del segundo nivel. Del mismo modo, un número (μ_d-μ_{d-1}) de vectores de base c_i (i = μ_{d-1}+1, …, μ_d(=n)) se asignan para representar información de atributo e información de predicado del nivel de orden d.

Para generar un texto cifrado por información de atributo de nivel de orden L, no solamente se usan información de atributo de nivel de orden L sino también de primer nivel a de orden L para generar un texto cifrado. Del mismo modo, para generar una clave secreta mediante información de predicado de nivel de orden L, no solamente se usa información de predicado de nivel de orden L sino de primer nivel a nivel de orden L para generar la clave secreta.

Es decir, para generar un texto cifrado mediante la información de atributo de nivel de orden L o para generar una clave secreta mediante la información de predicado de nivel de orden L, se usa un número μ_L de vectores de base c_i (i = 1, …, μ_L) asignados al primer nivel al de orden L. Por ejemplo, para generar un texto cifrado mediante información de atributo de tercer nivel, se usa un número μ_3 de vectores de base c_i (i = 1, …, μ_3) asignados al primer a tercer niveles para generar un texto cifrado, de manera que se refleja la información de atributo del primer a tercer nivel. Del mismo modo, para generar una clave secreta mediante información de predicado de tercer nivel, se usa el número μ_3 de vectores de base c_i (i = 1, …, μ_3) asignados al primer a tercer niveles para generar una clave secreta, de manera que se refleja información de predicado del primer al tercer nivel. Es decir, información de atributo o información de predicado que se usa en un nivel más bajo incluye información de atributo o información de predicado que se usa en un nivel más alto. De esta forma, la información de atributo y la información de predicado cada una tiene una estructura jerárquica. Entonces, usando las estructuras jerárquicas de información de atributo e información de predicado, un sistema de delegación se incorpora en el esquema PE para predicados de producto interior.

En la siguiente descripción, se usa un formato de jerarquía $\vec{\mu}$ para indicar una estructura jerárquica de un espacio de vector. El formato de jerarquía $\vec{\mu}$ se muestra en la Fórmula 110.

[Fórmula 110]

$$\vec{\mu} := (n, d; \mu_1, \ldots, \mu_d)$$

donde

$$\mu_0 = 0 < \mu_1 < \mu_2 < \cdots < \mu_d = n.$$

Es decir, el formato de jerarquía $\vec{\mu}$ tiene información n que indica el número de vectores de base (número de dimensiones) asignado para representar la estructura jerárquica, información d que indica la profundidad de jerarquía e información μ_1, …, μ_d que indica vectores de base asignados a cada nivel.

Se describirá ahora el esquema HPE para predicados de producto interior en espacios de vectores.

Permitamos que un espacio de atributo Σ_L (L = 1, …, d) sea un espacio asignado para representar información de atributo de nivel de orden L, donde cada Σ_L es como se muestra en la Fórmula 111.

[Fórmula 111]

$$\sum_L := \mathbb{F}_q{}^{\mu_L - \mu_{L-1}} \setminus \{\vec{0}\}$$

Permitamos que un conjunto de atributos jerárquicos sea Σ mostrado en la Fórmula 112, donde la unión es una unión disjunta.

[Fórmula 112]

$$\Sigma := \bigcup_{L=1}^{d} (\Sigma_1 \times \ldots \times \Sigma_L)$$

Entonces, los predicados jerárquicos mostrados en la Fórmula 114 en los atributos jerárquicos mostrados en la Fórmula 113 se definen como se muestra en la Fórmula 115.

[Fórmula 113]

$$(\vec{x}_1, \ldots, \vec{x}_h) \in \Sigma$$

[Fórmula 114]

$$f(\vec{v}_1, \ldots, \vec{v}_L)$$

donde

$$\vec{v}_i \in \mathbb{F}_q{}^{\mu_i - \mu_{i-1}} \setminus \{\vec{0}\}.$$

[Fórmula 115]

Sí y sólo sí $L \leq h$ y

$\vec{x}_i \cdot \vec{v}_i = 0$ para todo $1 \leq i \leq L$, entonces

$$f_{(\vec{v}_1,\ldots,\vec{v}_L)}(\vec{x}_1,\ldots,\vec{x}_h) = 1 \ .$$

Permitamos que un espacio de predicados jerárquicos sea F mostrado en la Fórmula 116.

[Fórmula 116]

$$\mathcal{F} := \left\{ f_{(\vec{v}_1,\ldots,\vec{v}_L)} \middle| \vec{v}_i \in \mathbb{F}_q{}^{\mu_i - \mu_{i-1}} \setminus \{\vec{0}\} \right\}$$

Permitamos que h en la Fórmula 117 y L en la Fórmula 118 cada uno sea llamado un nivel.

[Fórmula 117]

$$(\vec{x}_1,\ldots,\vec{x}_h)$$

[Fórmula 118]

$$(\vec{v}_1,\ldots,\vec{v}_L)$$

<2-4. Ejemplo de implementación de la estructura jerárquica>

La estructura jerárquica se explicará usando un simple ejemplo, donde se emplea un espacio de 6 dimensiones que tiene tres niveles, cada nivel que consiste en espacio bidimensional. Es decir, $\vec{\mu}$: = (n, d; μ_1, …, μ_d) = (6, 3; 2, 4, 6).

Un usuario que tiene una clave secreta de primer nivel sk_1 generada en base a un vector de predicado de primer nivel $\vec{v}_1$: = (v_1, v_2) puede generar una clave secreta de segundo nivel sk_2 en base a la clave secreta de primer nivel sk_1 y un vector de predicado de segundo nivel $\vec{v}_2$: = (v_3, v_4). Es decir, la clave secreta de segundo nivel sk_2 se genera en base a los vectores de predicado ($\vec{v}_1$, $\vec{v}_2$). Del mismo modo, un usuario que tiene la clave secreta de segundo nivel sk_2 puede generar una clave secreta de tercer nivel sk_3 en base a la clave secreta de segundo nivel sk_2 y un vector de predicado de tercer nivel $\vec{v}_3$: = (v_5, v_6). Es decir, la clave secreta de tercer nivel sk_3 se genera en base a los vectores de predicado ($\vec{v}_1$, $\vec{v}_2$, $\vec{v}_3$).

La clave secreta de primer nivel sk_1 generada en base al vector de predicado de primer nivel $\vec{v}_1$ es una clave secreta generada por ($\vec{v}_1$, (0, 0), (0, 0)). De esta manera, la clave secreta de primer nivel sk_1 puede descifrar un texto cifrado cifrado por un vector de atributo ($\vec{x}_1$, (*, *), (*, *)): = ((x_1, x_2), (*, *), (*, *)) si $\vec{v}_1 \cdot \vec{x}_1 = 0$. Esto es debido a que (*, *) · (0, 0) = 0. Aquí, “*”indica un valor arbitrario.

Del mismo modo, la clave secreta de segundo nivel sk_2 generada en base a los vectores de predicado de segundo nivel ($\vec{v}_1$, $\vec{v}_2$) es una clave secreta generada por ($\vec{v}_1$, $\vec{v}_2$, (0, 0)). De esta manera, la clave secreta de segundo nivel sk_2 puede descifrar un texto cifrado cifrado por vectores de atributo ($\vec{x}_1$, $\vec{x}_2$, (*, *)): = ((x_1, x_2), (x_3, x_4), (*, *)) si $\vec{v}_1 \cdot \vec{x}_1 = 0$ y $\vec{v}_2 \cdot \vec{x}_2 = 0$.

No obstante, la clave secreta de segundo nivel sk_2 no puede descifrar un texto cifrado cifrado por el vector de atributo de primer nivel $\vec{x}_1$: = (x_1, x_2) (es decir, ($\vec{x}_1$, (*, *), (*, *)). Esto es debido a que si no $\vec{v}_2$ = (0, 0), entonces (*, *) · $\vec{v}_2 \neq 0$ y $\vec{v}_2 \cdot \vec{x}_2 \neq 0$. Por lo tanto, se puede afirmar que la clave secreta de segundo nivel sk_2 tiene capacidades más limitadas que la clave secreta padre sk_1.

<3. Construcciones de los esquemas HPE y HPKEM>

<3-1. Esquema HPE>

Se describirá brevemente una construcción del esquema HPE.

El esquema HPE incluye cinco algoritmos de polinomio-tiempo probabilísticos: Setup, GenKey, Enc, Dec y $Delegate_L$ (L = 1, …, d-1).

(Setup)

El algoritmo Setup toma como entrada un parámetro de seguridad 1^λ y un formato de jerarquía $\vec{\mu}$ y saca una clave pública maestra pk y una clave secreta maestra sk. La clave secreta maestra sk es una clave de nivel superior.

(GenKey)

El algoritmo GenKey toma como entrada la clave pública maestra pk, la clave secreta maestra sk y vectores de predicado mostrados en la Fórmula 119 y saca una clave secreta de nivel de orden L mostrada en la Fórmula 120.

[Fórmula 119]

$$(\vec{v}_1,\ldots,\vec{v}_L)$$

[Fórmula 120]

$$\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_L)}$$

(Enc)

El algoritmo Enc toma como entrada la clave pública maestra pk, los vectores de atributo mostrados en la Fórmula 121 y un mensaje m y saca un texto cifrado c. Es decir, el algoritmo Enc saca el texto cifrado c que contiene el mensaje m y cifrado por los vectores de atributo mostrados en la Fórmula 121.

[Fórmula 121]

$$(\vec{x}_1,\ldots,\vec{x}_h)$$

donde

$1 \leq h \leq d$.

(Dec)

El algoritmo Dec toma como entrada la clave pública maestra pk, la clave secreta de nivel de orden L mostrada en la Fórmula 122 y el texto cifrado c y saca o bien el mensaje m o bien un símbolo distinguido 1 $\perp$. El símbolo distinguido 1 $\perp$ es información que indica un fallo de descifrado. Es decir, el algoritmo Dec descifra el texto cifrado c mediante la clave secreta de nivel de orden L y extrae el mensaje m. En caso de fallo de descifrado, el algoritmo Dec saca el símbolo distinguido 1 $\perp$.

[Fórmula 122]

$$\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_L)}$$

donde

$1 \leq L \leq d$.

(Delegate$_L$)

Delegate$_L$ toma como entrada la clave pública maestra pk, la clave secreta de nivel de orden L mostrada en la Fórmula 123 y un vector de predicado de nivel de orden (L+1) mostrado en la Fórmula 124 y saca una clave secreta de nivel de orden (L+1) mostrada en la Fórmula 125. Es decir, el algoritmo Delegate$_L$ saca una clave secreta de nivel más bajo.

[Fórmula 123]

$$\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_L)}$$

[Fórmula 124]

$$\vec{v}_{L+1}$$

[Fórmula 125]

$$\mathbf{sk}_{(\vec{v}_1,\ldots,\vec{v}_{L+1})}$$

<3-2. Esquema HPKEM>

Se describirá brevemente una construcción del esquema HPKEM.

Como con el esquema HPE, el esquema HPKEM incluye cinco algoritmos de polinomio-tiempo probabilísticos: Setup, GenKey, Enc, Dec y Delegate$_L$ (L = 1, …, d-1).

(Setup)

El algoritmo Setup toma como entrada un parámetro de seguridad 1^λ y un formato de jerarquía $\vec{\mu}$ y saca una clave pública maestra pk y una clave secreta maestra sk. La clave secreta maestra sk es una clave de nivel superior.

(GenKey)

El algoritmo GenKey toma como entrada la clave pública maestra pk, la clave secreta maestra sk y los vectores de predicado mostrados en la Fórmula 126 y saca una clave secreta de nivel de orden L mostrada en la Fórmula 127.

[Fórmula 126]

$$(\vec{v}_1,\ldots,\vec{v}_L)$$

[Fórmula 127]

$$\mathbf{sk}_{(\vec{v}_1,\ldots,\vec{v}_L)}$$

(Enc)

El algoritmo Enc toma como entrada la clave pública maestra pk y los vectores de atributo mostrados en la Fórmula 128 y saca un texto cifrado c y una clave de sesión K. Es decir, el algoritmo Enc saca el texto cifrado c que contiene información predeterminada (ρ) y cifrada por los vectores de atributo mostrados en la Fórmula 128 así como la clave de sesión K generada a partir de la información predeterminada (ρ).

[Fórmula 128]

$$(\vec{x}_1,\ldots,\vec{x}_h)$$

donde

$1 \leq h \leq d$.

(Dec)

El algoritmo Dec toma como entrada la clave pública maestra pk, la clave secreta de nivel de orden L mostrada en la Fórmula 129 y el texto cifrado c y saca o bien la clave de sesión K o bien un símbolo distinguido 1 $\perp$. El símbolo distinguido 1 $\perp$ es información que indica un fallo de descifrado. Es decir, el algoritmo Dec descifra el texto cifrado c mediante la clave secreta de nivel de orden L, extrae la información sobre la información predeterminada (ρ) y genera la clave de sesión K. En el caso de fallo de descifrado, el algoritmo Dec saca el símbolo distinguido 1 $\perp$.

[Fórmula 129]

$$\mathbf{sk}_{(\vec{v}_1,\ldots,\vec{v}_L)}$$

(Delegate$_L$)

El algoritmo $Delegate_L$ toma como entrada la clave pública maestra pk, la clave secreta de nivel de orden L mostrada en la Fórmula 130 y un vector de predicado de nivel de orden (L+1) mostrado en la Fórmula 131 y saca una clave secreta de nivel de orden (L+1) mostrada en la Fórmula 132. Es decir, el algoritmo $Delegate_L$ saca una clave secreta de nivel más bajo.

[Fórmula 130]

$$sk_{(\vec{v}_1,\ldots,\vec{v}_L)}$$

[Fórmula 131]

$$\vec{v}_{L+1}$$

[Fórmula 132]

$$sk_{(\vec{v}_1,\ldots,\vec{v}_{L+1})}$$

<3-3. Sistema de procesamiento criptográfico 10>

Se describirá el sistema de procesamiento criptográfico 10. El sistema de procesamiento criptográfico 10 ejecuta los algoritmos descritos anteriormente de los esquemas HPE y HPKEM.

La Fig. 7 es un diagrama de configuración del sistema de procesamiento criptográfico 10.

El sistema de procesamiento criptográfico 10 incluye un dispositivo de generación de clave 100, un dispositivo de cifrado 200, un dispositivo de descifrado 300 y un dispositivo de delegación de clave 400. Aquí, el dispositivo de descifrado 300 incluye el dispositivo de delegación de clave 400. Como se describió anteriormente, el sistema de procesamiento criptográfico 10 implementa procesos criptográficos jerárquicos, de modo que que incluye una pluralidad de los dispositivos de cifrado 200, una pluralidad de los dispositivos de descifrado 300 y una pluralidad de los dispositivos de delegación de clave 400.

El dispositivo de generación de clave 100 ejecuta los algoritmos Setup y GenKey de los esquemas HPKEM y HPE.

El dispositivo de cifrado 200 ejecuta el algoritmo Enc de los esquemas HPKEM y HPE.

El dispositivo de descifrado 300 ejecuta el algoritmo Dec de los esquemas HPKEM y HPE.

El dispositivo de delegación de clave 400 ejecuta el algoritmo $Delegate_L$ de los esquemas HPKEM y HPE.

La Fig. 8 es un diagrama de flujo que muestra operaciones del dispositivo de generación de clave 100, un dispositivo de cifrado de nivel de orden L 200 y un dispositivo de descifrado de nivel de orden L 300 del sistema de procesamiento de criptográfico 10. Es decir, la Fig. 8 es un diagrama de flujo que muestra operaciones a partir de la generación de claves maestras (una clave pública maestra y una clave secreta maestra) y la generación de una clave secreta de nivel de orden L para el cifrado y descifrado en el nivel de orden L.

(S101: Paso de generación de clave)

El dispositivo de generación de clave 100 ejecuta el algoritmo Setup para generar una clave pública maestra pk y una clave secreta maestra sk. En base a la clave pública maestra pk generada, la clave secreta maestra sk generada y un vector de predicado $\vec{v}_L$ ($\vec{v}_L = (v_1, \ldots, v_i)$ ($i = \mu_L$) que corresponde a un dispositivo de descifrado 300 predeterminado (el dispositivo de descifrado 300 de nivel de orden L), el dispositivo de generación de clave 100 ejecuta el algoritmo GenKey para generar una clave secreta de nivel de orden L. Entonces, el dispositivo de generación de clave 100 publica (distribuye) la clave pública maestra pk generada y proporciona en secreto la clave secreta de nivel de orden L al dispositivo de descifrado 300 predeterminado. El dispositivo de generación de clave 100 mantiene en secreto la clave secreta maestra.

(S102: Paso de cifrado)

En base a la clave pública maestra pk distribuida por el dispositivo de generación de clave 100 en (S101) y un vector de atributo $\vec{x}_L$ ($\vec{x}_L = (x_1, \ldots, x_i)$ ($i = \mu_L$) del dispositivo de descifrado 300, el dispositivo de cifrado 200 ejecuta el algoritmo Enc para generar un texto cifrado c. En el caso del esquema HPKEM, el dispositivo de cifrado 200 también genera una clave de sesión K. Entonces, el dispositivo de cifrado 200 transmite el texto cifrado c generado al

dispositivo de descifrado 300 a través de una red o similar. El vector de atributo $\vec{x}_L$ puede ser público o se puede obtener por el dispositivo de cifrado 200 a partir del dispositivo de generación de clave 100 o el dispositivo de descifrado 300.

(S103: Paso de descifrado)

En base a la clave pública maestra pk y la clave secreta de nivel de orden L proporcionada por el dispositivo de generación de clave 100 en (S101), el dispositivo de descifrado 300 ejecuta el algoritmo Dec para descifrar el texto cifrado c recibido desde el dispositivo de cifrado 200. Como resultado del descifrado del texto de cifrado c, el dispositivo de descifrado 300 obtiene la clave de sesión K en el caso del esquema HPKEM u obtiene el mensaje m en el caso del esquema HPE. En caso de fallo de descifrado, el dispositivo de descifrado 300 saca un símbolo distinguido 1 $\perp$.

La Fig. 9 muestra un diagrama de flujo que muestra operaciones de un dispositivo de delegación de clave de nivel de orden L 400, un dispositivo de cifrado de nivel de orden (L+1) 200 y un dispositivo de descifrado de nivel de orden (L+1) 300 del sistema de procesamiento criptográfico 10. Es decir, la Fig. 9 es un diagrama de flujo que muestra operaciones de la generación de una clave secreta de nivel de orden (L+1) para el cifrado y descifrado en el nivel de orden (L+1).

(S201: Paso de delegación de clave)

En base a la clave pública maestra pk distribuida por el dispositivo de generación de clave 100 en (S101), la clave secreta de nivel de orden L proporcionada por el dispositivo de generación de clave 100 o un dispositivo de delegación de clave de nivel de orden (L-1) 400 y un vector de predicado $\vec{v}_{L+1}$ ($\vec{v}_{L+1} = (v_i, \ldots, v_j)$ ($i = \mu_L+1$, $j = \mu_{L+1}$)) que corresponde al dispositivo de descifrado de nivel de orden (L+1) 300, el dispositivo de delegación de nivel de orden L 400 (el dispositivo de delegación de clave 400 incluido en el dispositivo de descifrado de nivel de orden L 300) ejecuta el algoritmo Delegate_L para generar una clave secreta de nivel de orden (L+1). Entonces, el dispositivo de delegación de clave de nivel de orden L 400 proporciona en secreto la clave secreta generada al dispositivo de descifrado de nivel de orden (L+1) 300.

(S202: Paso de cifrado)

En base a la clave pública maestra pk distribuida por el dispositivo de generación de clave 100 en (S101) y los vectores de atributo $\vec{x}_1$ a $\vec{x}_{L+1}$ ($\vec{x}_i$ ($i = 1, \ldots, L+1$) (= ($x_1, \ldots, x_i$) ($i = \mu_{L+1}$))) de los dispositivos de descifrado de primer nivel al de orden (L+1) 300, el dispositivo de cifrado 200 ejecuta el algoritmo Enc para generar un texto cifrado c. En el caso del esquema HPKEM, el dispositivo de cifrado 200 también genera una clave de sesión K. Entonces, el dispositivo de cifrado 200 transmite el texto cifrado c generado al dispositivo de descifrado 300 a través de una red o similar. Los vectores de atributo $\vec{x}_1$ a $\vec{x}_{L+1}$ ($\vec{x}_i$ ($i = 1, \ldots, L+1$)) pueden ser públicos o se pueden obtener por el dispositivo de cifrado 200 a partir del dispositivo de generación de clave 100 o el dispositivo de descifrado 300.

(S203: Paso de descifrado)

En base a la clave pública maestra pk distribuida por el dispositivo de generación de clave 100 en (S101) y la clave secreta proporcionada por el dispositivo de generación de clave de nivel de orden L 400 en (S201), el dispositivo de descifrado 300 ejecuta el algoritmo Dec para descifrar el texto cifrado c recibido desde el dispositivo de cifrado 200. Como resultado del descifrado del texto cifrado c, el dispositivo de descifrado 300 obtiene la clave de sesión K en el caso del esquema HPKEM u obtiene el mensaje m en el caso del esquema HPE.

<4. Conceptos para implementar los esquemas HPKEM y HPE>

Se describirán ahora conceptos requeridos para implementar los algoritmos descritos anteriormente de los esquemas HPKEM y HPE.

El método para implementar los procesos criptográficos se describirán usando un ejemplo en el cual espacios de vectores de emparejamiento duales (DPVS) que se describen más tarde se construyen por productos directos de grupos de emparejamiento asimétricos. No obstante, los DPVS no están limitados a los realizados por productos directos de grupos de emparejamiento asimétricos. Es decir, los procesos criptográficos que se describen más adelante se pueden implementar en DPVS construidos por otros métodos. Tres ejemplos típicos de DPVS se tratan en la Literatura no de Patente 17.

<4-1. Grupos de emparejamiento bilineal>

Se describirán grupos de emparejamiento bilineal ($q, G_1, G_2, G_T, g_1, g_2, g_T$).

Los grupos de emparejamiento bilineal ($q, G_1, G_2, G_T, g_1, g_2, g_T$) son una tupla de tres grupos cíclicos G_1, G_2,y G_T de orden q. g_1 es un generador de G_1 y g_2 es un generador de G_2. Los grupos de emparejamiento bilineal ($q, G_1, G_2, G_T, g_1, g_2, g_T$) satisfacen la siguiente condición de emparejamiento bilineal no degenerado:

(Condición: emparejamiento bilineal no degenerado)

Existe un emparejamiento bilineal no degenerado calculable por polinomio-tiempo mostrado en la Fórmula 133.

[Fórmula 133]

$$e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$$

Es decir, para cada $\xi\in\mathbb{G}_1,\ \eta\in\mathbb{G}_2,$

$$e(s\xi,t\eta)=e(\xi,\eta)^{st}$$ y

$$g_T=e(g_1,g_2)\neq 1.$$

Este se llama emparejamiento bilineal simétrico cuando $G_1 = G_2$ (=: G) y emparejamiento bilineal asimétrico cuando $G_1 \neq G_2$. Un emparejamiento bilineal simétrico se puede construir usando curvas (hiper) elípticas supersingulares. Por otra parte, un emparejamiento bilineal asimétrico se puede construir usando cualquier curva (hiper) elíptica. Un emparejamiento bilineal asimétrico se puede construir usando, por ejemplo, curvas elípticas ordinarias.

<4-2. Espacios de vectores V y V*>

Un grupo cíclico (espacio unidimensional) se extiende a un espacio (vector) dimensional más alto. Es decir, como se muestra en la Fórmula 134, los espacios de vectores N dimensionales V y V* se construyen por productos directos de G_1 y G_2.

[Fórmula 134]

$$\mathbb{V}:=\overbrace{\mathbb{G}_1\times\cdots\times\mathbb{G}_1}^{N},$$

$$\mathbb{V}^*:=\overbrace{\mathbb{G}_2\times\cdots\times\mathbb{G}_2}^{N},$$

donde un elemento x del espacio $\mathbb{V}$ se representa por un vector N dimensional como

$$x:=(x_1g_1,\ldots,x_Ng_1)$$ y

del mismo modo, un elemento y del espacio $\mathbb{V}^*$ se representa por un vector N dimensional como

$$y:=(y_1g_2,\ldots,y_Ng_2),$$

donde $x_i,y_i\in\mathbb{F}_q$ para *i = 1, …, N*.

<4-3. Bases duales canónicas A y A*>

Se describirán las bases canónicas A y A* de los espacios de vectores N dimensionales V y V*.

La Fórmula 135 muestra las bases canónicas A y A*.

[Fórmula 135]

$$\mathbb{A}:=(a_1,\ldots,a_N),$$

$$\mathbb{A}^*:=(a_1^*,\ldots,a_N^*),$$

donde

$$a_1 := (g_1, 0, \ldots, 0), a_2 := (0, g_1, 0, \ldots, 0), \ldots, a_N := (0, \ldots, 0, g_1) ,$$
$$a_1^* := (g_2, 0, \ldots, 0), a_2^* := (0, g_2, 0, \ldots, 0), \ldots, a_N^* := (0, \ldots, 0, g_2).$$

Las bases canónicas A y A* satisfacen las condiciones mostradas en la Fórmula 136.

[Fórmula 136]

$$e\left(a_i, a_j^*\right) = g_T^{\delta_{i,j}} \qquad i, j \in \{1, \ldots, N\}$$

donde

$$\delta : \text{Kronecker } \delta \text{ (es decir, } \delta_{i,j} = 1 \text{ si } i = j \quad \text{y} \quad \delta_{i,j} = 0 \text{ si } i \neq j),$$

$$g_T := e(g_1, g_2) \neq 1$$

Es decir, las bases canónicas A y A* son bases ortonormales duales y los espacios V y V* son espacios de vectores duales emparejados a través de la operación de emparejamiento e.

Se explicará además la declaración de que las bases canónicas A y A* satisfacen las condiciones mostradas en la Fórmula 136.

En primer lugar, se explicará la ecuación $e(a_i, a^*_i) = g_T$. Por poner un ejemplo, se calculará $e(a_1, a^*_1)$. En base a $a_1 = (g_1, 0, \ldots, 0)$ y $a^*_1 = (g_2, 0, \ldots, 0)$ como se describió anteriormente, sigue que: $e(a_1, a^*_1) = e(g_1, g_2) \times e(0, 0) \times, \ldots, \times e(0, 0)$. Aquí, como se describió anteriormente, se mantiene la ecuación $e(g_1, g_2) = g_T$. También, en base a $e(0, 0) = e(0 \cdot g_1, 0 \cdot g_2) = e(g_1, g_2)^0$, sigue que: $e(0, 0) = 1$. De esta manera, se mantiene la ecuación $e(a_1, a^*_1) = g_T$. Los mismos cálculos también se mantienen para otros $e(a_i, a^*_i)$, de modo que se mantiene la ecuación $e(a_i, a^*_i) = g_T$.

A continuación, se explicará la ecuación $e(a_i, a^*_j) = 1$ $(i \neq j)$. Por poner un ejemplo, se calculará $e(a_1, a^*_2)$. En base a $a_1 = (g_1, 0, \ldots, 0)$ y $a^*_2 = (0, g_2, 0, \ldots, 0)$ como se describió anteriormente, sigue que: $e(a_1, a^*_2) = e(g_1, 0) \times e(0, g_2) \times e(0, 0) \times, \ldots, \times e(0, 0)$. En base a $e(g_1, 0) = e(g_1, 0 \cdot g_2) = e(g_1, g_2)^0$, se mantiene la ecuación $e(g_1, 0) = 1$. Del mismo modo, se mantiene la ecuación $e(0, g_2) = 1$. También, como se describió anteriormente, se mantiene la ecuación $e(0, 0) = 1$. De esta manera, se mantiene la ecuación $e(a_i, a^*_j) = 1$. Los mismos cálculos también se mantienen para otros $e(a_i, a^*_j)$, de modo que se mantiene la ecuación $e(a_i, a^*_j) = 1$.

De esta manera, las ecuaciones $e(a_i, a^*_i) = g_T$ y $e(a_i, a^*_j) = 1$ $(i \neq j)$ se mantienen sobre las bases canónicas A y A*.

<4-4. Operación de emparejamiento>

Una operación de emparejamiento e en los espacios de vectores N dimensionales V y V* se define como se muestra en la Fórmula 137.

[Fórmula 137]

$$e(x, y) := \prod_{i=1}^{N} e(x_i g_1, y_i g_2)$$

Es decir, la operación de emparejamiento e (x, y) en un vector x: = $(x_1 g_1, x_2 g_1, \ldots, x_N g_1)$ del espacio de vector N dimensional V y un vector y: = $(y_1 g_2, y_2 g_2, \ldots, y_N g_2)$ del espacio de vector N dimensional V* se define como el producto de operaciones de emparejamiento en los elementos respectivos de los vectores x e y. Entonces, en base a la condición descrita anteriormente de emparejamiento bilineal no degenerado, la operación de emparejamiento e (x, y) se puede expresar como se muestra en la Fórmula 138.

[Fórmula 138]

$$e(x, y) := \prod_{i=1}^{N} e(x_i g_1, y_i g_2) = e(g_1, g_2)^{\sum_{i=1}^{N} x_i y_i} = g_T^{\vec{x} \cdot \vec{y}} \in \mathbb{G}_T$$

<4-5. Cambio de base>

Se describirá un método de cambio de base para cambiar las bases canónicas A y A* a otras bases B y B*. La Fig. 10 es un diagrama para explicar el método de cambio de base.

La base canónica A del espacio V se cambia a otra base B: = (b_1, …, b_N) del espacio V. Usando una transformación lineal elegida uniformemente X mostrada en la Fórmula 139, la base canónica A del espacio V se cambia a otra base B del espacio V como se muestra en la Fórmula 140.

[Fórmula 139]

$$X := \left(x_{i,j}\right) \xleftarrow{\mathrm{U}} GL\left(N, \mathbb{F}_q\right)$$

[Fórmula 140]

$$b_i = \sum_{j=1}^{N} x_{i,j} a_j \qquad i = 1, \ldots, N$$

donde

$$\mathbb{B} := \left(b_1, \ldots, b_N\right).$$

Aquí, GL representa lineal general. Es decir, GL es un grupo lineal general, un conjunto de matrices cuadradas con determinantes no cero y un grupo bajo multiplicación.

Usando X, la base B*: = (b^*_1, …, b^*_N) del espacio V* se puede calcular eficientemente a partir de la base canónica A* del espacio V*. La base B* del espacio V* se calcula usando X como se muestra en la Fórmula 141.

[Fórmula 141]

$$b_i^* = \sum_{j=1}^{N} v_{i,j} a_j^* \qquad i = 1, \ldots, N$$

donde

$$\left(v_{i,j}\right) := \left(X^T\right)^{-1},$$

$$\mathbb{B}^* := \left(b_1^*, \ldots, b_N^*\right).$$

Aquí, se mantiene la Fórmula 142.

[Fórmula 142]

$$e\left(b_i, b_j^*\right) = g_T^{\delta_{i,j}} \qquad i, j \in \{1, \ldots, N\}$$

donde

$$\delta : \text{Kronecker } \delta \text{ (es decir, } \delta_{i,j} = 1 \text{ si } i = j \quad \text{y} \quad \delta_{i,j} = 0 \text{ si } i \neq j),$$

$$g_T := e\left(g_1, g_2\right) \neq 1$$

Es decir, las bases B y B* son bases ortonormales duales de los espacios duales V y V*. Esto significa que incluso cuando las bases canónicas A y A* se cambian usando X, se conservan las bases ortonormales duales.

<4-6. Mapas de distorsión>

Se describirá una transformación lineal, llamada un mapa de distorsión, para un generador x en el espacio V sobre la base canónica A.

Un mapa de distorsión $\varphi_{i,j}$ en la base canónica A del espacio V es un mapa mostrado en la Fórmula 143.

[Fórmula 143]

Si $\phi_{i,j}(a_j) = a_i$ y

$k \neq j$, entonces $\phi_{i,j}(a_k) = 0$.

Dado que se mantiene la Fórmula 144, el mapa de distorsión $\varphi_{i,j}$ puede lograr la transformación mostrada en la Fórmula 145.

[Fórmula 144]

$$\phi_{i,j}(x) = \phi_{i,j}(x_1 a_1 + x_2 a_2 + \cdots + x_N a_N) = \phi_{i,j}(x_j a_j)$$
$$= x_j \phi_{i,j}(a_j) = x_j a_i$$

[Fórmula 145]

Para $x := (x_1 g_1, \ldots, x_j g_1, \ldots, x_N g_1)$,

$$\phi_{i,j}(x) := (\overbrace{0,\ldots,0}^{i-1}, x_j g_1, \overbrace{0,\ldots,0}^{N-i})$$

Es decir, un elemento, esto es un vector de base j, en la base canónica A del vector x se puede transformar en otro elemento, esto es un vector de base i, en la base canónica A. En este momento, elementos distintos del vector de base j que se transforma todos llegan a ser 0. Es decir, en el vector x, el vector de base j llega a ser el vector de base i y otros elementos llegan a ser 0.

Un mapa de distorsión $\varphi^*_{i,j}$ en la base canónica A* del espacio V* se puede representar de la misma manera que el mapa de distorsión $\varphi_{i,j}$ en la base canónica A del espacio V.

Usando el mapa de distorsión $\varphi_{i,j}$ ($\varphi^*_{i,j}$) cualquier transformación lineal W, expresada como una matriz NxN mostrada en la Fórmula 146, para $x \in V$ se puede calcular eficientemente mediante la Fórmula 147.

[Fórmula 146]

$$(\gamma_{i,j}) \in \mathbb{F}_q^{N \times N}$$

[Fórmula 147]

$$W(x) := \sum_{i=1,j=1}^{N,N} \gamma_{i,j} \phi_{i,j}(x)$$

<5. Espacios de vectores de emparejamiento duales (DPVS)>

En base a los conceptos descritos en el anterior 4, se describirán espacios de vectores de emparejamiento duales (DPVS). Los esquemas HPE y HPKEM que se describen más tarde se implementan en DPVS.

Los DPVS (q, V, V*, G_T, A, A*) incluyen un orden primo q, dos espacios de vectores N dimensionales V y V* sobre F_q, un grupo cíclico G_T de orden q, una base canónica A: = (a_1, …, a_{N-1}) del espacio V y una base canónica A*: = (a^*_1, …, a^*_{N-1}) del espacio V*. Los DPVS (q, V, V*, G_T, A, A*) satisfacen las tres condiciones siguientes: (1) existe un emparejamiento bilineal no degenerado, (2) las bases canónicas A y A* son bases ortonormales duales y (3) existen mapas de distorsión.

(1) Emparejamiento bilineal no degenerado (Ver el anterior 4-1.)

Existe un emparejamiento bilineal no degradable calculable por polinomio-tiempo e.

Es decir, la primera condición es que existe un emparejamiento bilineal no degenerado e mostrado en la Fórmula 148.

[Fórmula 148]

$$e: \mathbb{V} \times \mathbb{V}^* \rightarrow \mathbb{G}_T$$

Es decir, si *e(sx, ty) = e(x, y)st y*

e(x, y) = 1 para todo y $\in \mathbb{V}$, entonces x = 0.

(2) Bases ortonormales duales (Ver el anterior 4-2.)

Las bases canónicas A y A* de los espacios V y V* son bases ortonormales duales.

Es decir, la segunda condición es que las bases canónicas A y A* de los espacios V y V* satisfacen la condición mostrada en la Fórmula 149.

[Fórmula 149]

$$e\left(a_i, a_j^*\right) = g_T^{\delta_{i,j}}$$ para cada i y j,

donde

δ : Kronecker δ (es decir, $\delta_{i,j} = 1$ si $i = j$ y $\delta_{i,j} = 0$ si $i \neq j$),

$$g_T \neq 1 \in \mathbb{G}^T$$

.

(3) Mapas de distorsión (Ver el anterior 4-6.)

Existen mapas de distorsión calculables por polinomio-tiempo $\varphi_{i,j}$ y $\varphi^*_{i,j}$.

Es decir, la tercera condición es que los endomorfismos $\varphi_{i,j}$ y $\varphi^*_{i,j}$ de los espacios V y V* mostrados en la Fórmula 150 son calculables por polinomio-tiempo.

[Fórmula 150]

Si $\phi_{i,j}\left(a_j\right) = a_i$ y

$k \neq j$, entonces $\phi_{i,j}\left(a_k\right) = 0$.

Si $\phi^*_{i,j}\left(a^*_j\right) = a^*_i$ y

$k \neq j$, entonces $\phi^*_{i,j}\left(a^*_k\right) = 0$.

Satisfaciendo la segunda condición, también se puede afirmar que los espacio V y V* son espacios duales emparejados a través de la operación de emparejamiento e (ver el anterior 4-2).

<6. Esbozo de un método para implementar los esquemas HPKEM y HPE>

En base a los conceptos (ver el anterior 4) y los DPVS (ver el anterior 5) descrito anteriormente, se describirá brevemente un método mediante el cual el sistema de procesamiento criptográfico 10 mencionado anteriormente (ver el anterior 3) implementa los esquemas HPE y HPKEM.

En primer lugar, se describirá un esbozo del esquema PE para predicados de producto interior que se implementan por el sistema de procesamiento criptográfico 10. Por simplicidad de descripción, se omitirá la noción de jerárquico y se describirá un esbozo del esquema PE para predicados de producto interior solamente con un nivel.

El sistema de procesamiento criptográfico 10 implementa el sistema PE para predicados de producto interior en los DPVS (q, V, V*, G_T, A, A*), donde los espacios V y V* son espacios (n+3) dimensionales.

El dispositivo de generación de clave 100 genera bases ortogonales B: = (b_1, …, b_{n+3}) y B*: = (b^*_1, …, b^*_{n+3}) a partir de las bases canónicas A y A* mediante el método de cambio de base descrito en el anterior 4-5. El dispositivo de generación de clave 100 genera una base B^: = (b_1, …, b_n, d_{n+1}, b_{n+3}) en la que vectores de base b_{n+1} y b_{n+2} de la base B: = (b_1, …, b_{n+3}) se sustituyen con un vector de base d_{n+1} que es la suma de los vectores de base b_{n+1} y b_{n+2}. La base B^ se usa como una clave pública maestra pk y la base B* se usa como una clave secreta maestra sk. Además, el dispositivo de generación de clave 100 genera una clave secreta k* a partir de un vector de predicado $\vec{v}$ ($\vec{v}$ = (v_1, …, v_n) $\in F^n_q$) como se muestra en la Fórmula 151 y transmite en secreto la clave secreta k* al dispositivo de descifrado 300.

[Fórmula 151]

$$k^* := \sigma\left(v_1 b_1^* + \cdots + v_n b_n^*\right) + \eta b_{n+1}^* + (1-\eta) b_{n+2}^*$$

donde

$$\sigma, \eta \xleftarrow{U} \mathbb{F}_q .$$

El dispositivo de cifrado 200 genera dos textos cifrados c_1 y c_2 a partir de un vector de atributo $\vec{x}$ ($\vec{x}$ = (x_1, …, x_n) $\in F^n_q$) y un mensaje m. Los textos cifrados c_1 y c_2 se generan como se muestra Fórmula 152.

[Fórmula 152]

$$c_1 := \delta_1\left(x_1 b_1 + \cdots + x_n b_n\right) + \zeta d_{n+1} + \delta_2 b_{n+3},$$

$$c_2 := g_T^{\zeta} m$$

donde

$$\delta_1, \delta_2, \zeta \xleftarrow{U} \mathbb{F}_q .$$

En base a los textos cifrados c_1 y c_2 y la clave secreta k*, el dispositivo de descifrado 300 calcula la Fórmula 153 para extraer el mensaje m.

[Fórmula 153]

$$m := c_2 / e\left(c_1, k^*\right)$$

Si $\vec{v} \cdot \vec{x}$ = 0, el dispositivo de descifrado 300 puede obtener el mensaje m calculando la Fórmula 153 como se muestra en la Fórmula 154.

[Fórmula 154]

$$\begin{aligned} & e\left(c_1, k^*\right) \\ &= \left(\prod_{i=1}^{n} e\left(\delta_1 x_i b_i, \sigma v_i b_i^*\right) \cdot e\left(\zeta b_{n+1}, \eta b_{n+1}^*\right) \cdot e\left(\zeta b_{n+2}, (1-\eta) b_{n+2}^*\right)\right) \\ &= g_T^{\delta_1 \sigma\left(\sum_{i=1}^{n} x_i v_i\right) + \zeta\eta + \zeta(1-\eta)} \\ &= g_T^{\zeta} \end{aligned}$$

A continuación, un esbozo del esquema PE para predicados de producto interior con capacidad de delegación jerárquica, es decir el esquema HPE para los predicados de producto interior, se describirá usando un simple ejemplo. El ejemplo emplea espacios 9 dimensionales, cada espacio que tiene seis dimensiones (tres niveles, cada uno que tiene dos dimensiones) que se usan para vectores de predicado y vectores de atributo y otras tres dimensiones. Es decir, los espacios V y V* son espacios 9 dimensionales. Por lo tanto, una clave pública maestra incluye una base B^: = (b_1, …, b_6, d_7, b_9), donde d_7: = b_7 + b_8. Una clave secreta maestra incluye una base B*: (b^*_1, …, b^*_9).

En la siguiente descripción, un subíndice “dec” representa “descifrado” e indica un vector de clave usado para descifrar un texto cifrado. Un subíndice “ran” representa “aleatorización” e indica un vector de aleatorización para

aleatorizar el coeficiente de un vector de base predeterminado de una clave de nivel más bajo. Un subíndice “del” representa “delegación” e indica un vector de generación de clave para generar un vector de clave de nivel más bajo.

Los textos cifrados c_1 y c_2 se generan mediante los vectores de atributo $(\vec{x}_1, \vec{x}_2, \vec{x}_3) = ((x_1, x_2), (x_3, x_4), (x_5, x_6))$ y un mensaje m, como se muestra en la Fórmula 155.

[Fórmula 155]

$$c_1 := \delta_1 (x_1 b_1 + x_2 b_2) + \cdots + \delta_3 (x_5 b_5 + x_6 b_6) + \zeta d_7 + \delta_4 b_9,$$

$$c_2 := g_T^{\zeta} m$$

donde

$$\delta_1, \ldots, \delta_4, \zeta \xleftarrow{U} \mathbb{F}_q.$$

Si el vector de atributo es de un nivel más alto tal como $\vec{x}_1 := (x_1, x_2)$, el vector de atributo se modifica como se muestra en la Fórmula 156.

[Fórmula 156]

$$\vec{x}^{+} := \left((x_1, x_2), \left(x_3^{+}, x_4^{+}\right), \left(x_5^{+}, x_6^{+}\right)\right)$$

donde

$$\left(x_3^{+}, x_4^{+}, x_5^{+}, x_6^{+}\right) \xleftarrow{U} \mathbb{F}_q^4.$$

Es decir, el texto cifrado c_1 generado por el vector de atributo $\vec{x}_1$ se genera como el texto cifrado c_1 generado por el vector de atributo $\vec{x}^{+}$ mostrado en la Fórmula 156.

Una clave secreta de primer nivel $\vec{k}^{*}_1 := (k^{*}_{1,dec}, k^{*}_{1,ran,1}, k^{*}_{1,ran,2}, k^{*}_{1,del,3}, \ldots, k^{*}_{1,del,6})$ generada en base a un vector de predicado de primer nivel $\vec{v}_1 := (v_1, v_2) \in F^2_q$ consta de tres tipos de elementos: $k^{*}_{1,dec}$, $(k^{*}_{1,ran,1}, k^{*}_{1,ran,2})$ y $(k^{*}_{1,del,3}, \ldots, k^{*}_{1,del,6})$. $k^{*}_{1,dec}$ es un vector de clave usado para descifrar un texto cifrado. $(k^{*}_{1,ran,1}, k^{*}_{1,ran,2})$ son vectores de aleatorización para aleatorizar el coeficiente de un vector de base predeterminado de un vector de clave de nivel más bajo. $(k^{*}_{1,del,3}, \ldots, k^{*}_{1,del,6})$ son vectores de generación de clave para generar un vector de clave de nivel más bajo. $k^{*}_{1,dec}$, $(k^{*}_{1,ran,1}, k^{*}_{1,ran,2})$ y $(k^{*}_{1,del,3}, \ldots, k^{*}_{1,del,6})$ se generan como se muestra en la Fórmula 157.

[Fórmula 157]

$$k^{*}_{1,\mathrm{dec}} := \sigma_{1,0} \left(v_1 b_1^{*} + v_2 b_2^{*}\right) + \eta_0 b_7^{*} + (1 - \eta_0) b_8^{*},$$

$$k^{*}_{1,\mathrm{ran},j} := \sigma_{1,j} \left(v_1 b_1^{*} + v_2 b_2^{*}\right) + \eta_j b_7^{*} - \eta_j b_8^{*} \qquad (j = 1,2),$$

$$k^{*}_{1,\mathrm{del},j} := \sigma_{1,j} \left(v_1 b_1^{*} + v_2 b_2^{*}\right) + \psi b_j^{*} + \eta_j b_7^{*} - \eta_j b_8^{*} \qquad (j = 3,\ldots,6)$$

donde

$$\sigma_{1,j}, \eta_j, \psi \xleftarrow{U} \mathbb{F}_q \qquad (j = 0,\ldots,6).$$

Si los vectores de atributo usados en la generación del texto cifrado c_1 es $((x_1, x_2), (*, *), (*, *))$ de manera que $(x_1, x_2) \cdot (v_1, v_2) = 0$, entonces se mantiene la Fórmula 158. Por lo tanto, $k^{*}_{1,0}$ puede descifrar los textos cifrados c_1 y c_2 calculando la Fórmula 159.

[Fórmula 158]

$$e\left(c_1, k^{*}_{1,\mathrm{dec}}\right) = g_T^{\zeta}$$

[Fórmula 159]

$c_2 / e\left(c_1, k^*_{1,0}\right)$

Una clave secreta de segundo nivel $\vec{k}^*_2$: = ($k^*_{2,dec}$, $k^*_{2,ran,1}$, $k^*_{2,ran,2}$, $k^*_{2,ran,3}$, $k^*_{2,del,5}$, $k^*_{2,del,6}$) se genera mediante un vector de predicado de segundo nivel $\vec{v}_2$: = (v_3, v_4).

Para generar $k^*_{2,dec}$, $\sigma_{2,0}$ ($v_3 k^*_{1,del,3} + v_4 k^*_{1,del,4}$) se añade a $k^*_{1,dec}$. Para generar $k^*_{2,ran,j}$, $\sigma_{2,j}$ ($v_3 k^*_{1,del,3} + v_4 k^*_{1,del,4}$) se añade a 0 (j = 1, 2, 3). Para generar $k^*_{2,del,j}$, $\sigma_{2,j}$ ($v_3 k^*_{1,del,3} + v_4 k^*_{1,del,4}$) se añade a $\psi^+ k^*_{1,del,j}$ (j = 5, 6). Aquí, $\sigma_{2,j}$ (j = 0, 1, 2, 3, 5. 6) y ψ^+ son valores seleccionados uniformemente.

Además, los coeficientes de ($v_1 b^*_1 + v_2 b^*_2$), b^*_7 y b^*_8 de la clave secreta de segundo nivel están aleatorizados (distribuidos uniformemente). Por lo tanto, para generar $k^*_{2,\ dec}$, también se añade ($\alpha_{0,1}\ k^*_{1,ran,1} + \alpha_{0,2}\ k^*_{1,ran,2}$). Para generar $k^*_{2,ran,j}$, se añade ($\alpha_{j,1}\ k^*_{1,ran,1} + \alpha_{j,2}\ k^*_{1,ran,2}$) (j = 1, 2, 3). Para generar $k^*_{2,del,j}$, se añade ($\alpha_{j,1}\ k^*_{1,ran,1} + \alpha_{j,2}\ k^*_{1,ran,2}$) (j = 5, 6). Aquí, $\alpha_{j,1}$ y $\alpha_{j,2}$ (j = 0, 1, 2, 3, 5, 6) son valores seleccionados uniformemente.

Para resumir, la clave secreta de segundo nivel $\vec{k}^*_2$: = ($k^*_{2,dec}$, $k^*_{2,ran,1}$, $k^*_{2,ran,2}$, $k^*_{2,ran,3}$, $k^*_{2,del,5}$, $k^*_{2,del,6}$) se genera como se muestra en la Fórmula 160.

[Fórmula 160]

$$k^*_{2,\mathrm{dec}} := k^*_{1,\mathrm{dec}} + \left(\alpha_{0,1} k^*_{1,\mathrm{ran},1} + \alpha_{0,2} k^*_{1,\mathrm{ran},2}\right) + \sigma_{2,0}\left(v_3 k^*_{1,\mathrm{del},3} + v_4 k^*_{1,\mathrm{del},4}\right),$$

$$k^*_{2,\mathrm{ran},j} := \left(\alpha_{j,1} k^*_{1,\mathrm{ran},1} + \alpha_{j,2} k^*_{1,\mathrm{ran},2}\right) + \sigma_{2,j}\left(v_3 k^*_{1,\mathrm{del},3} + v_4 k^*_{1,\mathrm{del},4}\right) \qquad (j = 1,2,3),$$

$$k^*_{2,\mathrm{del},j} := \psi^+ k^*_{1,\mathrm{del},j} + \left(\alpha_{j,1} k^*_{1,\mathrm{ran},1} + \alpha_{j,2} k^*_{1,\mathrm{ran},2}\right) + \sigma_{2,j}\left(v_3 k^*_{1,\mathrm{del},3} + v_4 k^*_{1,\mathrm{del},4}\right) \qquad (j = 5,6)$$

donde

$$\alpha_{j,1}, \alpha_{j,2}, \sigma_{2,j}, \psi^+ \xleftarrow{\mathrm{U}} \mathbb{F}_q \qquad (j = 0,1,2,3,5,6).$$

$k^*_{2,dec}$ es un vector de clave usado para descifrar un texto cifrado. ($k^*_{2,ran,1}$, $k^*_{2,ran,2}$, $k^*_{2,ran,3}$) son vectores de aleatorización para aleatorizar el coeficiente de un vector de base predeterminado de un vector de clave de nivel más bajo. ($k^*_{2,del,5}$, $k^*_{2,del,6}$) se usan para generar una clave de nivel más bajo.

En general, en una clave secreta de nivel de orden L $\vec{k}^*_L$: = ($k^*_{L,dec}$, $k^*_{L,ran,j}$, $k^*_{L,del,j}$), $k^*_{L,dec}$ es un vector de clave usado para descifrar un texto cifrado. $k^*_{L,ran,j}$ es un vector de aleatorización para aleatorizar el coeficiente de un vector de base predeterminado de un vector de clave de nivel más bajo. $k^*_{L,del,j}$ es un vector de generación de clave para generar un vector de clave de nivel más bajo.

Segunda realización

En esta realización, en base a los conceptos descritos en la primera realización, se describirá el sistema de procesamiento criptográfico 10 que implementa el esquema HPE.

Con referencia a las Fig. 11 a 16, se describirán funciones y operaciones del sistema de procesamiento criptográfico 10 según la segunda realización.

La Fig. 11 es un diagrama de bloques funcional que muestra las funciones del sistema de procesamiento criptográfico 10 que implementa el esquema HPE. Como se describió anteriormente, el sistema de procesamiento criptográfico 10 incluye el dispositivo de generación de clave 100, el dispositivo de cifrado 200, el dispositivo de descifrado 300 y el dispositivo de delegación de clave 400. Se supone en esta realización que el dispositivo de descifrado 300 incluye el dispositivo de delegación de clave 400.

La Fig. 12 es un diagrama de flujo que muestra operaciones del dispositivo de generación de clave 100. La Fig. 13 es un diagrama de flujo que muestra operaciones del dispositivo de cifrado 200. La Fig. 14 es un diagrama de flujo que muestra operaciones del dispositivo de descifrado 300. La Fig. 15 es un diagrama de flujo que muestra operaciones del dispositivo de delegación de clave 400.

La Fig. 16 es un diagrama conceptual que muestra una estructura sobre una base de espacios de vectores de emparejamiento duales (DPVS).

Se describirán las funciones y operaciones del dispositivo de generación de clave 100. El dispositivo de generación de clave 100 incluye una unidad de generación de clave maestra 110, una unidad de almacenamiento de clave maestra 120, una unidad de generación de vector clave 130, una unidad de generación de vector de aleatorización 140, una unidad de generación de vector de generación de clave 150 y una unidad de distribución de clave 160.

(S301: Paso de generación de clave maestra)

Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 calcula la Fórmula 161 para generar una clave pública maestra pk y una clave secreta maestra sk y almacena las claves generadas en la unidad de almacenamiento de clave maestra 120.

[Fórmula 161]

(1)

$$N := n+3,$$
$$\left(q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*\right) \xleftarrow{R} \mathcal{G}_{\mathsf{dpvs}}\left(1^\lambda, N\right)$$

(2)

$$X := \left(\chi_{i,j}\right) \xleftarrow{U} GL\left(N, \mathbb{F}_q\right)$$

(3)

$$b_i = \sum_{j=1}^{N} \chi_{i,j} a_j,$$
$$\mathbb{B} := \left(b_1, \ldots, b_N\right)$$

(4)

$$d_{n+1} := b_{n+1} + b_{n+2},$$
$$\hat{\mathbb{B}} := \left(b_1, \ldots, b_n, d_{n+1}, b_{n+3}\right)$$

(5)

$$\left(\upsilon_{i,j}\right) := \left(X^T\right)^{-1}$$

(6)

$$b_i^* = \sum_{j=1}^{N} \upsilon_{i,j} a_j^*,$$
$$\mathbb{B}^* := \left(b_1^*, \ldots, b_N^*\right)$$

(7)

$$\mathsf{sk} := \left(X, \mathbb{B}^*\right), \mathsf{pk} := \left(1^\lambda, q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*, \hat{\mathbb{B}}\right)$$

devolver sk, pk

Es decir: (1) usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 genera el DPVS N(= n+3) dimensional (q, V, V*, G_T, A, A*) con un parámetro de seguridad 1^λ. G_{dpvs} es un algoritmo de generación de DPVS que toma como entrada 1^λ y N y saca un DPVS (q, V, V*, G_T, A, A*) con el parámetro de seguridad 1^λ y espacios N dimensionales.

(2) Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 selecciona aleatoriamente una transformación lineal X a fin de generar una base B a partir de una base canónica A.

(3) Usando el dispositivo de procesamiento y en base a la transformación lineal seleccionada X, la unidad de generación de clave maestra 110 genera la base B: = (b_1, …, b_N) a partir de la base A: = (a_1, …, a_N).

(4) Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 genera un vector de base B^: = (b_1, …, b_n, d_{n+1}, b_{n+3}) en el cual los vectores de base b_{n+1} y b_{n+2} de la base B se sustituyen con un vector de base d_{n+1} que es la suma de los vectores de base b_{n+1} y b_{n*2}.

(5) Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 genera una transformación lineal $(X^T)^{-1}$ a partir de la transformación lineal X a fin de generar una base B*: = (b^*_1, …, b^*_N) a partir de una base A*: = (a^*_1, …, a^*_N).

(6) Usando el dispositivo de procesamiento y en base a la transformación lineal $(X^T)^{-1}$ generada, la unidad de generación de clave maestra 110 genera la base B*: = (b^*_1, …, b^*_N) a partir de la base A*.

(7) La unidad de generación de clave maestra 110 designa la transformación lineal generada X y la base B* como la clave secreta maestra sk y (1^λ, q, V, V*, G_T, A, A*, B^) que incluye la base B^ generada como la clave pública maestra pk. La unidad de almacenamiento de clave maestra 120 almacena en un dispositivo de almacenamiento la clave pública maestra pk y la clave secreta maestra sk generadas por la unidad de generación de clave maestra 110.

Se supone que hay un número N (= n+3) de dimensiones en el DPVS, donde n indica el número de bases asignadas para representar la estructura jerárquica del formato de jerarquía $\vec{\mu}$. Es decir, además del número n de bases asignadas para representar la estructura jerárquica, se proporcionan tres vectores de base. El número de vectores de base, por supuesto, se puede aumentar aún más.

Como se muestra en la Fig. 16, el número n de vectores de base de entre el número N (= n+3) de vectores de base se asignan para los vectores de predicado y los vectores de atributo. La estructura de los vectores de base asignados para los vectores de predicado y los vectores de atributo es la misma que la estructura mostrada en la Fig. 6. Dos de los tres vectores de base restantes (los vectores de base de orden (n+1) y de orden (n+2)) se usan para información para generar una clave de sesión. El restante de los tres vectores de base restantes (el vector de base de orden (n+3)) se usa para aleatorizar el texto cifrado c_1.

Para resumir, en (S301), la unidad de generación de clave maestra 110 ejecuta el algoritmo Setup mostrado en la Fórmula 162 para generar la clave pública maestra pk y la clave secreta maestra sk.

[Fórmula 162]

$$\mathsf{Setup}\left(1^\lambda, \vec{\mu} := (n, d; \mu_1, \ldots, \mu_d)\right):$$
$$\left(\mathsf{param}, \mathbb{B}, \mathbb{B}^*\right) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}\left(1^\lambda, n+3\right),$$
$$d_{n+1} := b_{n+1} + b_{n+2}, \quad \hat{\mathbb{B}} := \left(b_1, \ldots, b_n, d_{n+1}, b_{n+3}\right),$$
$$\text{devolver } \mathsf{sk} := \left(X, \mathbb{B}^*\right), \ \mathsf{pk} := \left(1^\lambda, \mathsf{param}, \hat{\mathbb{B}}\right).$$

donde

$$\mathcal{G}_{\mathsf{ob}}\left(1^\lambda, N\right): \mathsf{param} := \left(q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*\right) \xleftarrow{R} \mathcal{G}_{\mathsf{dpvs}}\left(1^\lambda, N\right),$$
$$X := \left(\chi_{i,j}\right) \xleftarrow{U} GL\left(N, \mathbb{F}_q\right), \ \left(\upsilon_{i,j}\right) := \left(X^{\mathrm{T}}\right)^{-1},$$
$$b_i = \sum_{j=1}^{N} \chi_{i,j} a_j, \ \mathbb{B} := \left(b_1, \ldots, b_N\right),$$
$$b_i^* = \sum_{j=1}^{N} \upsilon_{i,j} a_j^*, \ \mathbb{B}^* := \left(b_1^*, \ldots, b_N^*\right),$$
$$\text{devolver } \left(\mathsf{param}, \mathbb{B}, \mathbb{B}^*\right)$$

(S302: Paso de generación de vector de clave $k^*_{L,dec}$)

Usando el dispositivo de procesamiento y en base a la clave pública maestra pk, la clave secreta maestra sk y los vectores de predicado ($\vec{v}_1$, …, $\vec{v}_L$) mostrados en la Fórmula 163, la unidad de generación de vector de clave 130 calcula la Fórmula 164 para generar un vector de clave $k^*_{L,dec}$ que es el primer elemento de una clave secreta de nivel de orden L (nivel L).

[Fórmula 163]

$$(\vec{v}_1,\ldots,\vec{v}_L) := \left(\left(v_1,\ldots,v_{\mu_1}\right),\ldots,\left(v_{\mu_{L-1}+1},\ldots,v_{\mu_L}\right)\right)$$

[Fórmula 164]

(1)

$$\sigma_{0,i},\eta_0 \xleftarrow{U} \mathbb{F}_q \qquad (i=1,\ldots,L)$$

(2)

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L}\sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \eta_0 b^*_{n+1} + (1-\eta_0) b^*_{n+2}$$

Es decir: (1) usando el dispositivo de procesamiento, la unidad de generación de vector de clave 130 genera números aleatorios $\sigma_{0,i}$ (i = 1, …, L) y η_0.

(2) Usando el dispositivo de procesamiento, la unidad de generación de vector de clave 130 fija cada uno de los vectores de predicado aleatorizados por el número aleatorio generado $\sigma_{0,t}$ como el coeficiente del vector de base b^*_i (i = 1, …, μ_L). Es decir, cada uno de los vectores de predicado se incrusta en el coeficiente del vector de base b^*_i (i = 1, …, μ_L). Usando el dispositivo de procesamiento, la unidad de generación de vector de clave 130 fija el número aleatorio η_0 como el coeficiente del vector de base b^*_{n+1} y fija un valor obtenido restando el número aleatorio η_0 de 1 (1- η_0) como el coeficiente del vector de base b^*_{n+2}. Es decir, los coeficientes de los vectores de base b^*_{n+1} y b^*_{n+2} se fijan de manera que la suma de los coeficientes de los vectores de base b^*_{n+1} y b^*_{n+2} es 1. La unidad de generación de vector de clave 130 de esta manera genera el vector de clave $k^*_{L,\mathrm{dec}}$.

(S303: Paso de generación de vector de aleatorización $k^*_{L,\mathrm{ran},j}$)

En base a la clave pública maestra pk, la clave secreta maestra sk y los vectores de predicado ($\vec{v}_1$, …, $\vec{v}_L$) mostrados en la Fórmula 163, la unidad de generación de vector de aleatorización 140 calcula la Fórmula 165 para generar el vector de aleatorización $k^*_{L,\mathrm{ran},j}$ (j = 1, …, L+1). El vector de aleatorización $k^*_{L,\mathrm{ran},j}$ (j = 1, …, L+1) es un vector, en una clave de nivel más bajo, para distribuir uniformemente el coeficiente de un vector de base en el que se incrusta cada uno de los vectores de predicado. El vector de aleatorización $k^*_{L,\mathrm{ran},j}$ es el elemento de orden j de la clave secreta de nivel de orden L.

[Fórmula 165]

(1)

$$\sigma_{j,i},\eta_j \xleftarrow{U} \mathbb{F}_q \qquad (j=1,\ldots,L+1;\ i=1,\ldots,L)$$

(2)

$$vv_j := \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) \qquad (j=1,\ldots,L+1)$$

(3)

$$dv_j := \eta_j b^*_{n+1} - \eta_j b^*_{n+2} \qquad (j=1,\ldots,L+1)$$

(4)

$$\begin{aligned} k^*_{L,\mathrm{ran},j} &:= vv_j + dv_j \\ &:= \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \eta_j b^*_{n+1} - \eta_j b^*_{n+2} \\ &\qquad (j=1,\ldots,L+1) \end{aligned}$$

Es decir, (1) usando el dispositivo de procesamiento, la unidad de generación de vector de aleatorización 140 genera los números aleatorios $\sigma_{j,i}$ (j = 1, …, L+1; i = 1, …, L) y η_j (j = 1, …, L+1).

(2) Usando el dispositivo de procesamiento, la unidad de generación de vector de aleatorización 140 genera un vector vv_j, para cada j de j = 1, …, L+1, fijando cada uno de los vectores de predicado aleatorizados mediante el número aleatorio $\sigma_{j,t}$ como el coeficiente del vector de base b^*_i (i = 1, …, μ_L). Es decir, cada uno de los vectores de predicado se incrusta en el coeficiente del vector de base b^*_i (i = 1, …, μ_L).

(3) Usando el dispositivo de procesamiento, la unidad de generación de vector de aleatorización 140 genera un vector dv_j, para cada j de j = 1, …, L+1, fijando el número aleatorio η_j como el coeficiente del vector de base b^*_{n+1} y fijando un valor obtenido restando el número aleatorio η_j de 0 (- η_j) como el coeficiente del vector de base b^*_{n+2}. Es decir, los coeficientes de los vectores de base b^*_{n+1} y b^*_{n+2} se fijan de manera que la suma de los coeficientes de los vectores de base b^*_{n+1} y b^*_{n+2} es 0.

(4) La unidad de generación de vector de aleatorización 140 genera el vector de aleatorización $k^*_{L,ran,j}$ (j = 1, …, L+1), para cada j de j = 1, …, L+1, sumando los vectores generados vv_j y dv_j.

(S304: Paso de generación de vector de generación de clave $k^*_{L,del,j}$)

Usando el dispositivo de procesamiento y en base a la clave pública maestra pk, la clave secreta maestra sk y los vectores de predicado ($\vec{v}_1$, …, $\vec{v}_L$) mostrados en la Fórmula 163, la unidad de generación de vector de generación de clave 150 calcula la Fórmula 166 para generar un vector de generación de clave $k^*_{L,del,j}$ (j = μ_L+1, …, n). El vector de generación de clave $k^*_{L,del,j}$ (j = μ_L+1, …, n) es un vector para generar una clave secreta de nivel más bajo (vector de clave de nivel más bajo). El vector de generación de clave $k^*_{L,del,j}$ es el elemento de orden j de la clave secreta de nivel de orden L.

[Fórmula 166]

(1)

$$\sigma_{j,i},\psi,\eta_j \xleftarrow{U} \mathbb{F}_q \qquad (j=\mu_L+1,\ldots,n;\ i=1,\ldots,L)$$

(2)

$$vv_j := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^* \right) \qquad (j=\mu_L+1,\ldots,n)$$

(3)

$$\psi v_j := \psi b_j^* \qquad (j=\mu_L+1,\ldots,n)$$

(4)

$$dv_j := \eta_j b_{n+1}^* - \eta_j b_{n+2}^* \qquad (j=\mu_L+1,\ldots,n)$$

(5)

$$k^*_{L,\mathrm{del},j} := vv_j + \psi v_j + dv_j$$
$$:= \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^* \right) + \psi b_j^* + \eta_j b_{n+1}^* - \eta_j b_{n+2}^* \qquad (j=\mu_L+1,\ldots,n)$$

Es decir, (1) usando el dispositivo de procesamiento, la unidad de generación de vector de generación de clave 150 genera los números aleatorios $\sigma_{j,i}$ (j = μ_L+1, …, n; i = 1, …, L), ψ y η_j (j = μ_L+1, …, n).

(2) Usando el dispositivo de procesamiento, la unidad de generación de vector de generación de clave 150 genera un vector vv_j, para cada j de j = μ_L+1, …, n, fijando cada uno de los vectores de predicado aleatorizados por el número aleatorio $\sigma_{j,t}$ como el coeficiente del vector de base b^*_i (i = 1, …, μ_L). Es decir, cada uno de los vectores de predicado se incrusta en el coeficiente del vector de base b^*_i (i = 1, …, μ_L).

(3) Usando el dispositivo de procesamiento, la unidad de generación de vector de generación de clave 150 genera un vector ψv_j, para cada j de j = μ_L+1, …, n, fijando el número aleatorio ψ como el coeficiente del vector de base b^*_j.

(4) Usando el dispositivo de procesamiento, la unidad de generación de vector de generación de clave 150 genera un vector dv_j, para cada j de j = μ_L+1, …, n, fijando el número aleatorio η_j como el coeficiente del vector de base b^*_{n+1} y fijando un valor obtenido restando el número aleatorio η_j de 0 (- η_j) como el coeficiente del vector de base b^*_{n+2}. Es

decir, los coeficientes de los vectores de base b^*_{n+1} y b^*_{n+2} se fijan de manera que la suma de los coeficientes de los vectores de base b^*_{n+1} y b^*_{n+2} es 0.

(5) La unidad de generación de vector de generación de clave 150 genera el vector de generación de clave $k^*_{L,del,j}$ (j = μ_L+1, …, n), para cada j de j = μ_L+1, …, n, sumando los vectores generados vv_j, ψv_j y dv_j.

Para resumir, en (S302) a (S304), usando el dispositivo de procesamiento, la unidad de generación de vector de clave 130, la unidad de generación de vector de aleatorización 140 y la unidad de generación de vector de generación de clave 150 ejecutan el algoritmo GenKey mostrado en la Fórmula 167. Este genera la clave secreta de nivel de orden L (información de clave $\vec{k}^*_L$) que incluye el vector de clave $k^*_{L,dec}$, el vector de aleatorización $k^*_{L,ran,j}$ (j = 1, …, L+1) y el vector de generación de clave $k^*_{L,del,j}$ (j = μ_L+1, …, n).

[Fórmula 167]

$$\begin{aligned}
&\mathsf{GenKey}\left(\mathsf{pk},\mathsf{sk},\left(\vec{v}_1,\ldots,\vec{v}_L\right)\right) := \left(\left(v_1,\ldots,v_{\mu_1}\right),\ldots,\left(v_{\mu_{L-1}+1},\ldots,v_{\mu_L}\right)\right):\\
&\quad \sigma_{j,i},\psi,\eta_j \xleftarrow{\mathrm{U}} \mathbb{F}_q \ \text{for}\ j=0,\ldots,L+1,\mu_L+1,\ldots,n;\ i=1,\ldots,L\\
&\quad k^*_{L,\mathsf{dec}} := \sum_{t=1}^{L}\sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i\right)+\eta_0 b^*_{n+1}+\left(1-\eta_0\right)b^*_{n+2},\\
&\quad k^*_{L,\mathsf{ran},j} := \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i\right)+\eta_j b^*_{n+1}-\eta_j b^*_{n+2}\\
&\qquad \text{for}\ j=1,\ldots,L+1,\\
&\quad k^*_{L,\mathsf{del},j} := \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i\right)+\psi b^*_j+\eta_j b^*_{n+1}-\eta_j b^*_{n+2}\\
&\qquad \text{for}\ j=\mu_L+1,\ldots,n,\\
&\text{devolver}\ \vec{k}^*_L := \left(k^*_{L,\mathsf{dec}},k^*_{L,\mathsf{ran},1},\ldots,k^*_{L,\mathsf{ran},L+1},k^*_{L,\mathsf{del},\mu_L+1},\ldots,k^*_{L,\mathsf{del},n}\right).
\end{aligned}$$

(S305: Paso de distribución de clave)

La unidad de distribución de clave 160 transmite la clave pública maestra generada por la unidad de generación de clave maestra 110 y la información de clave $\vec{k}^*_L$ generada por la unidad de generación de vector de clave 130, la unidad de generación de vector de aleatorización 140 y la unidad de vector de generación de clave 150 al dispositivo de descifrado 300 a través del dispositivo de comunicación. La unidad de distribución de clave 160 también transmite la clave pública maestra al dispositivo de cifrado 200 a través del dispositivo de comunicación. La información de clave $\vec{k}^*_L$ se transmite en secreto al dispositivo de descifrado 300. Cualquier método se puede usar para transmitir en secreto la información de clave $\vec{k}^*_L$ al dispositivo de descifrado 300. Por ejemplo, la información de clave $\vec{k}^*_1$ se puede transmitir usando un proceso criptográfico de la técnica anterior.

Se describirán las funciones y operaciones del dispositivo de cifrado 200. El dispositivo de cifrado 200 incluye una unidad de ajuste de información de transmisión 210, una unidad de generación de vector de cifrado 220, una unidad de generación de información de cifrado 230, una unidad de transmisión de datos 240 y una unidad de adquisición de clave pública 250.

Se supone que la unidad de adquisición de clave pública 250 ha obtenido la clave pública maestra y los vectores de información de atributo que corresponden a los vectores de información de predicado del dispositivo de descifrado 300 antes de los pasos que se describen más adelante.

(S401: Paso de ajuste de información de transmisión)

Usando el dispositivo de procesamiento y en base a la clave pública maestra pk, la unidad de ajuste de información de transmisión 210 calcula la Fórmula 168 para generar un vector de información de transmisión ςv.

[Fórmula 168]

(1)

$$\zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q$$

(2)

$$\zeta v := \zeta d_{n+1}$$

Es decir, (1) usando el dispositivo de procesamiento, la unidad de ajuste de información de transmisión 210 genera un número aleatorio ς.

(2) Usando el dispositivo de procesamiento, la unidad de ajuste de información de transmisión 210 genera el vector de información de transmisión ςv ajustando el número aleatorio ς como el coeficiente del vector de base d_{n+1} en la base B^ incluida en la clave pública maestra pk.

(S402: Paso de generación de vector de cifrado c_1)

Usando el dispositivo de procesamiento y en base a la clave pública maestra pk y los vectores de atributo ($\vec{x}^*_1$, …, $\vec{x}^*_L$) mostrados en la Fórmula 169, la unidad de generación de vector de cifrado 220 calcula la Fórmula 170 para generar un vector de cifrado c_1.

[Fórmula 169]

$$\left(\vec{x}_1,\ldots,\vec{x}_L\right) := \left(\left(x_1,\ldots,x_{\mu_1}\right),\ldots,\left(x_{\mu_{L-1}+1},\ldots,x_{\mu_L}\right)\right)$$

[Fórmula 170]

(1)

$$\left(\vec{x}_{L+1},\ldots,\vec{x}_d\right) := \left(\left(x_{\mu_L+1},\ldots,x_{\mu_{L+1}}\right),\ldots,\left(x_{\mu_{d-1}+1},\ldots,x_{\mu_d}\right)\right)$$

$$\xleftarrow{U} \mathbb{F}_q{}^{\mu_{L+1}-\mu_L} \times \cdots \times \mathbb{F}_q{}^{n-\mu_{d-1}},$$

$$\delta_1,\ldots,\delta_d,\delta_{n+3},\zeta \xleftarrow{U} \mathbb{F}_q$$

(2)

$$xv := \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i\right)$$

(3)

$$rv := \delta_{n+3} b_{n+3}$$

(4)

$$\begin{aligned} c_1 &:= xv + \zeta v + rv \\ &:= \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i\right) + \zeta d_{n+1} + \delta_{n+3} b_{n+3} \end{aligned}$$

Es decir, (1) usando el dispositivo de procesamiento, la unidad de generación de vector de cifrado 220 genera los números aleatorios ($\vec{x}^*_{L+1}$, …, $\vec{x}^*_d$) y δ_i (i = 1, …, d, n+3).

(2) Usando el dispositivo de procesamiento, la unidad de generación de vector de cifrado 220 fija cada uno de los vectores de atributo como el coeficiente del vector de base b_i (i = 1, …, μ_L) de la base B incluida en la clave pública maestra pk. Es decir, cada uno de los vectores de atributo se incrusta en el coeficiente del vector de base b_i (i = 1, …, μ_L). Usando el dispositivo de procesamiento, la unidad de generación de vector de cifrado 220 fija el número aleatorio como el coeficiente del vector de base b_i (i = μ_L +1, …, n). La unidad de generación de vector de cifrado 220 genera de esta manera un vector xv.

(3) Usando el dispositivo de procesamiento, la unidad de generación de vector de cifrado 220 genera un vector rv ajustando el número aleatorio δ_{n+3} como el coeficiente del vector de base b_{n+3} de la base B incluida en la clave pública maestra pk.

(4) Usando el dispositivo de procesamiento, la unidad de generación de vector de cifrado 220 genera el vector de cifrado c_1 añadiendo los vectores generados xv y rv al vector de información de transmisión ςv generado por la unidad de ajuste de información de transmisión 210.

El vector rv se añade para mejorar la seguridad y no es un elemento de requisito.

(S403: Paso de generación de información de cifrado c_2)

Usando el dispositivo de procesamiento y en base a un mensaje m, la unidad de generación de información de cifrado 230 calcula la Fórmula 171 para generar información de cifrado c_2.

[Fórmula 171]

$$c_2 := g_T^{\zeta} m$$

donde

$$g_T = e(a_i, a_i^*) \neq 1.$$

(S404: Paso de transmisión de datos)

La unidad de transmisión de datos 240 transmite el vector de cifrado c_1 generado por la unidad de generación de vector de cifrado 220 y la información de cifrado c_2 generada por la unidad de generación de información de cifrado 230 al dispositivo de descifrado 300 a través del dispositivo de comunicación.

Para resumir, el dispositivo de cifrado 200 ejecuta el algoritmo Enc mostrado en la Fórmula 172 para generar el vector de cifrado c_1 y la información de cifrado c_2.

[Fórmula 172]

$$\begin{aligned}
&\mathsf{Enc}\left(\mathsf{pk}, m \in \mathbb{G}_T, \left(\vec{x}_1, \ldots, \vec{x}_L\right) := \left(\left(x_1, \ldots, x_{\mu_1}\right), \ldots, \left(x_{\mu_{L-1}+1}, \ldots, x_{\mu_L}\right)\right)\right): \\
&\quad \left(\vec{x}_{L+1}, \ldots, \vec{x}_d\right) \xleftarrow{\mathrm{U}} \mathbb{F}_q{}^{\mu_{L+1}-\mu_L} \times \cdots \times \mathbb{F}_q{}^{n-\mu_{d-1}}, \\
&\quad \delta_1, \ldots, \delta_d, \delta_{n+3}, \zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q, \\
&\quad c_1 := \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i\right) + \zeta d_{n+1} + \delta_{n+3} b_{n+3}, \quad c_2 := g_T^{\zeta} m, \\
&\quad \text{devolver} \left(c_1, c_2\right).
\end{aligned}$$

Se describirán las funciones y operaciones del dispositivo de descifrado 300. El dispositivo de descifrado 300 incluye una unidad de entrada de vector 310, una unidad de almacenamiento de vector de clave 320 y una unidad de operación de emparejamiento 330.

(S501: Paso de entrada de vector)

La unidad de entrada de vector 310 recibe a través del dispositivo de comunicación e introduce el vector de cifrado c_1 y la información de cifrado c_2 transmitida por la unidad de transmisión de datos 240 del dispositivo de cifrado 200.

(S502: Paso de descifrado)

Usando el dispositivo de procesamiento y en base a la clave pública maestra pk y el vector de clave $k^*_{L,dec}$ que es el primer elemento de la clave secreta de nivel de orden L, la unidad de operación de emparejamiento 330 calcula la Fórmula 173 para generar el mensaje m'.

[Fórmula 173]

$$m' := c_2 / e\left(c_1, k^*_{L,\mathsf{dec}}\right)$$

Es decir, usando el dispositivo de procesamiento, la unidad de operación de emparejamiento 330 realiza la operación de emparejamiento e sobre el vector de cifrado c_1 introducido por la unidad de entrada de vector 310 y el vector de clave $k^*_{L,dec}$ almacenado en el dispositivo de almacenamiento por la unidad de almacenamiento de vector de clave 320. La unidad de operación de emparejamiento 330 calcula de esta manera g^{ζ}_T. Entonces, dividiendo la información de cifrado c_2 ($=g^{\zeta}_T m$) por el calculado g^{ζ}_T, se calcula el mensaje m' (= m). Cuando el vector de clave $k^*_{L,dec}$ se proporciona por el dispositivo de generación de clave 100 o el dispositivo de delegación de clave 400 de un nivel más alto, la unidad de almacenamiento de vector de clave 320 almacena el vector de clave $k^*_{L,dec}$ en el dispositivo de almacenamiento.

Si L ≤ h se mantiene para el vector de atributo $\vec{x}_i$ (i = 1, …, h) usado por el dispositivo de cifrado 200 para cifrado y el vector de predicado $\vec{v}_i$ (i = 1, …, L) usado por el dispositivo de descifrado 300 para descifrado si $\vec{x}_i \cdot \vec{v}_i = 0$ para todo i (i = 1, …, L), entonces g_t^{ζ} se puede obtener realizando la operación de emparejamiento e sobre el vector de cifrado c_1 y el vector de clave $k^*_{L,dec}$ como se muestra en la Fórmula 174.

[Fórmula 174]

$$e\left(c_1, k^*_{L,\mathsf{dec}}\right) = g_T^{\sum_{1 \le i \le L} \sigma_i \delta_i \vec{x}_i \cdot \vec{v}_i + \zeta} = g_T^{\zeta}$$

Para resumir, el dispositivo de descifrado 300 ejecuta el algoritmo Dec mostrado en la Fórmula 175 para generar el mensaje m'.

[Fórmula 175]

$$\mathsf{Dec}\left(\mathsf{pk}, k^*_{L,\mathsf{dec}}, c_1, c_2\right) : m' := c_2 \Big/ e\left(c_1, k^*_{L,\mathsf{dec}}\right),$$

devolver m'.

Se describirán las funciones y operaciones del dispositivo de delegación de clave 400. El dispositivo de delegación de clave 400 incluye una unidad de adquisición de vector de clave 410 (unidad de adquisición de vector de generación de clave), una unidad de generación de vector de clave 420, una unidad de generación de vector de aleatorización 430, una unidad de generación de vector de generación de clave 440 y una unidad de distribución de clave 450.

(S601: Paso de adquisición de información de clave K^*_L)

La unidad de adquisición de vector de clave 410 obtiene, a través del dispositivo de comunicación, la clave secreta de nivel de orden L (información de clave $\vec{k}^*_L$) que incluye el vector de clave $k^*_{L,dec}$ que es el primer elemento de la clave secreta de nivel de orden L, el vector de aleatorización $k^*_{L,ran,j}$ (j = 1, …, L+1) y el vector de generación de clave $k^*_{L,del,j}$ ($j = \mu_L+1, \ldots, n$).

(S602: Paso de generación de vector de clave $k^*_{L+1,dec}$)

Usando el dispositivo de procesamiento y en base a la clave pública maestra pk, la información de clave $\vec{k}^*_L$, un vector de predicado $\vec{v}^*_{L+1}$ mostrado en la Fórmula 176, la unidad de generación de vector de clave 420 calcula la Fórmula 177 para generar un vector de clave $k^*_{L+1,dec}$ que es el primer elemento de una clave secreta de nivel de orden (L+1).

[Fórmula 176]

$$\vec{v}_{L+1} := \left(v_{\mu_L+1}, \ldots, v_{\mu_{L+1}}\right)$$

[Fórmula 177]

(1)

$$\alpha_{0,i}, \sigma_0 \xleftarrow{\mathrm{U}} \mathbb{F}_q \qquad (i = 1, \ldots, L+1)$$

(2)

$$rv := \sum_{i=1}^{L+1} \alpha_{0,i} k^*_{L,\mathsf{ran},i}$$

(3)

$$vv := \sigma_0 \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathsf{del},i}\right)$$

(4)

$$k^*_{L+1,\mathrm{dec}} := k^*_{L,\mathrm{dec}} + rv + vv$$
$$:= k^*_{L,\mathrm{dec}} + \sum_{i=1}^{L+1} \alpha_{0,i} k^*_{L,\mathrm{ran},i} + \sigma_0 \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i} \right)$$

Es decir, (1) usando el dispositivo de procesamiento, la unidad de generación de vector de clave 420 genera los números aleatorios $\alpha_{0,i}$ (i = 1, …, L+1) y σ_0.

(2) Usando el dispositivo de procesamiento, la unidad de generación de vector de clave 420 genera un vector rv sumando vectores en los cuales el coeficiente del vector de aleatorización $k^*_{L,\mathrm{ran},i}$ se multiplica por el número aleatorio $\alpha_{0,i}$ para cada i de i = 1, …, L+1. Cada uno de los vectores de predicado se incrusta en el coeficiente del vector de base b^*_i (i = 1, …, μ_L) del vector de aleatorización $k^*_{L,\mathrm{ran},i}$ (i = 1, …, L+1). De esta manera, cada uno de los vectores de predicado multiplicado por el número aleatorio se incrusta en el coeficiente del vector de base b^*_i (i = 1, …, μ_L) del vector rv.

(3) Usando el dispositivo de procesamiento, la unidad de generación de vector de clave 420 genera un vector vv sumando vectores en los que cada vector de los vectores de predicado $\vec{v}^*_{L+1}$ se fija como el coeficiente del vector de generación de clave $k^*_{L,\mathrm{del},i}$ (i = μ_L+1, …, μ_{L+1}) y multiplicando la suma por el número aleatorio σ_0. Es decir, cada uno de los vectores de predicado se incrusta en el coeficiente del vector de base b^*_i (i = μ_L+1, …, μ_{L+1}).

(4) Usando el dispositivo de procesamiento, la unidad de generación de vector de clave 420 genera el vector de clave $k^*_{L+1,\mathrm{dec}}$ sumando el vector de clave $k^*_{L,\mathrm{dec}}$, el vector rv y el vector vv.

(S603: Paso de generación de vector de aleatorización $k^*_{L+1,\mathrm{ran},j}$)

En base a la clave pública maestra pk, la información de clave $\vec{k}^*_L$ y el vector de predicado $\vec{v}_{L+1}$ mostrados en la Fórmula 176, la unidad de generación de vector de aleatorización 430 calcula la Fórmula 178 para generar un vector de aleatorización $k^*_{L+1,\mathrm{ran},j}$ (j = 1, …, L+2). El vector de aleatorización $k^*_{L+1,\mathrm{ran},j}$ (j = 1, …, L+2) es un vector, en una clave de nivel más bajo, para distribuir uniformemente el coeficiente de un vector de base en el que se incrusta cada uno de los vectores de predicado. El vector de aleatorización $k^*_{L+1,\mathrm{ran},j}$ es el elemento de orden j de la clave secreta de nivel de orden (L+1).

[Fórmula 178]

(1)

$$\alpha_{j,i}, \sigma_j \xleftarrow{\mathrm{U}} \mathbb{F}_q \qquad (j = 1,\ldots,L+2;\ i = 1,\ldots,L+1)$$

(2)

$$rv_j := \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\mathrm{ran},i} \qquad (j = 1,\ldots,L+2)$$

(3)

$$vv_j := \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i} \right) \qquad (j = 1,\ldots,L+2)$$

(4)

$$k^*_{L+1,\mathrm{ran},j} := rv_j + vv_j$$
$$:= \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\mathrm{ran},i} + \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i} \right)$$
$$(j = 1,\ldots,L+2)$$

Es decir, (1) usando el dispositivo de procesamiento, la unidad de generación de vector de aleatorización 430 genera los números aleatorios $\alpha_{j,i}$ (j = 1, …, L+2; i = 1, …, L) y σ_j (j = 1, …, L+2).

(2) Usando el dispositivo de procesamiento, la unidad de generación de vector de aleatorización 430 genera un vector rv_j, para cada j de j = 1, …, L+2, multiplicando el coeficiente del vector de aleatorización $k^*_{L,\mathrm{ran},j}$ (i = 1, …, L+1) por el número aleatorio $\alpha_{j,i}$ (i = 1, …, L+1). Como se describió anteriormente, cada uno de los vectores de predicado se incrusta en el coeficiente del vector de base b^*_i (i = 1, …, μ_L) del vector de aleatorización $k^*_{L,\mathrm{ran},i}$ (i = 1, …, L+1). De esta manera, cada uno de los vectores de predicado multiplicado por el número aleatorio se incrusta en el coeficiente del vector de base b^*_i (i = 1, …, μ_L) del vector rv_j.

(3) Usando el dispositivo de procesamiento, la unidad de generación de vector de aleatorización 430 genera un vector vv_j, para cada j de j = 1, …, L+2, sumando vectores en los que cada uno de los vectores de predicado se fija como el coeficiente del vector de generación de clave $k^*_{L,del,j}$ ($i = \mu_L+1, \ldots, \mu_{L+1}$) y multiplicando la suma por el número aleatorio σ_j. Es decir, cada uno de los vectores de predicado se incrusta en el coeficiente del vector de base b^*_i ($i = \mu_L+1, \ldots, \mu_{L+1}$).

(4) Usando el dispositivo de procesamiento, la unidad de generación de vector de aleatorización 430 genera el vector aleatorización $k^*_{L+1,ran,j}$ para cada j de j = 1, …, L+2, sumando los vectores generados rv_j y vv_j.

(S604: Paso de generación de vector de generación de clave $k^*_{L+1,del,j}$)

Usando el dispositivo de procesamiento y en base a la clave pública maestra pk, la información de clave $\vec{k}^*_L$ y el vector de predicado $\vec{v}_{L+1}$ mostrado en la Fórmula 176, la unidad de generación de vector de generación de clave 440 calcula la Fórmula 179 para generar un vector de generación de clave $k^*_{L+1,del,j}$ ($j = \mu_{L+1}+1, \ldots, n$). El vector de generación de clave $k^*_{L+1,del,j}$ ($j = \mu_{L+1}+1, \ldots, n$) es un vector para generar una clave secreta de nivel más bajo (vector de clave de nivel más bajo). El vector de generación de clave $k^*_{L+1,del,j}$ es el elemento de orden j de la clave secreta de nivel de orden (L+1).

[Fórmula 179]

(1)

$$\alpha_{j,i}, \sigma_j, \psi' \xleftarrow{U} \mathbb{F}_q \quad (j = \mu_{L+1}+1, \ldots, n;\ i = 1, \ldots, L+1)$$

(2)

$$rv_j := \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\mathrm{ran},i} \qquad (j = \mu_{L+1}+1, \ldots, n)$$

(3)

$$vv_j := \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i} \right) \qquad (j = \mu_{L+1}+1, \ldots, n)$$

(4)

$$\psi v_j := \psi' k^*_{L,\mathrm{del},j} \qquad (j = \mu_{L+1}+1, \ldots, n)$$

(5)

$$\begin{aligned} k^*_{L+1,\mathrm{del},j} &:= rv_j + vv_j + \psi v_j \\ &:= \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\mathrm{ran},i} + \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i} \right) + \psi' k^*_{L,\mathrm{del},j} \\ &\qquad (j = \mu_{L+1}+1, \ldots, n) \end{aligned}$$

Es decir, (1) usando el dispositivo de procesamiento, la unidad de generación de vector de generación de clave 440 genera los números aleatorios $\alpha_{j,i}$ ($j = \mu_{L+1}+1, \ldots, n$; $i = 1, \ldots, L+1$), σ_j ($j = \mu_{L+1}+1, \ldots, n$) y ψ'.

(2) Usando el dispositivo de procesamiento, la unidad de generación de vector de generación de clave 440 genera un vector rv_j, para cada j de $j = \mu_{L+1}+1, \ldots, n$, multiplicando el coeficiente del vector de aleatorización $k^*_{L,ran,i}$ ($i = 1, \ldots, L+1$) por el número aleatorio $\alpha_{j,i}$. Como se describió anteriormente, cada uno de los vectores de predicado se incrusta en el coeficiente del vector de base b^*_i ($i = 1, \ldots, \mu_L$) del vector de aleatorización $k^*_{L,ran,i}$ ($i = 1, \ldots, L+1$. De esta manera, cada uno de los vectores de predicado multiplicado por el número aleatorio se incrusta en el coeficiente del vector de base b^*_i ($i = 1, \ldots, \mu_L$) del vector rv_j.

(3) Usando el dispositivo de procesamiento, la unidad de generación de vector de generación de clave 440 genera un vector vv_j, para cada j de $j = \mu_{L+1}+1, \ldots, n$, sumando los vectores en los que cada uno de los vectores de predicado se fija como el coeficiente del vector de generación de clave $k^*_{L,del,i}$ ($i = \mu_L+1, \ldots, \mu_{L+1}$) y multiplicando la suma por el número aleatorio σ_j. Es decir, cada uno de los vectores de predicado se incrusta en el coeficiente del vector de base b^*_i ($i = \mu_L+1, \ldots, \mu_{L+1}$).

(4) Usando el dispositivo de procesamiento, la unidad de generación de vector de generación de clave 440 genera un vector ψv_j, para cada j de $j = \mu_{L+1}+1, \ldots, n$, multiplicando el coeficiente del vector de generación de clave $k^*_{L,del,i}$ por el número aleatorio ψ'. Cada uno de los vectores predicado se incrusta en el coeficiente del vector de base b^*_j (j

= μ_{L+1}+1, …, n) del vector de generación de clave $k^*_{L,del,j}$. De esta manera, cada uno de los vectores de predicado multiplicado por el número aleatorio se incrusta en el coeficiente del vector de base b^*_j del vector ψv_j (j = μ_{L+1}+1, …, n).

(5) Usando el dispositivo de procesamiento, la unidad de generación de vector de generación de clave 440 genera un vector de generación de clave $k^*_{L+1,del,j}$ (j = μ_{L+1}+1, …, n), para cada j de j = μ_{L+1}+1, …, n, sumando los vectores generados rv_j, vv_j y ψv_j.

Para resumir, en (S602) a (S604), usando el dispositivo de procesamiento, la unidad de generación de vector de clave 420, la unidad de generación de vector de aleatorización 430 y la unidad de generación de vector de generación de clave 440 ejecutan el algoritmo $Delegate_L$ mostrado en la Fórmula 180 para generar la clave secreta de nivel de orden (L+1) (información de clave $\vec{k}^*_{L+1}$) que incluye el vector de clave $k^*_{L+1,dec}$, el vector de aleatorización $k^*_{L+1,ran,j}$ (j = 1, …, L+2) y el vector de generación de clave $k^*_{L+1,del,j}$ (j = μ_{L+1}+1, …, n).

[Fórmula 180]

$$\mathsf{Delegate}_L\left(\mathsf{pk}, \vec{k}^*_L, \vec{v}_{L+1} := \left(v_{\mu_L+1}, \ldots, v_{\mu_{L+1}}\right)\right):$$

$$\alpha_{j,i}, \sigma_j, \psi' \xleftarrow{U} \mathbb{F}_q \quad \text{for } j = 0, \ldots, L+2, \mu_{L+1}+1, \ldots, n;\ i = 1, \ldots, L+1,$$

$$k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + \sum_{i=1}^{L+1} \alpha_{0,i} k^*_{L,\mathsf{ran},i} + \sigma_0 \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathsf{del},i}\right),$$

$$k^*_{L+1,\mathsf{ran},j} := \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\mathsf{ran},i} + \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathsf{del},i}\right)$$

$$\text{for } j = 0, \ldots, L+2,$$

$$k^*_{L+1,\mathsf{del},j} := \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\mathsf{ran},i} + \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathsf{del},i}\right) + \psi' k^*_{L,\mathsf{del},j}$$

$$\text{for } j = \mu_{L+1}+1, \ldots, n,$$

$$\text{devolver } \vec{k}^*_{L+1} := \begin{pmatrix} k^*_{L+1,\mathsf{dec}}, k^*_{L+1,\mathsf{ran},1}, \ldots, k^*_{L+1,\mathsf{ran},L+2}, \\ k^*_{L+1,\mathsf{del},\mu_{L+1}+1}, \ldots k^*_{L+1,\mathsf{del},n} \end{pmatrix}.$$

(S605: Paso de distribución de clave)

La unidad de distribución de clave 440 transmite la información de clave $\vec{k}^*_{L+1}$ generada por la unidad de generación de vector de clave 420, la unidad de generación de vector de aleatorización 430 y la unidad de generación de vector de generación de clave 440 al dispositivo de descifrado 300 de un nivel más bajo a través del dispositivo de comunicación. La información de clave $\vec{k}^*_{L+1}$ se transmite en secreto al dispositivo de descifrado 300. Cualquier método se puede usar para transmitir en secreto la información de clave $\vec{k}^*_{L+1}$ al dispositivo de descifrado 300. Por ejemplo, la información de clave $\vec{k}^*_{L+1}$ se puede transmitir usando un proceso criptográfico de la técnica anterior.

Como se describió anteriormente, los procesos criptográficos que se implementan por el sistema de procesamiento criptográfico 10 tienen una seguridad más alta que los procesos criptográficos propuestos en la Literatura no de Patente 18 y se puede dar una prueba de seguridad en un modelo estándar.

Esto es principalmente debido a las dos características (1) y (2) siguientes.

(1) El vector de base d_{n+1} en el que el dispositivo de cifrado 200 fija información de transmisión es bidimensional (vectores de base b_{n+1} y b_{n+2}). Debido a esta característica, se pueden seleccionar aleatoriamente los coeficientes de los vectores de base b^*_{n+1} y b^*_{n+2} del vector de clave $k^*_{L,dec}$ que corresponde al vector de base d_{n+1}. Solamente se publica el vector de base d_{n+1} y los vectores de base b_{n+1} y b_{n+2} se mantienen secretos.

(2) El dispositivo de delegación de clave 400 genera una clave de nivel más bajo usando un vector de aleatorización. Debido a esta característica, se puede aleatorizar el coeficiente de un vector de base predeterminado de la clave de nivel más bajo. Como resultado, no se compromete la seguridad de una clave generando su clave de nivel más bajo.

Cuando el vector de aleatorización no se usa, se construyen dos vectores de clave de nivel más bajo $k^*_{L+1,dec}$ (A) y $k^*_{L+1,dec}$ (B) generados a partir de la información de clave $\vec{k}^*_L$ como se muestra en la Fórmula 181.

[Fórmula 181]

$$k^*_{L+1,\mathrm{dec}}(\mathrm{A}) := k^*_{L,\mathrm{dec}} + \sigma_A\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i}\right)$$
$$:= \sum_{t=1}^{L} \sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i\right) + \sigma_A\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i}\right)$$
$$+ \eta_0 b^*_{n+1} + (1-\eta_0) b^*_{n+2}$$

$$k^*_{L+1,\mathrm{dec}}(\mathrm{B}) := k^*_{L,\mathrm{dec}} + \sigma_B\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i}\right)$$
$$:= \sum_{t=1}^{L} \sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i\right) + \sigma_B\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i}\right)$$
$$+ \eta_0 b^*_{n+1} + (1-\eta_0) b^*_{n+2}$$

Es decir, cuando no se usa el vector de aleatorización, el coeficiente del vector de base b^*_i ($i = 1, \ldots, \mu_L$) incluido en el vector de clave $k^*_{L,\mathrm{dec}}$ y en el que se incrusta información de predicado es el mismo entre los vectores de clave $k^*_{L+1,\mathrm{dec}}$ (A) y $k^*_{L+1,\mathrm{dec}}$ (B).

No obstante, cuando se usa el vector de aleatorización, se construyen los dos vectores de clave de nivel más bajo $k^*_{L+1,\mathrm{dec}}$ (A) y $k^*_{L+1,\mathrm{dec}}$ (B) generados a partir de la información de clave $\vec{k}^*_L$ como se muestra en la Fórmula 182.

[Fórmula 182]

$$k^*_{L+1,\mathrm{dec}}(\mathrm{A}) := k^*_{L,\mathrm{dec}} + \sum_{i=1}^{L+1} \alpha_{A,i} k^*_{L,\mathrm{ran},i} + \sigma_A\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i}\right)$$
$$:= \sum_{t=1}^{L} \sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i\right) + \sum_{i=1}^{L+1} \alpha_{A,i} k^*_{L,\mathrm{ran},i}$$
$$+ \sigma_A\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i}\right) + \eta_0 b^*_{n+1} + (1-\eta_0) b^*_{n+2}$$

$$k^*_{L+1,\mathrm{dec}}(\mathrm{B}) := k^*_{L,\mathrm{dec}} + \sum_{i=1}^{L+1} \alpha_{B,i} k^*_{L,\mathrm{ran},i} + \sigma_B\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i}\right)$$
$$:= \sum_{t=1}^{L} \sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i\right) + \sum_{i=1}^{L+1} \alpha_{A,i} k^*_{L,\mathrm{ran},i}$$
$$+ \sigma_B\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i}\right) + \eta_0 b^*_{n+1} + (1-\eta_0) b^*_{n+2}$$

Es decir, cuando se usa el vector de aleatorización, el vector de aleatorización $k^*_{L,\mathrm{ran},j}$ en el que el coeficiente se distribuye uniformemente mediante el número aleatorio $\alpha_{A,j}$ se añade al vector de clave $k^*_{L+1,\mathrm{dec}}$ (A). El vector de aleatorización $k^*_{L,\mathrm{ran},j}$ en el que el coeficiente se distribuye uniformemente mediante el número aleatorio $\alpha_{B,j}$ se añade al vector de clave $k^*_{L+1,\mathrm{dec}}$ (B). El vector de aleatorización $k^*_{L,\mathrm{ran},j}$ incluye el vector de base b^*_i ($i = 1, \ldots, \mu_L$). De esta manera, en los vectores de clave $k^*_{L+1,\mathrm{dec}}$ (A) y $k^*_{L+1,\mathrm{dec}}$ (B), el coeficiente del vector de base b^*_i ($i = 1, \ldots, \mu_L$) se distribuye uniformemente. Es decir, el coeficiente del vector de base b^*_i ($i = 1, \ldots, \mu_L$) en el que se fija la información de predicado es diferente entre los vectores de clave $k^*_{L+1,\mathrm{dec}}$ (A) y $k^*_{L+1,\mathrm{dec}}$ (B).

En la descripción anterior, el vector de base d_{n+1} en el que el dispositivo de cifrado 200 fija información de transmisión es bidimensional. No obstante, la dimensión del vector de base d_{n+1} puede ser tridimensional o más alta, es decir, m dimensional (vector de base b_{n+1}, …, vector de base b_{n+m}).

En este caso, en (S301), la unidad de generación de clave maestra 110 opera con N = n+m+1. En el paso de generación de vector de clave $k^*_{L,\mathrm{dec}}$ (S302), la unidad de generación de vector de clave 130 fija los coeficientes de los vectores de base b_{n+1}, … y b_{n+m} de manera que la suma de los coeficientes de los vectores de base b_{n+1}, … y b_{n+m} es 1. En el paso de generación de vector de aleatorización $k^*_{L,\mathrm{ran},j}$ (S303), la unidad de generación de vector de aleatorización 140 fija los coeficientes de los vectores de base b_{n+1}, … y b_{n+m} de manera que la suma de los coeficientes de los vectores de base b_{n+1}, … y b_{n+m} es 0. Del mismo modo, en el paso de generación de vector de generación de clave $k^*_{L,\mathrm{del},j}$ (S304), la unidad de generación de vector de generación de clave 150 fija los coeficientes de los vectores de base b_{n+1}, … y b_{n+m} de manera que la suma de los coeficientes de los vectores de base b_{n+1}, … y b_{n+m} es 0. En el paso de generación de vector de cifrado c_1 (S402), la unidad de generación de vector de cifrado 220 genera el vector rv ajustando un número aleatorio como el coeficiente del vector de base b_{n+m+1}.

En la descripción anterior, los procesos criptográficos se implementan en los espacios de vectores N(= n+3) dimensionales. Para los procesos criptográficos sin delegación, n es un entero de 1 o mayor. Por consiguiente, N es un entero de 4 o mayor. Para los procesos criptográficos con delegación, n es un entero de 2 o mayor. Por consiguiente, N es un entero de 5 o mayor. Como se describió anteriormente, en (S402), no es esencial que el dispositivo de cifrado 200 genere el vector rv usando el vector de base b_{n+3}. Cuando el vector rv no se genera, los procesos criptográficos se pueden implementar en espacios de vectores N(= n+2) dimensionales. De esta manera, para los procesos criptográficos sin delegación, N es un entero de 3 o mayor. Para los procesos criptográficos con delegación, N es un entero de 4 o mayor.

En los procesos criptográficos descritos anteriormente, no se usan los mapas de distorsión que se han descrito como una de las condiciones de DPVS. Los mapas de distorsión se usan no en los algoritmos para implementar los procesos criptográficos, sino para proporcionar la seguridad de los procesos criptográficos. De esta manera, los procesos criptográficos descritos anteriormente se pueden establecer en espacios sin mapas de distorsión. Es decir, no es esencial que existan mapas de distorsión en espacios para implementar los procesos criptográficos descritos anteriormente. Lo mismo aplica a los procesos criptográficos que se describen más adelante.

El esquema HPE se ha descrito anteriormente. El esquema HPKEM se describirá ahora. Solamente se describirá las partes del esquema HPKEM que son diferentes del esquema HPE anterior.

La Fig. 17 es un diagrama de bloques funcional que muestra funciones del sistema de procesamiento criptográfico 10 que implementa el esquema HPKEM.

Los pasos de procesamiento del dispositivo de generación de clave 100 y los pasos de procesamiento del dispositivo de delegación de clave 400 son los mismos que los del esquema HPE descrito anteriormente. De esta manera, solamente se describirán los pasos de procesamiento del dispositivo de cifrado 200 y los pasos de procesamiento del dispositivo de descifrado 300.

La Fig. 18 es un diagrama de flujo que muestra operaciones del dispositivo de cifrado 200. La Fig. 19 es un diagrama de flujo que muestra operaciones del dispositivo de descifrado 300.

Se describirán las funciones y operaciones del dispositivo de cifrado 200.

El dispositivo de cifrado 200 mostrado en la Fig. 17 incluye una unidad de generación de clave de sesión 260, además de las funciones incluidas en el dispositivo de cifrado 200 mostrado en la Fig. 11. El dispositivo de cifrado 200 mostrado en la Fig. 17 no incluye la unidad de generación de información de cifrado 230 incluida en el dispositivo de cifrado 200 mostrado en la Fig. 11.

(S701) y (S702) son los mismos que (S401) y (S402).

En (S703: paso de transmisión de datos), el vector de cifrado c_1 generado por la unidad de generación de vector de cifrado 220 en (S702) se transmite al dispositivo de descifrado 300 a través del dispositivo de comunicación. Es decir, en el esquema HPKEM, no se genera la información de cifrado c_2 en la que se incrusta un mensaje m y no se transmite al dispositivo de descifrado 300.

En (S704: paso de generación de clave de sesión), usando el dispositivo de procesamiento, la unidad de generación de clave de sesión 260 calcula la Fórmula 183 para generar una clave de sesión K.

[Fórmula 183]

$$K := g_T^{\zeta}$$

donde

$$g_T = e(a_i, a_i^*) \neq 1.$$

Para resumir, el dispositivo de cifrado 200 ejecuta el algoritmo Enc mostrado en la Fórmula 184 para generar el vector de cifrado c_1 y la clave de sesión K.

[Fórmula 184]

$$\mathsf{Enc}\left(\mathsf{pk},\left(\vec{x}_1,\ldots,\vec{x}_L\right)\right) := \left(\left(x_1,\ldots,x_{\mu_1}\right),\ldots,\left(x_{\mu_{L-1}+1},\ldots,x_{\mu_L}\right)\right):$$

$$\left(\vec{x}_{L+1},\ldots,\vec{x}_d\right) \xleftarrow{\mathrm{U}} \mathbb{F}_q{}^{\mu_{L+1}-\mu_L} \times \cdots \times \mathbb{F}_q{}^{n-\mu_{d-1}},$$

$$\delta_1,\ldots,\delta_d,\delta_{n+3},\zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q,$$

$$c_1 := \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i\right) + \zeta d_{n+1} + \delta_{n+3} b_{n+3}, \quad K := g_T^{\zeta},$$

$$\text{devolver } \left(c_1, K\right).$$

Se describirán las funciones y operaciones del dispositivo de descifrado 300.

La configuración de las funciones del dispositivo de descifrado 300 mostrado en la Fig. 17 es la misma que la del dispositivo de descifrado 300 mostrado en la Fig. 11.

(S801: Paso de entrada de vector)

La unidad de entrada de vector 310 recibe a través del dispositivo de comunicación e introduce el vector de cifrado c_1 transmitido por la unidad de transmisión de datos 240 del dispositivo de cifrado 200.

(S802: Paso de descifrado)

Usando el dispositivo de procesamiento y en base a la clave pública maestra pk y el vector de clave $k^*_{L,dec}$ que es el primer elemento de la clave secreta de nivel de orden L, la unidad de operación de emparejamiento 330 calcula la Fórmula 185 para generar una clave de sesión K.

[Fórmula 185]

$$K' := e\left(c_1, k^*_{L,\mathsf{dec}}\right)$$

Es decir, usando el dispositivo de procesamiento, la unidad de operación de emparejamiento 330 realiza la operación de emparejamiento e sobre el vector de cifrado c_1 introducido por la unidad de entrada de vector 310 y el vector de clave $k^*_{L,dec}$ almacenado en el dispositivo de almacenamiento por la unidad de almacenamiento de vector 320. La unidad de operación de emparejamiento 330 de esta manera calcula g^{ς}_T (= K) que es un valor que concierne a ς incrustado por el dispositivo de cifrado 200.

Para resumir, el dispositivo de descifrado 300 ejecuta el algoritmo Dec mostrado en la Fórmula 186 para generar la clave de sesión K' (= K).

[Fórmula 186]

$$\mathsf{Dec}\left(\mathsf{pk}, k^*_{L,\mathsf{dec}}, c_1\right): K' := e\left(c_1, k^*_{L,\mathsf{dec}}\right),$$

$$\text{devolver } K'.$$

Como se describió anteriormente, según el esquema HPKEM, la clave de sesión K se puede transmitir en secreto desde el dispositivo de cifrado 200 al dispositivo de descifrado 300. Esto significa que la clave de sesión se puede compartir entre el dispositivo de cifrado 200 y el dispositivo de descifrado 300.

Tercera realización

En una tercera realización, se describirá un esquema PE con delegación que es más genérico que los esquemas HPE y HPKEM descritos en la segunda realización.

Como se describió anteriormente, en los esquemas HPE y HPKEM descritos en la segunda realización, los vectores de base se usan como se muestra en la Fig. 16. Es decir, el número de vectores de base de entre el número (n+3) de vectores de base se usan para representar la estructura jerárquica de los vectores de base para vectores de atributo y vectores de predicado. En particular, un primer número μ_1 de vectores de base se usan como los vectores de base para los vectores de atributo y vectores de predicado de primer nivel. Un número (μ_2-μ_1) de vectores de base se usan como los vectores de base para los vectores de atributo y vectores de predicado de segundo nivel. Del mismo modo, un número (μ_L-μ_{L-1}) de vectores de base se usan como los vectores de base para los vectores de atributo y vectores de predicado de nivel de orden L.

El vector de clave de nivel de orden L $k^*_{L,dec}$ se calcula como se muestra en la Fórmula 164. Es decir, en el vector de clave de nivel de orden L $k^*_{L,dec}$, cada uno de los vectores de predicado se asigna como el coeficiente del vector de base b^*_i (i = 1, …, L) y 0 se asigna como el coeficiente del vector de base b^*_i (i = L+1, …, n).

El vector de cifrado de nivel de orden L c_1 se calcula como se muestra en la Fórmula 170. Es decir, en el vector de cifrado de nivel de orden L c_1 cada uno de los vectores de atributo se asigna como el coeficiente del vector de base b_i (i = 1, …, L) y el número aleatorio se asigna como el coeficiente del vector de base b_i (i = L+1, …, n).

Con esta disposición, se implementa la delegación jerárquica.

En el esquema PE (PKEM) que se describe en la tercera realización, como en la segunda realización, el número n de los vectores de base de entre el número (n+3) de vectores de base se usan como los vectores de base para vectores de atributo y vectores de predicado. No obstante, para cualquier clave (con independencia del nivel), todos del número n de vectores de base se usan como los vectores de base para vectores de predicado. Es decir, todos del número n de vectores de base se usan siempre como los vectores de base para vectores de atributo y vectores de predicado.

En el vector de clave $k^*_{L,dec}$, cada uno de los vectores de predicado se asigna como el coeficiente del vector de base b^*_i (i = 1, …, n). En el vector de cifrado de nivel de orden L c_1, cada uno de los vectores de atributo se asigna como el coeficiente del vector de base b_i (i = 1, …, n).

Es decir, no hay concepto de estructura jerárquica para el número n de vectores de base. Tampoco hay un concepto de delegación jerárquica para claves secretas. Por lo tanto, se puede realizar una delegación más flexible, comparado con los procesos criptográficos descritos en la segunda realización.

En primer lugar, se describirá la implementación del esquema PE con delegación.

La Fig. 20 es un diagrama de bloques funcional que muestra funciones del sistema de procesamiento criptográfico 10 que implementa el esquema PE con delegación. Las funciones incluidas en el sistema de procesamiento criptográfico 10 mostrado en la Fig. 20 son las mismas que las funciones incluidas en el sistema de procesamiento criptográfico 10 mostrado en la Fig. 11.

El flujo de operaciones del sistema de procesamiento criptográfico 10 para implementar el esquema PE con delegación según la tercera realización son las mismas que el flujo de operaciones del sistema de procesamiento criptográfico 10 según la segunda realización. De esta manera, las funciones y operaciones del sistema de procesamiento criptográfico 10 según la tercera realización se describirán con referencia a las Fig. 20 y 12 a 16.

Se describirán las funciones y operaciones del dispositivo de generación de clave 100.

(S301: Paso de generación de clave maestra)

Como en (S301) de la segunda realización, usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 calcula la Fórmula 187 para generar una clave pública maestra pk y una clave secreta maestra sk y almacena las claves en la unidad de almacenamiento de clave maestra 120.

[Fórmula 187]

$$\mathsf{Setup}\left(1^\lambda, \vec{\mu} := n\right) : \left(\mathsf{param}, \mathbb{B}, \mathbb{B}^*\right) \xleftarrow{\mathrm{R}} \mathcal{G}_{\mathsf{ob}}\left(1^\lambda, n+3\right),$$
$$d_{n+1} := b_{n+1} + b_{n+2}, \quad \hat{\mathbb{B}} := \left(b_1, \ldots, b_n, d_{n+1}, b_{n+3}\right),$$
$$\text{devolver } \mathsf{sk} := \left(X, \mathbb{B}^*\right), \ \mathsf{pk} := \left(1^\lambda, \mathsf{param}, \hat{\mathbb{B}}\right).$$

donde

$$\mathcal{G}_{\mathsf{ob}}\left(1^\lambda, N\right) : \mathsf{param} := \left(q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*\right) \xleftarrow{\mathrm{R}} \mathcal{G}_{\mathsf{dpvs}}\left(1^\lambda, N\right),$$
$$X := \left(\chi_{i,j}\right) \xleftarrow{\mathrm{U}} GL\left(N, \mathbb{F}_q\right), \ \left(\upsilon_{i,j}\right) := \left(X^{\mathrm{T}}\right)^{-1},$$
$$b_i = \sum_{j=1}^{N} \chi_{i,j} a_j, \ \mathbb{B} := \left(b_1, \ldots, b_N\right),$$
$$b_i^* = \sum_{j=1}^{N} \upsilon_{i,j} a_j^*, \ \mathbb{B}^* := \left(b_1^*, \ldots, b_N^*\right),$$
$$\text{devolver } \left(\mathsf{param}, \mathbb{B}, \mathbb{B}^*\right)$$

(S302: Paso de generación de vector de clave $k^*_{L,dec}$)

Usando el dispositivo de procesamiento y en base a la clave publica maestra pk, la clave secreta maestra sk y los vectores de predicado ($\vec{v}_1$, …, $\vec{v}_L$) mostrados en la Fórmula 188, la unidad de generación de vector de clave 130 calcula la Fórmula 189 para generar un vector de clave $k^*_{L,dec}$ que es el primer elemento de una clave secreta de nivel de orden L (nivel L).

[Fórmula 188]

$$(\vec{v}_1,\ldots,\vec{v}_L) := \left(\left(v_{1,1},\ldots,v_{1,n}\right),\ldots,\left(v_{L,1},\ldots,v_{L,n}\right)\right)$$

[Fórmula 189]

(1)

$$\sigma_{\mathrm{dec},t},\eta_{\mathrm{dec}} \xleftarrow{\mathrm{U}} \mathbb{F}_q \qquad (t=1,\ldots,L)$$

(2)

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L}\sigma_{\mathrm{dec},t}\left(\sum_{i=1}^{n} v_{t,i}b_i^*\right)+\eta_{\mathrm{dec}}b^*_{n+1}+(1-\eta_{\mathrm{dec}})b^*_{n+2}$$

(S303: Paso de generación de vector de aleatorización $k^*_{L,ran,j}$)

En base a la clave pública maestra pk, la clave secreta maestra sk y los vectores de predicado ($\vec{v}_1$, …, $\vec{v}_L$) mostrados en la Fórmula 188, la unidad de generación de vector de aleatorización 140 calcula la Fórmula 190 para generar el vector de aleatorización $k^*_{L,ran,j}$ (j = 1, …, L+1).

[Fórmula 190]

(1)

$$\sigma_{\mathrm{ran},j,t},\eta_{\mathrm{ran},j} \xleftarrow{\mathrm{U}} \mathbb{F}_q \qquad (j=1,\ldots,L+1;t=1,\ldots,L)$$

(2)

$$vv_j := \sum_{t=1}^{L}\sigma_{\mathrm{ran},j,t}\left(\sum_{i=1}^{n} v_{t,i}b_i^*\right) \qquad (j=1,\ldots,L+1)$$

(3)

$$dv_j := \eta_{\mathrm{ran},j}b^*_{n+1}-\eta_{\mathrm{ran},j}b^*_{n+2} \qquad (j=1,\ldots,L+1)$$

(4)

$$\begin{aligned} k^*_{L,\mathrm{ran},j} &:= vv_j + dv_j \\ &:= \sum_{t=1}^{L}\sigma_{\mathrm{ran},j,t}\left(\sum_{i=1}^{n} v_{t,i}b_i^*\right)+\eta_{\mathrm{ran},j}b^*_{n+1}-\eta_{\mathrm{ran},j}b^*_{n+2} \\ &\qquad (j=1,\ldots,L+1) \end{aligned}$$

(S304: Paso de generación de vector de generación de clave $k^*_{L,del,j}$)

Usando el dispositivo de procesamiento y en base a la clave publica maestra pk, la clave secreta maestra sk y los vectores de predicado ($\vec{v}_1$, …, $\vec{v}_L$) mostrados en la Fórmula 188, la unidad de generación de vector de generación de clave 150 calcula la Fórmula 191 para generar un vector de generación de clave $k^*_{L,del,j}$ (j = 1, …, n).

[Fórmula 191]

(1)

$$\sigma_{\mathsf{del},j,t},\eta_{\mathsf{del},j},\psi \xleftarrow{\mathrm{U}} \mathbb{F}_q \qquad (j=1,\ldots,n;\ t=1,\ldots,L)$$

(2)

$$vv_j := \sum_{t=1}^{L} \sigma_{\mathsf{del},j,t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) \qquad (j=1,\ldots,n)$$

(3)

$$\psi v_j := \psi b_j^* \qquad (j=1,\ldots,n)$$

(4)

$$dv_j := \eta_{\mathsf{del},j} b_{n+1}^* - \eta_{\mathsf{del},j} b_{n+2}^* \qquad (j=1,\ldots,n)$$

(5)

$$\begin{aligned} k_{L,\mathsf{del},j}^* &:= vv_j + \psi v_j + dv_j \\ &:= \sum_{t=1}^{L} \sigma_{\mathsf{del},j,t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) + \psi b_j^* + \eta_{\mathsf{del},j} b_{n+1}^* - \eta_{\mathsf{del},j} b_{n+2}^* \\ &\qquad (j=1,\ldots,n) \end{aligned}$$

Para resumir, en (S302) a (S304), usando el dispositivo de procesamiento, la unidad de generación de vector de clave 130, la unidad de generación de vector de aleatorización 140 y la unidad de generación de vector de generación de clave 150 ejecutan el algoritmo GenKey mostrado en la Fórmula 192. Este genera la clave secreta de nivel de orden L (información de clave $\vec{k}^*_L$) que incluye el vector de clave $k^*_{L,\mathrm{dec}}$, el vector de aleatorización $k^*_{L,\mathrm{ran},j}$ (j = 1, …, L+1) y el vector de generación de clave $k^*_{L,\mathrm{del},j}$ (j = 1, …, n).

[Fórmula 192]

$$\begin{aligned} &\mathsf{GenKey}\left(\mathsf{pk},\mathsf{sk},\left(\vec{v}_1,\ldots,\vec{v}_L\right)\right) := \left(\left(v_{1,1},\ldots,v_{1,n}\right),\ldots,\left(v_{L,1},\ldots,v_{L,n}\right)\right): \\ &\quad \sigma_{\mathsf{dec},t},\eta_{\mathsf{dec}},\sigma_{\mathsf{ran},j,t},\eta_{\mathsf{ran},j}\ (j=1,\ldots,L+1), \\ &\quad \sigma_{\mathsf{del},j,t},\eta_{\mathsf{del},j}\ (j=1,\ldots,n),\ \ \psi \xleftarrow{\mathrm{U}} \mathbb{F}_q \\ &\qquad \text{for } t=1,\ldots,L, \\ &\quad k_{L,\mathsf{dec}}^* := \sum_{t=1}^{L} \sigma_{\mathsf{dec},t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) + \eta_{\mathsf{dec}} b_{n+1}^* + (1-\eta_{\mathsf{dec}}) b_{n+2}^*, \\ &\quad k_{L,\mathsf{ran},j}^* := \sum_{t=1}^{L} \sigma_{\mathsf{ran},j,t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) + \eta_{\mathsf{ran},j} b_{n+1}^* - \eta_{\mathsf{ran},j} b_{n+2}^* \\ &\qquad \text{for } j=1,\ldots,L+1, \\ &\quad k_{L,\mathsf{del},j}^* := \sum_{t=1}^{L} \sigma_{\mathsf{del},j,t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) + \psi b_j^* + \eta_{\mathsf{del},j} b_{n+1}^* - \eta_{\mathsf{del},j} b_{n+2}^* \\ &\qquad \text{for } j=1,\ldots,n, \\ &\quad \text{devolver } \vec{k}_L^* := \left(k_{L,\mathsf{dec}}^*, k_{L,\mathsf{ran},1}^*,\ldots,k_{L,\mathsf{ran},L+1}^*, k_{L,\mathsf{del},1}^*,\ldots,k_{L,\mathsf{del},n}^*\right). \end{aligned}$$

(S305: Paso de distribución de clave)

Como en (S305) de la segunda realización, la unidad de distribución de clave 160 transmite la clave pública maestra generada por la unidad de generación de clave maestra 110 y la información de clave $\vec{k}^*_L$ generada por la unidad de generación de vector de clave 130, la unidad de generación de vector de aleatorización 140 y la unidad de generación de vector de generación de clave 150 al dispositivo de descifrado 300 a través del dispositivo de comunicación. La unidad de distribución de clave 160 transmite la clave pública maestra al dispositivo de cifrado 200 a través del dispositivo de comunicación.

Se describirán las funciones y operaciones del dispositivo de cifrado 200.

(S401: Paso de ajuste de información de transmisión)

Como en (S401) de la segunda realización, usando el dispositivo de procesamiento y en base a la clave publica maestra pk, la unidad de ajuste de información de transmisión 210 calcula la Fórmula 193 para generar un vector de información de transmisión ςv.

[Fórmula 193]

(1)

$$\zeta \xleftarrow{U} \mathbb{F}_q$$

(2)

$$\zeta v := \zeta d_{n+1}$$

(S402: Paso de generación de vector de cifrado c_{1j})

Usando el dispositivo de procesamiento y en base a la clave publica maestra pk y los vectores de atributo ($\vec{x}_1$, …, $\vec{x}_L$) mostrados en la Fórmula 194, la unidad de generación de vector de cifrado 220 calcula la Fórmula 195 para generar un vector de cifrado c_1.

[Fórmula 194]

$$\left(\vec{x}_1,\ldots,\vec{x}_L\right) := \left(\left(x_{1,1},\ldots,x_{1,n}\right),\ldots,\left(x_{L,1},\ldots,x_{L,n}\right)\right)$$

[Fórmula 195]

(1)

$$\delta_1,\ldots,\delta_L,\delta_{n+3},\zeta \xleftarrow{U} \mathbb{F}_q$$

(2)

$$xv := \sum_{t=1}^{L} \delta_t \left(\sum_{i=1}^{n} x_{t,i} b_i\right)$$

(3)

$$rv := \delta_{n+3} b_{n+3}$$

(4)

$$c_1 := xv + \zeta v + rv$$
$$:= \sum_{t=1}^{L} \delta_t \left(\sum_{i=1}^{n} x_{t,i} b_i\right) + \zeta d_{n+1} + \delta_{n+3} b_{n+3}$$

(S403: Paso de generación de información de cifrado c_2)

Como en (S403) de la segunda realización, usando el dispositivo de procesamiento y en base a un mensaje m, la unidad de generación de información de cifrado 230 calcula la Fórmula 196 para generar información de cifrado c_2.

[Fórmula 196]

$$c_2 := g_T^{\zeta} m$$

(S404: Paso de transmisión de datos)

Como en (S404) de la segunda realización, la unidad de transmisión de datos 240 transmite el vector de cifrado c_1 generado por la unidad de generación de vector de cifrado 220 y la información de cifrado c_2 generada por la unidad de generación de información de cifrado 230 al dispositivo de descifrado 300 a través del dispositivo de comunicación.

Para resumir, el dispositivo de cifrado 200 ejecuta el algoritmo Enc mostrado en la Fórmula 197 para generar el vector de cifrado c_1 y la información de cifrado c_2.

[Fórmula 197]

$$\mathsf{Enc}\left(\mathsf{pk}, m \in \mathbb{G}_T, \left(\vec{x}_1, \ldots, \vec{x}_L\right) := \left(\left(x_{1,1}, \ldots, x_{1,n}\right), \ldots, \left(x_{L,1}, \ldots, x_{L,n}\right)\right)\right):$$
$$\delta_1, \ldots, \delta_L, \delta_{n+3}, \zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q,$$
$$c_1 := \sum_{t=1}^{L} \delta_t \left(\sum_{i=1}^{n} x_{t,i} b_i\right) + \zeta d_{n+1} + \delta_{n+3} b_{n+3}, \quad c_2 := g_T^{\zeta} m,$$
$$\text{devolver } \left(c_1, c_2\right).$$

Se describirán las funciones y operaciones del dispositivo de descifrado 300.

(S501: Paso de entrada de vector)

Como en (S501) de la segunda realización, la unidad de entrada de vector 310 recibe a través del dispositivo de comunicación e introduce el vector de cifrado c_1 y la información de cifrado c_2 transmitida por la unidad de transmisión de datos 240 del dispositivo de cifrado 200.

(S502: Paso de descifrado)

Como en (S502) de la segunda realización, usando el dispositivo de procesamiento y en base a la clave pública maestra pk y el vector de clave $k^*_{L,dec}$ que es el primer elemento de la clave secreta de nivel de orden L, la unidad de operación de emparejamiento 330 calcula la Fórmula 198 para generar un mensaje m'.

[Fórmula 198]

$$m' := c_2 / e\left(c_1, k^*_{L,\mathsf{dec}}\right)$$

Si $\vec{x}_i \cdot \vec{v}_j = 0$ se mantiene para el vector de atributo $\vec{x}_1$ (i = 1, …, h) usado por el dispositivo de cifrado 200 para cifrado y el vector de predicado $\vec{v}_j$ (j = 1, …, L) del vector de clave usado por el dispositivo de descifrado 300 para descifrado para cada i de (i = 1, …, h) y cada j de (j = 1, …, L), entonces la unidad de operación de emparejamiento 330 puede generar el mensaje m. Se supone que el mensaje $m \in G_T$.

Para resumir, el dispositivo de descifrado 300 ejecuta el algoritmo Dec mostrado en la Fórmula 199 para generar el mensaje m'.

[Fórmula 199]

$$\mathsf{Dec}\left(\mathsf{pk}, k^*_{L,\mathsf{dec}}, c_1, c_2\right): m' := c_2 / e\left(c_1, k^*_{L,\mathsf{dec}}\right),$$
$$\text{devolver } m'.$$

Se describirán las funciones y operaciones del dispositivo de delegación de clave 400.

(S601: Paso de adquisición de información de clave $\vec{k}^*_L$)

Como en (S601) de la segunda realización, la unidad de adquisición de vector de clave 410 obtiene a través del dispositivo de comunicación la clave secreta de nivel de orden L (información de clave $\vec{k}^*_L$) que incluye el vector de clave $k^*_{L,dec}$ que es el primer elemento de la clave secreta de nivel de orden L, el vector de aleatorización $k^*_{L,ran,j}$ (j = 1, …, L+1) y el vector de generación de clave $k^*_{L,del,j}$ (j = 1, …, n).

(S602: Paso de generación de vector de clave $k^*_{L+1,dec}$)

Usando el dispositivo de procesamiento y en base a la clave publica maestra pk, la información de clave $\vec{k}^*_L$ y un vector de predicado $\vec{v}_{L+1}$ mostrados en la Fórmula 200, la unidad de generación de vector de clave 420 calcula la Fórmula 201 para generar un vector de clave $k^*_{L+1,dec}$ que es el primer elemento de una clave secreta de nivel de orden (L+1).

[Fórmula 200]

$$\vec{v}_{L+1} := \left(v_{L+1,1},\ldots,v_{L+1,n}\right)$$

[Fórmula 201]

(1)

$$\alpha_{\mathsf{dec},t},\sigma_{\mathsf{dec}} \xleftarrow{\mathrm{U}} \mathbb{F}_q \qquad \left(t=1,\ldots,L+1\right)$$

(2)

$$rv := \sum_{t=1}^{L+1} \alpha_{\mathsf{dec},t} k^*_{L,\mathsf{ran},t}$$

(3)

$$vv := \sigma_{\mathsf{dec}} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathsf{del},i}\right)$$

(4)

$$\begin{aligned} k^*_{L+1,\mathsf{dec}} &:= k^*_{L,\mathsf{dec}} + rv + vv \\ &:= k^*_{L,\mathsf{dec}} + \sum_{t=1}^{L+1} \alpha_{\mathsf{dec},t} k^*_{L,\mathsf{ran},t} + \sigma_{\mathsf{dec}} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathsf{del},i}\right) \end{aligned}$$

(S603: Paso de generación de vector de aleatorización $k^*_{L+1,ran,j}$)

En base a la clave publica maestra pk, la información de clave $\vec{k}^*_L$ y el vector de predicado $\vec{v}_{L+1}$ mostrados en la Fórmula 200, la unidad de generación de vector de aleatorización 430 calcula la Fórmula 202 para generar un vector de aleatorización $k^*_{L+1,ran,j}$ (j = 1, …, L+2).

[Fórmula 202]

(1)

$$\alpha_{\mathsf{ran},j,t},\sigma_{\mathsf{ran},j} \xleftarrow{\mathrm{U}} \mathbb{F}_q \qquad \left(j=1,\ldots,L+2;\ t=1,\ldots,L+1\right)$$

(2)

$$rv_j := \sum_{t=1}^{L+1} \alpha_{\mathsf{ran},j,t} k^*_{L,\mathsf{ran},t} \qquad \left(j=1,\ldots,L+2\right)$$

(3)

$$vv_j := \sigma_{\mathsf{ran},j} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathsf{del},i}\right) \qquad \left(j=1,\ldots,L+2\right)$$

(4)

$$\begin{aligned} k^*_{L+1,\mathsf{ran},j} &:= rv_j + vv_j \\ &:= \sum_{t=1}^{L+1} \alpha_{\mathsf{ran},j,t} k^*_{L,\mathsf{ran},t} + \sigma_{\mathsf{ran},j} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathsf{del},i}\right) \\ &\qquad \left(j=1,\ldots,L+2\right) \end{aligned}$$

(S604: Paso de generación de vector de generación de clave $k^*_{L+1,del,j}$)

Usando el dispositivo de procesamiento y en base a la clave publica maestra pk, la información de clave $\vec{k}^*_L$ y el vector de predicado $\vec{v}_{L+1}$ mostrados en la Fórmula 200, la unidad de generación de vector de generación de clave 440 calcula la Fórmula 203 para generar un vector de generación de clave $k^*_{L+1,del,j}$ (j = 1, …, n).

[Fórmula 203]

(1)

$$\alpha_{\mathsf{del},j,t}, \sigma_{\mathsf{del},j}, \psi' \xleftarrow{\mathrm{U}} \mathbb{F}_q \quad (j = 1,\ldots,n;\ i = 1,\ldots,L+1)$$

(2)

$$rv_j := \sum_{t=1}^{L+1} \alpha_{\mathsf{del},j,t} k^*_{L,\mathsf{del},t} \qquad (j = 1,\ldots,n)$$

(3)

$$vv_j := \sigma_{\mathsf{del},j} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathsf{del},i} \right) \qquad (j = 1,\ldots,n)$$

(4)

$$\psi v_j := \psi' k^*_{L,\mathsf{del},j} \qquad (j = 1,\ldots,n)$$

(5)

$$\begin{aligned} k^*_{L+1,\mathsf{del},j} &:= rv_j + vv_j + \psi v_j \\ &:= \sum_{t=1}^{L+1} \alpha_{\mathsf{del},j,t} k^*_{L,\mathsf{del},t} + \sigma_{\mathsf{del},j} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathsf{del},i} \right) \\ &\quad + \psi' k^*_{L,\mathsf{del},j} \\ &\qquad\qquad (j = 1,\ldots,n) \end{aligned}$$

Para resumir, en (S602) a (S604), usando el dispositivo de procesamiento, la unidad de generación de vector de clave 420, la unidad de generación de vector de aleatorización 430 y la unidad de generación de vector de generación de clave 440 ejecutan el algoritmo $\mathsf{Delegate}_L$ mostrado en la Fórmula 204 para generar la clave secreta de nivel de orden (L+1) (información de clave $\vec{k}^*_{L+1}$) que incluye el vector de clave $k^*_{L+1,\mathsf{dec}}$, el vector de aleatorización $k^*_{L+1,\mathsf{ran},j}$ (j = 1, …, L+2) y el vector de generación de clave $k^*_{L+1,\mathsf{del},j}$ (j = 1, …, n).

[Fórmula 204]

$$\begin{aligned} &\mathsf{Delegate}_L \left(\mathsf{pk}, \vec{k}^*_L, \vec{v}_{L+1} := (v_{L+1,1},\ldots,v_{L+1,n}) \right): \\ &\quad \alpha_{\mathsf{dec},t}, \sigma_{\mathsf{dec}}, \alpha_{\mathsf{ran},j,t}, \sigma_{\mathsf{ran},j} \ (j = 1,\ldots,L+2), \\ &\quad \alpha_{\mathsf{del},j,t}, \sigma_{\mathsf{del},j} \ (j = 1,\ldots,n), \psi' \xleftarrow{\mathrm{U}} \mathbb{F}_q \\ &\qquad \text{for } t = 1,\ldots,L+1, \\ &\quad k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + \sum_{t=1}^{L+1} \alpha_{\mathsf{dec},t} k^*_{L,\mathsf{ran},t} + \sigma_{\mathsf{dec}} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathsf{del},i} \right), \\ &\quad k^*_{L+1,\mathsf{ran},j} := \sum_{t=1}^{L+1} \alpha_{\mathsf{ran},j,t} k^*_{L,\mathsf{ran},t} + \sigma_{\mathsf{ran},j} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathsf{del},i} \right) \\ &\qquad \text{for } j = 1,\ldots,L+2, \\ &\quad k^*_{L+1,\mathsf{del},j} := \sum_{t=1}^{L+1} \alpha_{\mathsf{del},j,t} k^*_{L,\mathsf{del},t} + \sigma_{\mathsf{del},j} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathsf{del},i} \right) + \psi' k^*_{L,\mathsf{del},j} \\ &\qquad \text{for } j = 1,\ldots,n, \\ &\quad \text{devolver } \vec{k}^*_{L+1} := \left(k^*_{L+1,\mathsf{dec}}, k^*_{L+1,\mathsf{ran},1},\ldots,k^*_{L+1,\mathsf{ran},L+2}, k^*_{L+1,\mathsf{del},1},\ldots k^*_{L+1,\mathsf{del},n} \right). \end{aligned}$$

(S605: Paso de distribución de clave)

Como en (S605) de la segunda realización, la unidad de distribución de clave 450 transmite la información de clave $\vec{k}^*_{L+1}$ generada por la unidad de generación de vector de clave 420, la unidad de generación de vector de aleatorización 430 y la unidad de generación de vector de generación de clave 440 al dispositivo de descifrado 300 de un nivel más bajo a través del dispositivo de comunicación.

Como se describió anteriormente, si se mantiene $\vec{x}_i \cdot \vec{v}_j = 0$ para el vector de atributo $\vec{x}_i$ (i = 1, …, h) usado por el dispositivo de cifrado 200 para cifrado y el vector de predicado $\vec{v}_j$ (j = 1, …, L) del vector de clave $k^*_{L,dec}$ usado por el dispositivo de descifrado 300 para descifrado para cada i de (i = 1, …, h) y cada j de (j = 1, …, L), entonces el dispositivo de descifrado 300 tiene éxito en el descifrado. Es decir, cuando el vector de clave $k^*_{1,dec}$ generado en base al vector de predicado ($\vec{v}_1$) se usa para descifrado, el dispositivo de descifrado 300 tiene éxito en el descifrado si $\vec{x} \cdot \vec{v}_1 = 0$. Cuando el vector de clave $k^*_{2,dec}$ generado en base a los vectores de predicado ($\vec{v}_1$, $\vec{v}_2$) se usa para descifrado, el dispositivo de descifrado 300 tiene éxito en el descifrado si $\vec{x} \cdot \vec{v}_1 = 0$ y $\vec{x} \cdot \vec{v}_2 = 0$. Es decir, como con el algoritmo descrito en la segunda realización, el vector de clave de nivel más bajo $k^*_{2,dec}$ tiene capacidades más limitadas que el vector de clave de nivel más alto $k^*_{1,dec}$.

En esta realización, como en la segunda realización, se supone que el vector de base d_{n+1} en el que el dispositivo de cifrado 200 fija la información de transmisión es bidimensional. No obstante, la dimensión del vector de base d_{n+1} puede ser tridimensional o mayor, es decir, m dimensional (vector de base b_{n+1}, …, vector de base b_{n+m}).

Como en la segunda realización, el esquema HPKEM también se puede implementar modificando el algoritmo Enc ejecutado por el dispositivo de cifrado 200 y el algoritmo Dec ejecutado por el dispositivo de descifrado 300 como se muestra en la Fórmula 205 y la Fórmula 206 respectivamente.

[Fórmula 205]

$$\mathsf{Enc}\left(\mathsf{pk}, \left(\vec{x}_1, \ldots, \vec{x}_L\right) := \left(\left(x_{1,1}, \ldots, x_{1,n}\right), \ldots, \left(x_{L,1}, \ldots, x_{L,n}\right)\right)\right):$$

$$\delta_1, \ldots, \delta_L, \delta_{n+3}, \zeta \xleftarrow{U} \mathbb{F}_q,$$

$$c_1 := \sum_{t=1}^{L} \delta_t \left(\sum_{i=1}^{n} x_{t,i} b_i\right) + \zeta d_{n+1} + \delta_{n+3} b_{n+3}, \quad K := g_T^{\zeta},$$

$$\text{devolver } (c_1, K).$$

[Fórmula 206]

$$\mathsf{Dec}\left(\mathsf{pk}, k^*_{L,\mathsf{dec}}, c_1\right): K' := e\left(c_1, k^*_{L,\mathsf{dec}}\right),$$

$$\text{devolver } K'.$$

Cuarta realización

En las realizaciones anteriores, se han descrito los métodos para implementar los procesos criptográficos en espacios de vectores duales. En esta realización, se describirá un método para implementar los procesos criptográficos en modos duales.

Es decir, en las realizaciones anteriores, los procesos criptográficos se implementan en grupos cíclicos de orden primo q, No obstante, cuando un anillo R se expresa usando un número compuesto M como se muestra en la Fórmula 207, los procesos criptográficos descritos en las realizaciones anteriores se pueden adaptar a un módulo que tiene el anillo R como el coeficiente.

[Fórmula 207]

$$\mathbb{R} := \mathbb{Z}/M\mathbb{Z}$$

donde

$\mathbb{Z}$: entero,

M: número compuesto.

Por ejemplo, cuando el esquema HPE descrito en la segunda realización se implementa en el módulo que tiene el anillo R como el coeficiente, se expresa como se muestra en las Fórmulas 208 a 212.

[Fórmula 208]

$$\mathsf{Setup}\left(1^{\lambda}, \vec{\mu} := (n, d; \mu_1, \ldots, \mu_d)\right):$$

$$\left(\mathsf{param}, \mathbb{B}, \mathbb{B}^*\right) \xleftarrow{\mathrm{R}} \mathcal{G}_{\mathsf{ob}}\left(1^{\lambda}, n+3\right),$$

$$d_{n+1} := b_{n+1} + b_{n+2}, \quad \hat{\mathbb{B}} := (b_1, \ldots, b_n, d_{n+1}, b_{n+3}),$$

devolver $\mathsf{sk} := \left(X, \mathbb{B}^*\right)$, $\mathsf{pk} := \left(1^{\lambda}, \mathsf{param}, \hat{\mathbb{B}}\right)$.

donde

$$\mathcal{G}_{\mathsf{ob}}\left(1^{\lambda}, N\right): \mathsf{param} := \left(M, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*\right) \xleftarrow{\mathrm{R}} \mathcal{G}_{\mathsf{dpvs}}\left(1^{\lambda}, N\right),$$

$$X := \left(\chi_{i,j}\right) \xleftarrow{\mathrm{U}} GL(N, \mathbb{R}), \quad \left(\upsilon_{i,j}\right) := \left(X^{\mathrm{T}}\right)^{-1},$$

$$b_i = \sum_{j=1}^{N} \chi_{i,j} a_j, \ \mathbb{B} := (b_1, \ldots, b_N),$$

$$b_i^* = \sum_{j=1}^{N} \upsilon_{i,j} a_j^*, \ \mathbb{B}^* := (b_1^*, \ldots, b_N^*),$$

devolver $\left(\mathsf{param}, \mathbb{B}, \mathbb{B}^*\right)$

[Fórmula 209]

$$\mathsf{GenKey}\left(\mathsf{pk}, \mathsf{sk}, (\vec{v}_1, \ldots, \vec{v}_L)\right) := \left(\left(v_1, \ldots, v_{\mu_1}\right), \ldots, \left(v_{\mu_{L-1}+1}, \ldots, v_{\mu_L}\right)\right):$$

$$\sigma_{j,i}, \psi, \eta_j \xleftarrow{\mathrm{U}} \mathbb{R} \text{ for } j = 0, \ldots, L+1, \mu_L + 1, \ldots, n; \ i = 1, \ldots, L$$

$$k_{L,\mathsf{dec}}^* := \sum_{t=1}^{L} \sigma_{0,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \eta_0 b_{n+1}^* + (1-\eta_0) b_{n+2}^*,$$

$$k_{L,\mathsf{ran},j}^* := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \eta_0 b_{n+1}^* - \eta_j b_{n+2}^*$$

$$\text{for } j = 1, \ldots, L+1,$$

$$k_{L,\mathsf{del},j}^* := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \psi b_j^* + \eta_j b_{n+1}^* - \eta_j b_{n+2}^*$$

$$\text{for } j = \mu_L + 1, \ldots, n,$$

devolver $\vec{k}_L^* := \left(k_{L,0}^*, \ldots, k_{L,L+1}^*, k_{L,\mu_L+1}^*, \ldots, k_{L,n}^*\right)$.

[Fórmula 210]

$$\mathsf{Enc}\left(\mathsf{pk}, m \in \mathbb{G}_T, \left(\vec{x}_1, \ldots, \vec{x}_L\right) := \left(\left(x_1, \ldots, x_{\mu_1}\right), \ldots, \left(x_{\mu_{L-1}+1}, \ldots, x_{\mu_L}\right)\right)\right):$$

$$\left(\vec{x}_{L+1}, \ldots, \vec{x}_d\right) \xleftarrow{\mathrm{U}} \mathbb{R}^{\mu_{L+1}-\mu_L} \times \cdots \times \mathbb{R}^{n-\mu_{d-1}},$$

$$\delta_1, \ldots, \delta_d, \delta_{n+3}, \zeta \xleftarrow{\mathrm{U}} \mathbb{R},$$

$$c_1 := \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i\right) + \zeta d_{n+1} + \delta_{n+3} b_{n+3}, \quad c_2 := g_T^{\zeta} m,$$

devolver (c_1, c_2).

[Fórmula 211]

$$\mathsf{Dec}\left(\mathsf{pk}, k_{L,\mathsf{dec}}^*, c_1, c_2\right): m' := c_2 / e\left(c_1, k_{L,\mathsf{dec}}^*\right),$$

devolver m'.

[Fórmula 212]

$$\text{Delegate}_L\left(\text{pk}, \vec{k}^*_L, \vec{v}_{L+1} := \left(v_{\mu_L+1}, \ldots, v_{\mu_{L+1}}\right)\right):$$

$$\alpha_{j,i}, \sigma_j, \psi' \xleftarrow{U} \mathbb{R} \quad \text{for } j = 0, \ldots, L+2, \mu_{L+1}+1, \ldots, n;\ i = 1, \ldots, L+1,$$

$$k^*_{L+1,\text{dec}} := k^*_{L,\text{dec}} + \sum_{i=1}^{L+1} \alpha_{0,i} k^*_{L,\text{ran},i} + \sigma_0\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\text{del},i}\right),$$

$$k^*_{L+1,\text{ran},j} := \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\text{ran},i} + \sigma_j\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\text{del},i}\right) \quad \text{for } j = 0, \ldots, L+2,$$

$$k^*_{L+1,\text{del},j} := \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\text{ran},i} + \sigma_j\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\text{del},i}\right) + \psi' k^*_{L,\text{del},j}$$

$$\text{for } j = \mu_{L+1}+1, \ldots, n,$$

$$\text{devolver } \vec{k}^*_{L+1} := \left(k^*_{L+1,0}, \ldots, k^*_{L+1,L+2}, k^*_{L+1,\mu_{L+1}+1}, \ldots k^*_{L+1,n}\right).$$

En esta realización, se ha descrito solamente el método para implementar el esquema HPE de la segunda realización en el módulo que tiene el anillo R como el coeficiente. No obstante, en principio, los procesos descritos para el campo F_q en las realizaciones anteriores se pueden implementar en el módulo que tiene el anillo R como el coeficiente sustituyendo el campo Fq con el anillo R.

Se describirá ahora una configuración hardware del sistema de procesamiento criptográfico 10 (el dispositivo de generación de clave 100, el dispositivo de cifrado 200, el dispositivo de descifrado 300 y el dispositivo de delegación de clave 400) según las realizaciones.

La Fig. 21 es un diagrama que muestra un ejemplo de configuración hardware del dispositivo de generación de clave 100, el dispositivo de cifrado 200, el dispositivo de descifrado 300 y el dispositivo de delegación de clave 400.

Como se muestra en la Fig. 21, el dispositivo de generación de clave 100, el dispositivo de cifrado 200, el dispositivo de descifrado 300 y el dispositivo de delegación de clave 400 cada uno incluye la CPU 911 (unidad central de proceso, también llamada unidad de procesamiento, unidad aritmética, microprocesador, microordenador o procesador). La CPU 911 se conecta a través del bus 912 con la ROM 913, la RAM 914, el LCD 901 (visualizador de cristal líquido), el teclado 902 (K/B), la placa de comunicación 915 y el dispositivo de disco magnético 920 y controla estos dispositivos hardware. El dispositivo de disco magnético 920 (dispositivo de disco fijo) se puede sustituir con un dispositivo de almacenamiento tal como un dispositivo de disco óptico o un dispositivo de lectura/escritura de tarjeta de memoria. El dispositivo de disco magnético 920 se conecta a través de una interfaz de disco fija predeterminada.

La ROM 913 y el dispositivo de disco magnético 920 son ejemplos de una memoria no volátil. La RAM 914 es un ejemplo de una memoria volátil. La ROM 913, la RAM 914 y el dispositivo de disco magnético 920 son ejemplos de un dispositivo de almacenamiento (memoria). El teclado 902 y la placa de comunicación 915 son ejemplos de un dispositivo de entrada. La placa de comunicación 915 es un ejemplo de un dispositivo de comunicación (interfaz de red). El LCD 901 es un ejemplo de dispositivo de visualización.

El dispositivo de disco magnético 920, la ROM 913 o similar almacena un sistema operativo 921 (OS), un sistema de ventanas 922, programas 923 y ficheros 924. Los programas 923 se ejecutan por la CPU 911, el sistema operativo 921 y el sistema de ventanas 922.

Los programas 923 almacenan software o programas para ejecutar las funciones descritas en lo que antecede como “la unidad de generación de clave maestra 110”, “la unidad de almacenamiento de clave maestra 120”, “la unidad de generación de vector de clave 130”, “la unidad de generación de vector de aleatorización 140”, “la unidad de generación de vector de generación de clave 150”, “la unidad de distribución de clave 160”, “la unidad de ajuste de información de transmisión 210”, “la unidad de generación de vector de cifrado 220”, “la unidad de generación de información de cifrado 230”, “la unidad de transmisión de datos 240”, “la unidad de adquisición de clave pública 250”, “la unidad de generación de clave de sesión 260”, “la unidad de entrada de vector 310”, “la unidad de almacenamiento de vector de clave 320”, “la unidad de operación de emparejamiento 330”, “la unidad de adquisición de vector de clave 410”, “la unidad de generación de vector de clave 420”, “la unidad de generación de vector de aleatorización 430”, “la unidad de generación de vector de generación de clave 440”, “la unidad de distribución de clave 450”, etcétera. Los programas se leen y ejecutan por la CPU 911.

Los ficheros 924 almacenan información, datos, valores de señal, valores de variables y parámetros, tales como “la clave pública maestra pk”, “la clave secreta maestra sk”, “el vector de cifrado c” y “el vector de clave” descritos en lo que antecede, cada uno de los cuales se almacena como un ítem de un “fichero” o una “base de datos”. El “fichero” o la “base de datos” se almacena en un dispositivo de almacenamiento tal como un disco o memoria. La información, datos, valores de señal, valores de variable y parámetros almacenados en el dispositivo de

almacenamiento tal como el disco o memoria se leen por la CPU 911 a través de un circuito de lectura/escritura a una memoria principal o una memoria caché y se usan para operaciones de la CPU 911 tales como extracción, búsqueda, referencia, comparación, cálculo, computación, procesamiento, salida, impresión y visualización. La información, datos, valores de señal, valores de variable y parámetros se almacenan temporalmente en la memoria principal, la memoria caché o una memoria de almacenamiento temporal durante las operaciones de la CPU 911 tales como extracción, búsqueda, referencia, comparación, cálculo, computación, procesamiento, salida, impresión y visualización.

En los diagramas de flujo descritos en lo que antecede, una flecha representa principalmente una entrada/salida de datos o una señal y cada dato o valor de señal se almacena en la RAM 914 u otros tipos de medio de almacenamiento tales como un disco óptico o un chip IC. El dato o señal se transfiere en línea a través del bus 912, una línea de señal, un cable, otros tipos de medio de transferencia o una onda de radio.

Lo que se describe en lo que antecede como “una … unidad” puede ser “un … circuito”, “un … dispositivo”, “una … herramienta”, “unos … medios” o “una … función” y también puede ser “un … paso”, “un … procedimiento” o “un … proceso”. Lo que se describe como “un … dispositivo” puede ser “un … circuito”, “una … herramienta”, “unos … medios” o “una … función” y también puede ser “un … paso”, “un … procedimiento” o “un … proceso”. Lo que se describe como “un … proceso” puede ser “un … paso”. Es decir, lo que se describe como “una … unidad” se puede implementar mediante microprograma almacenado en la ROM 913. Alternativamente, “la … unidad” se puede implementar únicamente por software o únicamente por hardware tal como elementos, dispositivos, placas y cableado o por una combinación de software y hardware o por una combinación que incluye microprograma. El microprograma o software se almacena como un programa en un medio de almacenamiento tal como la ROM 913. El programa se lee por la CPU 911 y ejecuta por la CPU 911. Es decir, el programa hace a un ordenador o similar funcionar como “la … unidad” descrita anteriormente. Alternativamente, el programa hace al ordenador o similar ejecutar un procedimiento o un método de “la … unidad” descrita anteriormente.

Lista de signos de referencia

10: sistema de procesamiento criptográfico

100: dispositivo de generación de clave

110: unidad de generación de clave maestra

120: unidad de almacenamiento de clave maestra

130: unidad de generación de vector de clave

140: unidad de generación de vector de aleatorización.

150: unidad de generación de vector de generación de clave

160: unidad de distribución de clave

200: dispositivo de cifrado

210: unidad de ajuste de información de transmisión

220: unidad de generación de vector de cifrado

230: unidad de generación de información de cifrado

240: unidad de transmisión de datos

250: unidad de adquisición de clave pública

260: unidad de generación de clave de sesión

300: dispositivo de descifrado

310: unidad de entrada de vector

320: unidad de almacenamiento de vector de clave

330: unidad de operación de emparejamiento

400: dispositivo de delegación de clave

410: unidad de adquisición de vector de clave

420: unidad de generación de vector de clave

430: unidad de generación de vector de aleatorización

440: unidad de generación de vector de generación de clave

450: unidad de distribución de clave

REIVINDICACIONES

1. Un sistema de procesamiento criptográfico (10) que realiza un proceso de cifrado de predicado usando módulos duales de un espacio V y un espacio V* emparejados a través de una operación de emparejamiento mostrada en la Fórmula 1, el sistema de procesamiento criptográfico que comprende:

un dispositivo de cifrado (200) que, usando un dispositivo de procesamiento, genera como un vector de cifrado c_1 un vector de una base B^, la base B^ que tiene, de entre los vectores de base b_i (i = 1, …, n, …, N) (N que es un entero de 3 o mayor y n que es un entero de 1 a N-2) que constituye una base B predeterminada del espacio V, los vectores de base b_i (i = 1, …, n) y un vector de base d_{n+1} que es una suma de dos o más vectores de base b_i (i = n+1, …, m) de entre los vectores de base b_i (i = n+1, …, N), el vector de cifrado c_i que es el vector en el que la información de atributo se incrusta como coeficientes de uno o más vectores de base de entre el vector de base b_i (i = 1, …, n) e información predeterminada se incrusta como un coeficiente del vector de base d_{n+1}; y

un dispositivo de descifrado (300) que, usando el dispositivo de procesamiento, realiza la operación de emparejamiento e (c_1, $k^*_{L,dec}$) mostrada en la Fórmula 1 en el vector de cifrado c_1 generado por el dispositivo de cifrado y un vector de clave $k^*_{L,dec}$ para descifrar el vector de cifrado c_1 y para extraer un valor que concierne a la información predeterminada, el vector de clave $k^*_{L,dec}$ que es un vector de una base B* del espacio V* y construido de manera que la información de predicado se incrusta como coeficientes de uno o más vectores de base de los vectores de base b^*_i (i = 1, …, n) de entre los vectores de base b^*_i (i = 1, …, n, …, N) que constituyen la base B* y coeficientes de vectores de base b^*_i (i = n+1, …, m) de la base B* se incrustan de manera que una suma de los coeficientes de los vectores de base b^*_i (i = n+1, …, m) es 1.

[Fórmula 1]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

donde

$$p := \sum_{i=1}^{N} \chi_i b_i ,$$

$$q := \sum_{i=1}^{N} \eta_i b_i^* ,$$

χ_i, η_i : valores predeterminados.

2. El sistema de procesamiento criptográfico de la reivindicación 1, en el que dichos módulos duales comprenden espacios de vectores duales.

3. El sistema de procesamiento criptográfico de la reivindicación 2, que además comprende:

un dispositivo de generación de clave (100) que, usando el dispositivo de procesamiento, genera como el vector de clave $k^*_{L,dec}$ el vector en el cual la información de predicado se fija como los coeficientes del uno o más vectores de base de los vectores de base b^*_i (i = 1, …, n) de entre los vectores de base b^*_i (i = 1, …, N) que constituyen la base B* y los coeficientes de los vectores de base b^*_i (i = n+1, …, m) se fijan de manera que la suma de los coeficientes de los vectores de base b^*_i (i = n+1, …, m) es 1 y en el que

el dispositivo de descifrado obtiene el vector de claves $k^*_{L,dec}$ generado por el dispositivo de generación de clave y realiza la operación de emparejamiento sobre el vector de claves $k^*_{L,dec}$ obtenido y el vector de cifrado c_1.

4. El sistema de procesamiento criptográfico de la reivindicación 3, que además comprende:

un dispositivo de delegación de clave (400) que genera como un vector de clave $k^*_{L+1,dec}$ un vector que puede descifrar uno o más, pero no todos, de los vectores de cifrado que se pueden descifrar por el vector de clave $k^*_{L,dec}$ generado por el dispositivo de generación de clave, el vector de clave $k^*_{L+1,dec}$ que es el vector en el que los números aleatorios que tiene valores distribuidos uniformemente se fijan como coeficientes de vectores de base en los cuales se fija información de predicado.

5. Un dispositivo de generación de clave (100) que genera un vector de clave $k^*_{L,dec}$ que es una clave secreta en un esquema de cifrado de predicado, el dispositivo de generación de clave que comprende:

una unidad de almacenamiento de clave maestra (120) que, cuando un espacio V y un espacio V* son módulos duales emparejados a través de una operación de emparejamiento, almacena en un dispositivo de almacenamiento una base predeterminada B* del espacio V*; y

una unidad de generación de vector de clave (130) que, usando un dispositivo de procesamiento, genera como el vector de clave $k^*_{L,dec}$ un vector en el que se fija información de predicado como coeficientes de uno o más vectores de base b^*_i (i = 1, …, μ_L) de un vector de base b^*_i (i = 1, …, n) de entre vectores de base b^*_i (i = 1, …, n, …, N) (N que es un entero de 3 o mayor y n que es un entero de 1 a N-2) que constituyen la base B* almacenada por la unidad de almacenamiento de clave maestra y coeficientes de dos o más vectores de base predeterminados de entre los vectores de base b^*_i (i = n+1, …, N) se fijan de manera que una suma de los coeficientes de los dos o más vectores de base predeterminados es 1.

6. El dispositivo de generación de clave de la reivindicación 5, en el que dichos módulos duales comprenden espacios de vectores duales.

7. El dispositivo de generación de clave de la reivindicación 6,

en el que la unidad de generación de vector de clave genera el vector de clave $k^*_{L,dec}$ como se muestra en la Fórmula 2.

[Fórmula 2]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{0,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^* \right) + \eta_0 b^*_{n+1} + (1-\eta_0) b^*_{n+2}$$

donde

$\sigma_{0,i}, \eta_0$ (*i = 1, …, L*): valores predeterminados,

v_i (*i = 1, …, μ_L*): información de predicado.

8. El dispositivo de generación de clave de la reivindicación 6,

en el que la unidad de generación de vector de clave genera el vector de clave $k^*_{L,dec}$ como se muestra en la Fórmula 3.

[Fórmula 3]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{\mathrm{dec},t} \left(\sum_{i=1}^{n} v_{t,i} b_i^* \right) + \eta_{\mathrm{dec}} b^*_{n+1} + (1-\eta_{\mathrm{dec}}) b^*_{n+2}$$

donde

$\sigma_{\mathrm{dec},t}, \eta_{\mathrm{dec}}$ (*i = 1, …, L*): valores predeterminados,

$v_{t,i}$ (*t = 1,…, L; i = 1, …, n*): información de predicado.

9. Un dispositivo de generación de clave de la reivindicación 6, que además comprende:

una unidad de generación de vector de generación de claves (150) que, usando el dispositivo de procesamiento, genera como un vector de generación de claves $k^*_{L,del,j}$ al menos un numero (n-μ_L) de vectores que puede descifrar uno o más, pero no todos, de los vectores de cifrado que se pueden descifrar por el vector de clave $k^*_{L,dec}$ generado por la unidad de generación de vector de clave, el vector de generación de clave $k^*_{L,del,j}$ que es un vector en el que un valor predeterminado se fija como un coeficiente de un vector de base b^*_i para al menos cada j de j = μ_L+1, …, n; y

una unidad de generación de vector de aleatorización (140) que, usando el dispositivo de procesamiento, genera como un vector de aleatorización $k^*_{L,ran,j}$ al menos un numero (L+1) de vectores para ajustar valores distribuidos uniformemente como coeficientes de vectores de base del vector de clave $k^*_{L+1,dec}$ generado con el vector de generación de clave $k^*_{L,del,j}$ generado por la unidad de generación de vector de generación de clave, los coeficientes que se fijan de manera que se fija la información de predicado y el vector de aleatorización $k^*_{L,ran,j}$ que es un vector en el que se fija un valor predeterminado como un coeficiente de un vector de base b^*_j para al menos cada j de j = 1, …, L+1.

10. El dispositivo de generación de clave de la reivindicación 9,

en el que la unidad de generación de vector de clave genera el vector de generación de clave $k^*_{L,del,j}$ como se muestra en la Fórmula 4 y

en el que la unidad de generación de vector de aleatorización genera el vector de aleatorización $k^*_{L,ran,j}$ como se muestra en la Fórmula 5.

[Fórmula 4]

$$k^*_{L,\mathrm{del},j} := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^* \right) + \psi b_j^* + \eta_j b_{n+1}^* - \eta_j b_{n+2}^* \quad \left(j = \mu_L + 1, \ldots, n \right)$$

donde

$\sigma_{j,i}, \psi, \eta_j$ ($j = \mu_L+1, \ldots, n; i=1, \ldots, L$): valores predeterminados,

v_i ($i = 1, \ldots, \mu_L$): información de predicado.

[Fórmula 5]

$$k^*_{L,\mathrm{ran},j} := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^* \right) + \eta_j b_{n+1}^* - \eta_j b_{n+2}^* \quad \left(j = 1, \ldots, L+1 \right)$$

donde

$\sigma_{j,i}, \eta_j$ ($j = 1, \ldots, L+1; i=1, \ldots, L$): valores predeterminados,

v_i ($i = 1, \ldots, \mu_L$): información de predicado.

11. El dispositivo de generación de clave de la reivindicación 9,

en el que la unidad de generación de vector de clave genera el vector de generación de clave $k^*_{L,del,j}$ como se muestra en la Fórmula 6 y

en el que la unidad de generación de vector de aleatorización genera el vector de aleatorización $k^*_{L,ran,j}$ como se muestra en la Fórmula 7.

[Fórmula 6]

$$k^*_{L,\mathrm{del},j} := \sum_{t=1}^{L} \sigma_{\mathrm{del},j,t} \left(\sum_{i=1}^{n} v_{t,i} b_i^* \right) + \psi b_j^* + \eta_{\mathrm{del},j} b_{n+1}^* - \eta_{\mathrm{del},j} b_{n+2}^* \quad \left(j = 1, \ldots, n \right)$$

donde

$\sigma_{\mathrm{del},j,t}, \eta_{\mathrm{del},j}, \psi$ ($j = 1, \ldots, n; t=1, \ldots, L$): valores predeterminados,

$v_{t,i}$ ($t = 1, \ldots, L; i = 1, \ldots, n$): información de predicado.

[Fórmula 7]

$$k^*_{L,\mathrm{ran},j} := \sum_{t=1}^{L} \sigma_{\mathrm{ran},j,t} \left(\sum_{i=1}^{n} v_{t,i} b^*_i \right) + \eta_{\mathrm{ran},j} b^*_{n+1} - \eta_{\mathrm{ran},j} b^*_{n+2}$$
$$(j = 1, \ldots, L+1)$$

donde

$\sigma_{\mathrm{ran},j,t}, \eta_{\mathrm{ran},j}$ (*j = 1, …, L+1; t = 1, …, L*): valores predeterminados,

$v_{t,i}$ (*t = 1,…, L; i = 1, …, n*): información de predicado.

12. Un dispositivo de delegación de clave (400) que genera un vector de clave $k^*_{L+1,dec}$ que puede descifrar uno o más, pero no todos, de los vectores de cifrado que se pueden descifrar por el vector de clave $k^*_{L,dec}$ que es una clave secreta en un esquema de cifrado de predicado, el dispositivo de delegación de clave que comprende:

una unidad de adquisición de vector de clave (410) que, cuando un espacio V y un espacio V* son módulos duales emparejados a través de una operación de emparejamiento, obtiene el vector de clave $k^*_{L,dec}$ en el cual se fija información de predicado como coeficientes de uno o más vectores de base b^*_i (i = 1, …, μ_L) de vectores de base b^*_i (i = 1, …, n) de entre los vectores de base b^*_i (i = 1, …, n, …, N) (N que es un entero de 3 o mayor y n que es un entero de 1 a N-2) que constituye una base B* predeterminada del espacio V* y coeficientes de dos o más vectores de base predeterminados de entre los vectores de base b^*_i (i = n+1, …, N) se fijan de manera que una suma de los coeficientes de los dos o más vectores de base predeterminados es 1;

una unidad de adquisición de vector de generación de clave (410) que obtiene al menos un número (n-μ_L) de vectores de generación de clave $k^*_{L,del,j}$ en los cuales se fija un valor predeterminado como un coeficiente de un vector de base b^*_j para al menos cada j de j = μ_L+1, …, n; y

una unidad de generación de vector de clave (420) que genera el vector de claves $k^*_{L+1,dec}$ multiplicando por información de predicado un coeficiente de cada vector de base de uno o más vectores de generación de clave $k^*_{L,del,j}$ de entre los vectores de generación de clave $k^*_{L,del,j}$ obtenidos por la unidad de adquisición de vector de generación de clave y añadiendo cada resultado al vector de clave $k^*_{L,dec}$ obtenido por la unidad de adquisición de vector de clave.

13. El dispositivo de delegación de clave de la reivindicación 12, en el que dichos módulos duales comprenden espacios de vectores duales.

14. El dispositivo de delegación de clave de la reivindicación 13, que además comprende:

una unidad de adquisición de vector de aleatorización que obtiene al menos un número (L+1) de vectores de aleatorización $k^*_{L,ran,j}$ en los cuales se fija un valor predeterminado como un coeficiente de un vector de base b^*_j para al menos cada j de j = 1, …, L+1 y en el que

la unidad de generación de vector de clave genera el vector de clave $k^*_{L+1,dec}$ multiplicando por un número aleatorio un coeficiente de cada vector de base de uno o más vectores de aleatorización $k^*_{L,ran,j}$ de entre los vectores de aleatorización $k^*_{L,ran,j}$ obtenidos por la unidad de adquisición de vector de aleatorización y añadiendo además cada resultado al vector de clave $k^*_{L+1,dec}$.

15. El dispositivo de delegación de clave de la reivindicación 14,

en el que la unidad de adquisición de vector de clave obtiene el vector de clave $k^*_{L,dec}$ como se muestra en la Fórmula 8,

en el que la unidad de adquisición de vector de generación de clave obtiene el vector de generación de clave $k^*_{L,del,j}$ como se muestra en la Fórmula 9,

en el que la unidad de adquisición de vector de aleatorización obtiene el vector de aleatorización $k^*_{L,ran,j}$ como se muestra en la Fórmula 10 y

en el que la unidad de generación de vector de clave genera el vector de clave $k^*_{L+1,dec}$ como se muestra en la Fórmula 11.

[Fórmula 8]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{0,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i \right) + \eta_0 b^*_{n+1} + (1-\eta_0) b^*_{n+2}$$

donde

$\sigma_{0,i}, \eta_0$ (*i = 1, …, L*): valores predeterminados,

v_i (*i = 1, …, μ_L*): información de predicado.

[Fórmula 9]

$$k^*_{L,\mathrm{del},j} := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^* \right) + \psi b_j^* + \eta_j b_{n+1}^* - \eta_j b_{n+2}^* \quad (j = \mu_L + 1, \ldots, n)$$

donde

$\sigma_{j,i}, \psi, \eta_j$ (*j = μ_L+1, …, n; i = 1, …, L*): valores predeterminados,

v_i (*i = 1, …, μ_L*): información de predicado.

[Fórmula 10]

$$k^*_{L,\mathrm{ran},j} := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^* \right) + \eta_j b_{n+1}^* - \eta_j b_{n+2}^* \quad (j = 1, \ldots, L+1)$$

donde

$\sigma_{j,i}, \eta_j$ (j = 1, …, L+1; i = 1, …, L): valores predeterminados,

v_i (*i = 1, …, μ_L*): información de predicado.

[Fórmula 11]

$$k^*_{L+1,\mathrm{dec}} := k^*_{L,\mathrm{dec}} + \sum_{i=1}^{L+1} \alpha_{0,i} k^*_{L,\mathrm{ran},i} + \sigma_0 \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i} \right)$$

donde

$\alpha_{0,i}, \sigma_0$ (*i = 1, …, L+1*): valores predeterminados,

v_i (*i = μ_L+1,…, μ_{L+1}*): información de predicado.

16. El dispositivo de delegación de clave de la reivindicación 14,

en el que la unidad de adquisición de vector de clave obtiene el vector de clave $k^*_{L,dec}$ como se muestra en la Fórmula 12,

en el que la unidad de adquisición de vector de generación de clave obtiene el vector de generación de clave $k^*_{L,del,j}$ como se muestra en la Fórmula 13,

en el que la unidad de adquisición de vector de aleatorización obtiene el vector de aleatorización $k^*_{L,ran,j}$ como se muestra en la Fórmula 14 y

en el que la unidad de generación de vector de clave genera el vector de clave $k^*_{L+1,dec}$ como se muestra en la Fórmula 15.

[Fórmula 12]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{\mathrm{dec},t} \left(\sum_{i=1}^{n} v_{t,i} b^*_i \right) + \eta_{\mathrm{dec}} b^*_{n+1} + (1 - \eta_{\mathrm{dec}}) b^*_{n+2}$$

donde

$\sigma_{\mathrm{dec},t}, \eta_{\mathrm{dec}}$ (*t = 1, …, L*): valores predeterminados,

$v_{t,i}$ (*t = 1,…, L; i = 1, …, n*): información de predicado.

[Fórmula 13]

$$k^*_{L,\mathrm{del},j} := \sum_{t=1}^{L} \sigma_{\mathrm{del},j,t} \left(\sum_{i=1}^{n} v_{t,i} b^*_i \right) + \psi b^*_j + \eta_{\mathrm{del},j} b^*_{n+1} - \eta_{\mathrm{del},j} b^*_{n+2} \quad (j = 1, \ldots, n)$$

donde

$\sigma_{\mathrm{del},j,t}, \eta_{\mathrm{del},j}, \psi$ (*j = 1, …, n; t = 1, …, L*): valores predeterminados,

$v_{t,i}$ (*t = 1,…, L; i = 1, …, n*): información de predicado.

[Fórmula 14]

$$k^*_{L,\mathrm{ran},j} := \sum_{t=1}^{L} \sigma_{\mathrm{ran},j,t} \left(\sum_{i=1}^{n} v_{t,i} b^*_i \right) + \eta_{\mathrm{ran},j} b^*_{n+1} - \eta_{\mathrm{ran},j} b^*_{n+2} \quad (j = 1, \ldots, L+1)$$

donde

$\sigma_{\mathrm{ran},j,t}, \eta_{\mathrm{ran},j}$ (*j = 1, …, L+1; t = 1, …, L*): valores predeterminados,

$v_{t,i}$ (*t = 1,…, L; i = 1, …, n*): información de predicado.

[Fórmula 15]

$$k^*_{L+1,\mathrm{dec}} := k^*_{L,\mathrm{dec}} + \sum_{t=1}^{L+1} \alpha_{\mathrm{dec},t} k^*_{L,\mathrm{ran},t} + \sigma_{\mathrm{dec}} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathrm{del},i} \right)$$

donde

$\sigma_{\mathrm{dec},t}, \sigma_{\mathrm{dec}}$ (*t = 1, …, L+1*): valores predeterminados,

$v_{L+1,i}$ (*i = 1, …, n*): información de predicado.

17. El dispositivo de delegación de clave de la reivindicación 14, que además comprende:

una unidad de generación de vector de generación de clave (440) que, usando un dispositivo de procesamiento, genera como un vector de generación de clave $k^*_{L+1,\mathrm{del},j}$ al menos un número $(n-\mu_{L+1})$ de vectores que pueden descifrar uno o más, pero no todos, de los vectores de cifrado que se pueden descifrar por el vector de clave $k^*_{L+1,\mathrm{dec}}$ generado por la unidad de generación de vector de clave, el vector de generación de clave $k^*_{L+1,\mathrm{del},j}$ que es un vector en el que se fija un valor predeterminado como un coeficiente de un vector de base b^*_j para al menos cada j de $j = \mu_{L+1}+1, \ldots, n$; y

una unidad de generación de vector de aleatorización (430) que, usando el dispositivo de procesamiento, genera como un vector de aleatorización $k^*_{L+1,\mathrm{ran},j}$ al menos un número (L+2) de vectores para ajustar valores distribuidos uniformemente como coeficientes de vectores de base del vector de clave $k^*_{L+2,\mathrm{dec}}$ generado con el vector de generación de clave $k^*_{L+1,\mathrm{del},j}$ generado por la unidad de generación de vector de generación de clave, los coeficientes que se fijan de manera que se fija información de predicado y el vector de aleatorización $k^*_{L+1,\mathrm{ran},j}$

que es un vector en el que se fija un valor predeterminado como un coeficiente de un vector de base b^*_j para al menos cada j de j = 1, …, L+2.

18. El dispositivo de delegación de clave de la reivindicación 17,

en el que la unidad de adquisición de vector de generación de clave obtiene el vector de generación de clave $k^*_{L,del,j}$ como se muestra en la Fórmula 16,

en el que la unidad de adquisición de vector de aleatorización obtiene el vector de aleatorización $k^*_{L,ran,j}$ como se muestra en la Fórmula 17,

en el que la unidad de generación de vector de clave genera el vector de generación de clave $k^*_{L+1,del,j}$ como se muestra en la Fórmula 18 y

en el que la unidad de generación de vector de aleatorización genera el vector de aleatorización $k^*_{L+1,ran,j}$ como se muestra en la Fórmula 19.

[Fórmula 16]

$$k^*_{L,\mathrm{del},j} := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i \right) + \psi b^*_j + \eta_j b^*_{n+1} - \eta_j b^*_{n+2} \quad \left(j = \mu_L + 1, \ldots, n \right)$$

donde

$\sigma_{j,t}, \psi, \eta_j$ ($j = \mu_L+1, \ldots, n;\ t = 1, \ldots, L$): valores predeterminados,

v_i ($i = 1, \ldots, \mu_L$): información de predicado.

[Fórmula 17]

$$k^*_{L,\mathrm{ran},j} := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i \right) + \eta_j b^*_{n+1} - \eta_j b^*_{n+2} \quad \left(j = 1, \ldots, L+1 \right)$$

donde

$\sigma_{j,t}, \eta_j$ ($j = 1, \ldots, L+1;\ t = 1, \ldots, L$): valores predeterminados,

v_i ($i = 1, \ldots, \mu_L$): información de predicado.

[Fórmula 18]

$$k^*_{L+1,\mathrm{del},j} := \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\mathrm{ran},i} + \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i} \right) + \psi' k^*_{L,\mathrm{del},j} \quad \left(j = \mu_{L+1} + 1, \ldots, n \right)$$

donde

$\alpha_{j,i}, \sigma_j, \psi'$ ($j = \mu_{L+1}+1, \ldots, n;\ i = 1, \ldots, L+1$): valores predeterminados,

v_i ($i = \mu_L+1, \ldots, \mu_{L+1}$) : información de predicado.

[Fórmula 19]

$$k^*_{L+1,\mathrm{ran},j} := \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\mathrm{ran},i} + \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i} \right) \quad (j = 1,\ldots,L+2)$$

donde

$\alpha_{j,i}, \sigma_j$ (*j = 1, …, L+2; i = 1, ..., L+1*): valores predeterminados,

v_i (*i = μ_L+1, …, μ_{L+1}*) : información de predicado.

19. El dispositivo de delegación de clave de la reivindicación 17,

en el que la unidad de adquisición de vector de generación de clave obtiene el vector de generación de clave $k^*_{L,\mathrm{del},j}$ como se muestra en la Fórmula 20,

en el que la unidad de adquisición de vector de aleatorización obtiene el vector de aleatorización $k^*_{L,\mathrm{ran},j}$ como se muestra en la Fórmula 21,

en el que la unidad de generación de vector de clave genera el vector de generación de clave $k^*_{L+1,\mathrm{del},j}$ como se muestra en la Fórmula 22 y

en el que la unidad de generación de vector de aleatorización genera el vector de aleatorización $k^*_{L+1,\mathrm{ran},j}$ como se muestra en la Fórmula 23.

[Fórmula 20]

$$k^*_{L,\mathrm{del},j} := \sum_{t=1}^{L} \sigma_{\mathrm{del},j,t} \left(\sum_{i=1}^{n} v_{t,i} b^*_i \right) + \psi b^*_j + \eta_{\mathrm{del},j} b^*_{n+1} - \eta_{\mathrm{del},j} b^*_{n+2} \quad (j = 1,\ldots,n)$$

donde

$\sigma_{\mathrm{del},j,t}, \eta_{\mathrm{del},j}, \psi$ (*j = 1, …, n; t = 1, …, L*): valores predeterminados,

$v_{t,i}$ (*t = 1,…, L; i = 1, …, n*): información de predicado.

[Fórmula 21]

$$k^*_{L,\mathrm{ran},j} := \sum_{t=1}^{L} \sigma_{\mathrm{ran},j,t} \left(\sum_{i=1}^{n} v_{t,i} b^*_i \right) + \eta_{\mathrm{ran},j} b^*_{n+1} - \eta_{\mathrm{ran},j} b^*_{n+2} \quad (j = 1,\ldots,L+1)$$

donde

$\sigma_{\mathrm{ran},j,t}, \eta_{\mathrm{ran},j}$ (*j = 1, …, L+1; t = 1, …, L*): valores predeterminados,

$v_{t,i}$ (*t = 1,…, L; i = 1, …, n*): información de predicado.

[Fórmula 22]

$$k^*_{L+1,\mathrm{del},j} := \sum_{t=1}^{L+1} \alpha_{\mathrm{del},j,t} k^*_{L,\mathrm{del},t} + \sigma_{\mathrm{del},j} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathrm{del},i} \right) + \psi' k^*_{L,\mathrm{del},j} \quad (j = 1,\ldots,n)$$

donde

$\alpha_{\mathrm{del},j,t}, \sigma_{\mathrm{del},j}, \psi'$ (*j = 1, …, n; i = 1, …, L+1*): valores predeterminados,

$v_{L+1,i}$ (*i = 1, …, n*) : información de predicado.

[Fórmula 23]

$$k^*_{L+1,\mathrm{ran},j} := \sum_{t=1}^{L+1} \alpha_{\mathrm{ran},j,t} k^*_{L,\mathrm{ran},t} + \sigma_{\mathrm{ran},j} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathrm{del},i} \right) \quad (j = 1, \ldots, L+2)$$

donde

$\alpha_{\mathrm{ran},j,t}, \sigma_{\mathrm{ran},j}$ (*j = 1, …, L+2; t = 1, ..., L+1*): valores predeterminados,

$v_{L+1,i}$ (*i = 1, …, n*) : información de predicado.

20. Un dispositivo de cifrado (200) que genera un vector de cifrado c_1 que es un texto cifrado en un esquema de cifrado de predicado, el dispositivo de cifrado que comprende:

una unidad de adquisición de clave pública (250) que, cuando un espacio V y un espacio V* son módulos duales emparejados a través de una operación de emparejamiento obtiene una base B^ e información de atributo predeterminada, la base B^ que tiene, de entre los vectores de base b_i (i = 1, …, n, …N) (N que es un entero de 3 o mayor y n que es un entero de 1 a N-2) que constituyen una base predeterminada B del espacio V, vectores de base b_i (i = 1, …, n) y un vector de base d_{n+1} que es una suma de dos o más vectores de base predeterminados de entre los vectores de base b_i (i = n+1, …, N);

una unidad de ajuste de información de transmisión (210) que, usando un dispositivo de procesamiento, genera como un vector de información de transmisión çv un vector de la base B^ obtenido por la unidad de adquisición de clave pública, el vector de información de transmisión çv que es el vector en el que se fija información predeterminada como un coeficiente del vector de base d_{n+1}; y

una unidad de generación de vector de cifrado (220) que, usando el dispositivo de procesamiento, genera el vector de cifrado c_1 añadiendo un vector de información de atributo en el que se fija información de atributo como coeficientes de uno o más vectores de base de entre los vectores de base b_i (i = 1, …, n) de la base B^ al vector de información de transmisión çv generado por la unidad de ajuste de información de transmisión.

21. El dispositivo de cifrado de la reivindicación 20, en el que dichos módulos duales comprenden espacios de vectores duales.

22. El dispositivo de cifrado de la reivindicación 21,

en el que la unidad de ajuste de información de transmisión genera el vector de información de transmisión çv como se muestra en la Fórmula 24 y

en el que la unidad de generación de vector de cifrado genera el vector de cifrado c_1 como se muestra en la Fórmula 25.

[Fórmula 24]

$$\zeta v := \zeta d_{n+1}$$

donde

ζ : valor predeterminado.

[Fórmula 25]

$$c_1 := \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i \right) + \zeta d_{n+1}$$

donde

$\left(\vec{x}_1, \ldots, \vec{x}_L \right) := \left(\left(x_1, \ldots, x_{\mu_1} \right), \ldots, \left(x_{\mu_{L-1}+1}, \ldots, x_{\mu_L} \right) \right)$: información de atributo,

$\left(\vec{x}_{L+1},\ldots,\vec{x}_d\right) := \left(\left(x_{\mu_L+1},\ldots,x_{\mu_{L+1}}\right),\ldots,\left(x_{\mu_{d-1}+1},\ldots,x_{\mu_d}\right)\right)$: valores predeterminados,

$\delta_1,\ldots,\delta_d$: valores predeterminados,

23. El dispositivo de cifrado de la reivindicación 21,

en el que la unidad de ajuste de información de transmisión genera el vector de información de transmisión ςv como se muestra en la Fórmula 26 y

en el que la unidad de generación de vector de cifrado genera el vector de cifrado c_1 como se muestra en la Fórmula 27.

[Fórmula 26]

$$\zeta v := \zeta d_{n+1}$$

donde

ζ : valor predeterminado.

[Fórmula 27]

$$c_1 := \sum_{t=1}^{L} \delta_t \left(\sum_{i=1}^{n} x_{t,i} b_i\right) + \zeta d_{n+1}$$

donde

$\left(\vec{x}_1,\ldots,\vec{x}_L\right) := \left(\left(x_{1,1},\ldots,x_{1,n}\right),\ldots,\left(x_{L,1},\ldots,x_{L,n}\right)\right)$: información de atributo,

$\delta_1,\ldots,\delta_d$: valores predeterminados,

24. El dispositivo de cifrado de la reivindicación 21, que además comprende:

una unidad de generación de información de cifrado (230) que genera información de cifrado c_2 mostrada en la Fórmula 28.

[Fórmula 28]

$$c_2 := g_T^{\zeta} m$$

donde

$g_T = e(a_i, a_i^*) \neq 1$,

A es una base del espacio **V** y es **A** : = ($a_1, \ldots, a_N$),

A* es una base del espacio **V*** y es **A*** : = ($a^*_1, \ldots, a^*_N$).

25. Un dispositivo de descifrado (300) que descifra un texto cifrado en un esquema de cifrado de predicado, el dispositivo de descifrado que comprende:

una unidad de entrada de vector (310) que, cuando un espacio V y un espacio V* son módulos duales emparejados a través de una operación de emparejamiento, introduce un vector de cifrado c_1 de una base B^, la base B^ que tiene, de entre los vectores de base b_i (i = 1, …, n, …N) (N que es un entero de 3 o mayor y n que es un entero de 1 a N-2) que constituyen una base predeterminada B del espacio V, los vectores de base b_i (i = 1, …, n) y un vector de base d_{n+1} que es una suma de dos o más vectores de base predeterminados de entre los vectores de base b_i (i = n+1, …, N), el vector de cifrado c_1 que es un vector en el que se fija información de atributo como coeficientes de al menos los vectores de base b_i (i = 1, …, μ_h) de entre los vectores de base b_i (i = 1, …, n) y se fija información predeterminada como un coeficiente del vector de base d_{n+1};

una unidad de almacenamiento de vector de clave (320) que almacena en un dispositivo de almacenamiento un vector de clave $k^*_{L,dec}$ en el que se fija información de predicado v_i (i = 1, …, μ_L) como coeficientes de al menos los vectores de base b^*_i (i = 1, …, μ_L) ($\mu_L \leq \mu_h$) de vectores de base b^*_i (i = 1, …, n) de entre los vectores de base b^*_i (i = 1, …, n, … N) de una base predeterminada B* del espacio V* y coeficientes de vectores de base b^*_i que corresponden a los vectores de base b_i que constituyen el vector de base d_{n+1} se fijan de manera que una suma de los coeficientes de los vectores de base b^*_i es 1; y

una unidad de operación de emparejamiento (330) que, usando un dispositivo de procesamiento, realiza la operación de emparejamiento sobre el vector de cifrado c_1 introducido por la unidad de entrada de vector y el vector de clave $k^*_{L,dec}$ almacenado por la unidad de almacenamiento de vector de clave para extraer del vector de cifrado c_1 un valor que concierne a la información predeterminada.

26. El dispositivo de descifrado de la reivindicación 25, en donde dichos módulos duales comprenden espacios de vectores duales.

27. El dispositivo de descifrado de la reivindicación 26,

en el que la unidad de entrada de vector introduce el vector de cifrado c_1 como se muestra en la Fórmula 29,

en el que la unidad de almacenamiento de vector de clave almacena el vector de clave $k^*_{L,dec}$ como se muestra en la Fórmula 30 y

en el que la unidad de operación de emparejamiento realiza la operación de emparejamiento como se muestra en la Fórmula 31 para extraer del vector de cifrado el valor que concierne a la información predeterminada.

[Fórmula 29]

$$c_1 := \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i \right) + \zeta d_{n+1}$$

donde

$\left(\vec{x}_1, \ldots, \vec{x}_h\right) := \left(\left(x_1, \ldots, x_{\mu_1}\right), \ldots, \left(x_{\mu_{L-1}+1}, \ldots, x_{\mu_h}\right)\right)$: información de atributo,

$\left(\vec{x}_{h+1}, \ldots, \vec{x}_d\right) := \left(\left(x_{\mu_{h+1}+1}, \ldots, x_{\mu_{h+2}}\right), \ldots, \left(x_{\mu_{d-1}+1}, \ldots, x_{\mu_d}\right)\right)$: valores predeterminados,

$\delta_1, \ldots, \delta_d, \zeta$: valores predeterminados.

[Fórmula 30]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{0,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i \right) + \eta_0 b^*_{n+1} + (1-\eta_0) b^*_{n+2}$$

donde

$\sigma_{0,i}, \eta_0$ (*i = 1, …, L*): valores predeterminados,

v_i (*i = 1, …, μ_L*): información de predicado.

[Fórmula 31]

$$e\left(c_1, k^*_{L,\mathrm{dec}}\right)$$

donde

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b^*_i),$$

$$p := \sum_{i=1}^{N} \chi_i b_i,$$

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i: valores predeterminados.

28. El dispositivo de descifrado de la reivindicación 26,

en el que la unidad de entrada de vector introduce el vector de cifrado c_1 como se muestra en la Fórmula 32,

en el que la unidad de almacenamiento de vector de clave almacena el vector de clave $k^*_{L,dec}$ como se muestra en la Fórmula 33 y

en el que la unidad de operación de emparejamiento realiza la operación de emparejamiento como se muestra en la Fórmula 34 para extraer del vector de cifrado el valor que concierne a la información predeterminada.

[Fórmula 32]

$$c_1 := \sum_{t=1}^{h} \delta_t \left(\sum_{i=1}^{n} x_{t,i} b_i \right) + \zeta d_{n+1}$$

donde

$\left(\vec{x}_1, \ldots, \vec{x}_h \right) := \left(\left(x_{1,1}, \ldots, x_{1,n} \right), \ldots, \left(x_{h,1}, \ldots, x_{h,n} \right) \right)$: información de atributo,

$\delta_1, \ldots, \delta_d, \zeta$: valores predeterminados.

[Fórmula 33]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{\mathrm{dec},t} \left(\sum_{i=1}^{n} v_{t,i} b_i^* \right) + \eta_{\mathrm{dec}} b_{n+1}^* + (1 - \eta_{\mathrm{dec}}) b_{n+2}^*$$

donde

$\sigma_{\mathrm{dec},t}, \eta_{\mathrm{dec}}$ (*t = 1, …, L*): valores predeterminados,

$v_{t,i}$ (*t = 1, …, L; i = 1, …, n*): información de atributo.

[Fórmula 34]

$$e\left(c_1, k^*_{L,\mathrm{dec}} \right)$$

donde

$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$,

$p := \sum_{i=1}^{N} \chi_i b_i$,

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i: valores predeterminados.

29. El dispositivo de descifrado de la reivindicación 26,

en el que la unidad de entrada de vector introduce el vector de cifrado c_1 como se muestra en la Fórmula 35 y la información de cifrado c_2 como se muestra en la Fórmula 36 en la que se cifra un mensaje m,

en el que la unidad de almacenamiento de vector de clave almacena el vector de clave $k^*_{L,dec}$ como se muestra en la Fórmula 37 y

en el que la unidad de operación de emparejamiento realiza una operación como se muestra en la Fórmula 38 para extraer el mensaje m del vector de cifrado c_1.

[Fórmula 35]

$$c_1 := \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i \right) + \zeta d_{n+1}$$

donde

$\left(\vec{x}_1, \ldots, \vec{x}_h \right) := \left(\left(x_1, \ldots, x_{\mu_1} \right), \ldots, \left(x_{\mu_{L-1}+1}, \ldots, x_{\mu_h} \right) \right)$: información de atributo,

$\left(\vec{x}_{h+1}, \ldots, \vec{x}_d \right) := \left(\left(x_{\mu_{h+1}+1}, \ldots, x_{\mu_{h+2}} \right), \ldots, \left(x_{\mu_{d-1}+1}, \ldots, x_{\mu_d} \right) \right)$: valores predeterminados.

$\delta_1, \ldots, \delta_d, \zeta$: valores predeterminados,

[Fórmula 36]

$$c_2 := g_T^{\zeta} m$$

donde

$g_T = e(a_i, a_i^*) \neq 1$,

A es una base del espacio **V** y es **A** : = (a_1, …, a_N),

A* es una base del espacio **V*** y es **A*** : = (a^*_1, …, a^*_N).

[Fórmula 37]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{0,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^* \right) + \eta_0 b_{n+1}^* + (1-\eta_0) b_{n+2}^*$$

donde

$\sigma_{0,i}, \eta_0$ (i = 1, …, L): valores predeterminados,

v_i (i = 1, …, μ_L): información de predicado.

[Fórmula 38]

$$m := c_2 / e\left(c_1, k^*_{L,\mathrm{dec}} \right)$$

donde

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*),$$

$$p := \sum_{i=1}^{N} \chi_i b_i ,$$

$$q := \sum_{i=1}^{N} \eta_i b_i^* ,$$

χ_i, η_i: valores predeterminados.

30. El dispositivo de descifrado de la reivindicación 26,

en el que la unidad de entrada de vector introduce el vector de cifrado c_1 como se muestra en la Fórmula 39 y la información de cifrado c_2 como se muestra en la Fórmula 40 en la que se cifra un mensaje m,

en el que la unidad de almacenamiento de vector de clave almacena el vector de clave $k^*_{L,dec}$ como se muestra en la Fórmula 41 y

en el que la unidad de operación de emparejamiento realiza una operación como se muestra en la Fórmula 42 para extraer el mensaje m del vector de cifrado c_1.

[Fórmula 39]

$$c_1 := \sum_{t=1}^{h} \delta_t \left(\sum_{i=1}^{n} x_{t,i} b_i \right) + \zeta d_{n+1}$$

donde

$\left(\vec{x}_1, \ldots, \vec{x}_h \right) := \left(\left(x_{1,1}, \ldots, x_{1,n} \right), \ldots, \left(x_{h,1}, \ldots, x_{h,n} \right) \right)$: información de atributo,

$\delta_1, \ldots, \delta_d, \zeta$: valores predeterminados,

[Fórmula 40]

$$c_2 := g_T^{\zeta} m$$

donde

$g_T = e(a_i, a_i^*) \neq 1$,

A es una base del espacio **V** y es **A** : = (a_1, …, a_N),

A* es una base del espacio **V*** y es **A*** : = (a^*_1, …, a^*_N).

[Fórmula 41]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{\mathrm{dec},t} \left(\sum_{i=1}^{n} v_{t,i} b_i^* \right) + \eta_{\mathrm{dec}} b^*_{n+1} + (1 - \eta_{\mathrm{dec}}) b^*_{n+2}$$

donde

$\sigma_{\mathrm{dec},t}, \eta_{\mathrm{dec}}$ (t = 1, …, L): valores predeterminados,

$v_{t,i}$ (t = 1, …, L; i = 1, …, n): información de predicado.

[Fórmula 42]

$$m := c_2 / e\left(c_1, k^*_{L,\mathrm{dec}} \right)$$

donde

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*),$$

$$p := \sum_{i=1}^{N} \chi_i b_i,$$

$$q := \sum_{i=1}^{N} \eta_i b_i^*,$$

χ_i, η_i: valores predeterminados.

31. Un método de procesamiento criptográfico de realización de un proceso de cifrado de predicado usando espacios de vectores duales de un espacio V y un espacio V* emparejados a través de una operación de emparejamiento mostrada en la Fórmula 44, el método de procesamiento criptográfico que comprende:

generar como un vector de cifrado c_1 un vector de una base B^, la base B^ que tiene, de entre los vectores de base b_i (i = 1, …, n, …, N) (N que es un entero de 3 o mayor y n que es un entero de 1 a N-2) que constituyen una base B predeterminada del espacio V, los vectores de base b_i (i = 1, …, n) y un vector de base d_{n+1} que es una suma de dos o más vectores de base b_i (i = n+1, …, m) de entre los vectores de base b_i (i = n+1, …, N), el

vector de cifrado c_1 que es el vector en el que la información de atributo se incrusta como coeficientes de uno o más vectores de base de entre el vector de base b_i (i = 1, …, n) e información predeterminada se incrusta como un coeficiente del vector de base d_{n+1}; y

realizar la operación de emparejamiento $e(c_1, k^*_{L,dec})$ mostrada en la Fórmula 44 sobre el vector de cifrado c_1 generado y un vector de clave $k^*_{L,dec}$ para descifrar el vector de cifrado c_1 y para extraer un valor que concierne a la información predeterminada, el vector de clave $k^*_{L,dec}$ que es un vector de una base B* del espacio V* y construido de manera que una información de predicado se incrusta como coeficientes de uno o más vectores de base de los vectores de base b^*_i (i = 1, …, n) de entre los vectores de base b^*_i (i = 1, …, n, …, N) que constituyen la base B* y coeficientes de vectores de base b^*_i (i = n+1, …, m) de la base B* se incrustan de manera que una suma de los coeficientes de los vectores de base b^*_i (i = n+1, …, m) es 1.

[Fórmula 44]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

donde

$$p := \sum_{i=1}^{N} \chi_i b_i ,$$

$$q := \sum_{i=1}^{N} \eta_i b_i^* ,$$

χ_i, η_i: valores predeterminados.

32. Un programa de procesamiento criptográfico que realiza un proceso de cifrado de predicado usando espacios de vectores duales de un espacio V y un espacio V* emparejados a través de una operación de emparejamiento mostrada en la Fórmula 45, el programa de procesamiento criptográfico que hace a un ordenador ejecutar:

un proceso de cifrado que genera como un vector de cifrado c_1 un vector de una base B^, la base B^ que tiene, de entre los vectores de base b_i (i = 1, …, n, …, N) (N que es un entero de 3 o mayor y n que es un entero de 1 a N-2) que constituyen una base B predeterminada del espacio V, los vectores de base b_i (i = 1, …, n) y un vector de base d_{n+1} que es una suma de dos o más vectores de base b_i (i = n+1, …, m) de entre los vectores de base b_i (i = n+1, …, N), el vector de cifrado c_1 que es el vector en el que la información de atributo se incrusta como coeficientes de uno o más vectores de base de entre los vectores de base b_i (i = 1, …, n) e información predeterminada se incrusta como un coeficiente del vector de base d_{n+1}; y

un proceso de descifrado que realiza la operación de emparejamiento $e(c_1, k^*_{L,dec})$ mostrada en la Fórmula 45 sobre el vector de cifrado c_1 generado por el dispositivo de cifrado y un vector de clave $k^*_{L,dec}$ para descifrar el vector de cifrado c_1 y para extraer un valor que concierne a la información predeterminada, el vector de clave $k^*_{L,dec}$ que es un vector de una base B* del espacio V* y construido de manera que la información de predicado se incrusta como coeficientes de uno o más vectores de base de los vectores de base b^*_i (i = 1, …, n) de entre los vectores de base b^*_i (i = 1, …, n, …, N) que constituyen la base B* y coeficientes de vectores de base b^*_i (i = n+1, …, m) de la base B* se incrustan de manera que una suma de los coeficientes de los vectores de base b^*_i (i = n+1, …, m) es 1.

[Fórmula 45]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

donde

$$p := \sum_{i=1}^{N} \chi_i b_i ,$$

$$q := \sum_{i=1}^{N} \eta_i b_i^* ,$$

χ_i, η_i: valores predeterminados.

Fig. 1

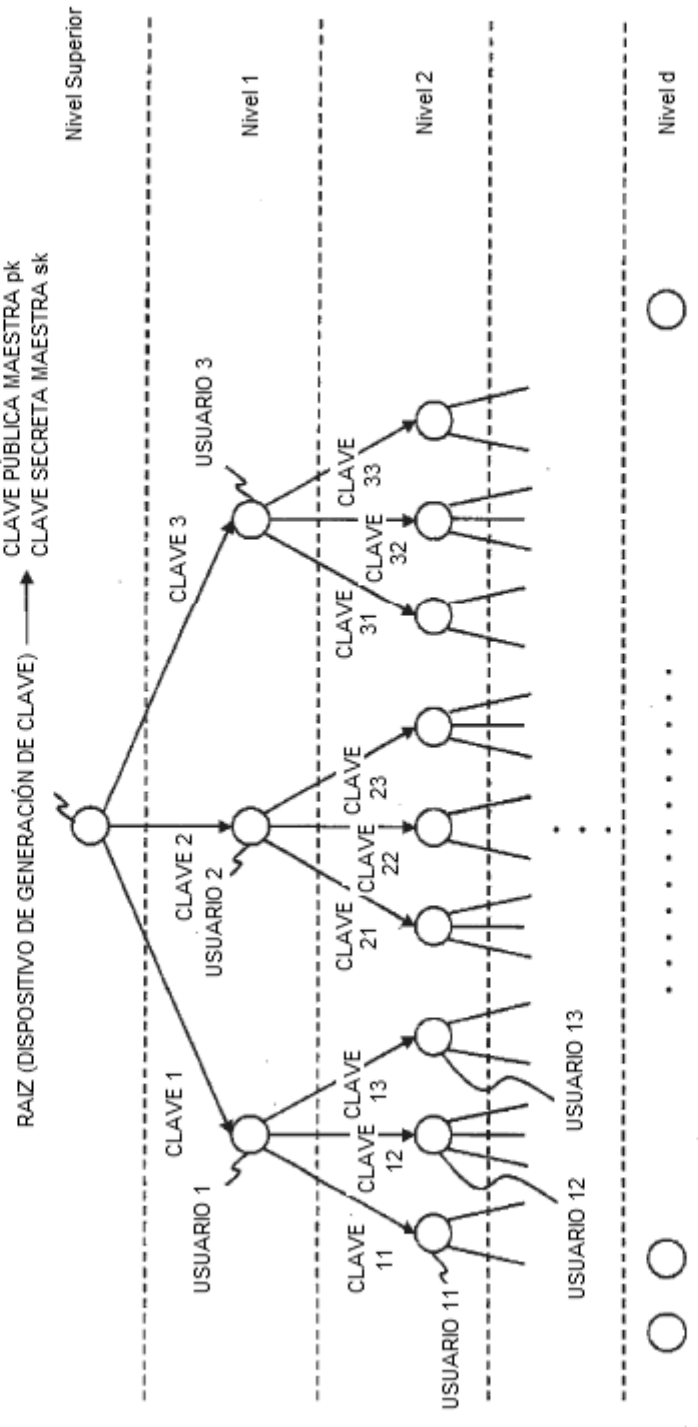

RAIZ (DISPOSITIVO DE GENERACIÓN DE CLAVE)
CLAVE PÚBLICA MAESTRA pk
CLAVE SECRETA MAESTRA sk
Nivel Superior
Nivel 1
Nivel 2
Nivel d
CLAVE 1
CLAVE 2
CLAVE 3
USUARIO 1
USUARIO 2
USUARIO 3
CLAVE 11
CLAVE 12
CLAVE 13
CLAVE 21
CLAVE 22
CLAVE 23
CLAVE 31
CLAVE 32
CLAVE 33
USUARIO 11
USUARIO 12
USUARIO 13

Fig. 2

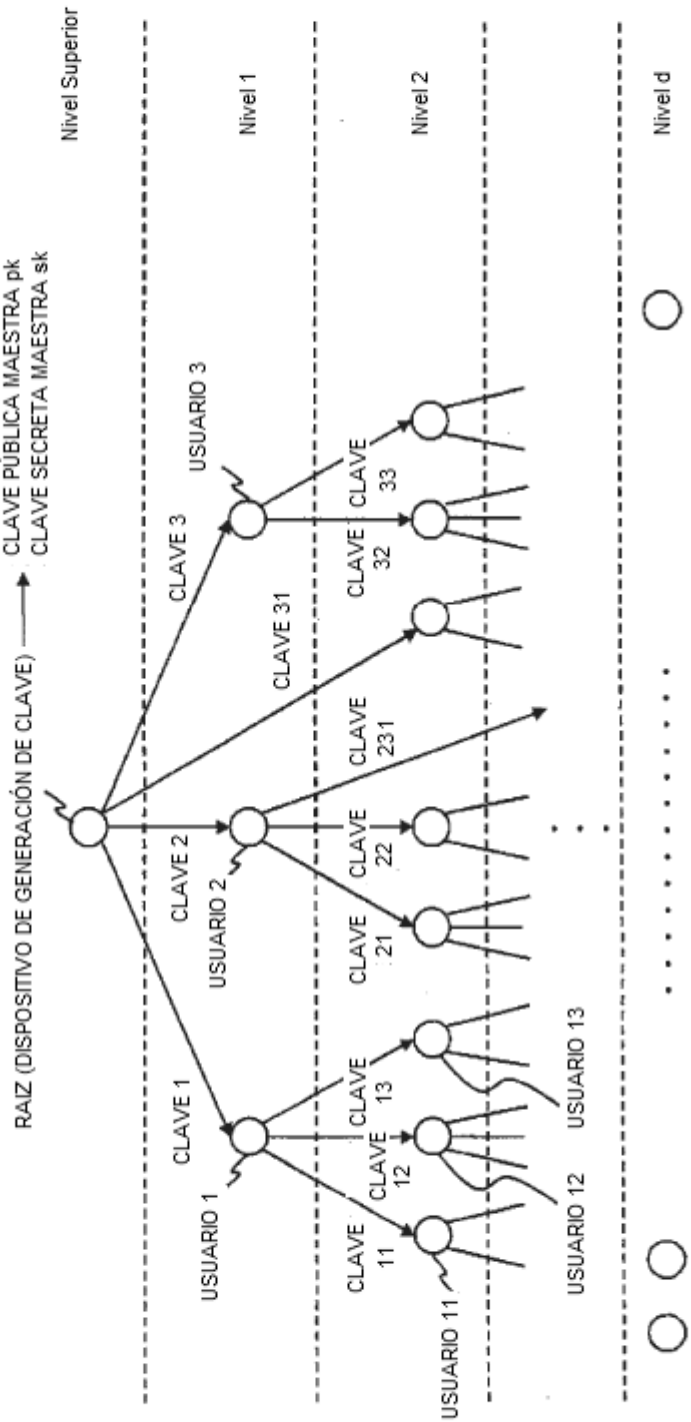

RAIZ (DISPOSITIVO DE GENERACIÓN DE CLAVE)
CLAVE PÚBLICA MAESTRA pk
CLAVE SECRETA MAESTRA sk
Nivel Superior
Nivel 1
Nivel 2
Nivel d
CLAVE 1
CLAVE 2
CLAVE 3
USUARIO 1
USUARIO 2
USUARIO 3
CLAVE 11
CLAVE 12
CLAVE 13
CLAVE 21
CLAVE 22
CLAVE 231
CLAVE 31
CLAVE 32
CLAVE 33
USUARIO 11
USUARIO 12
USUARIO 13

Fig. 3

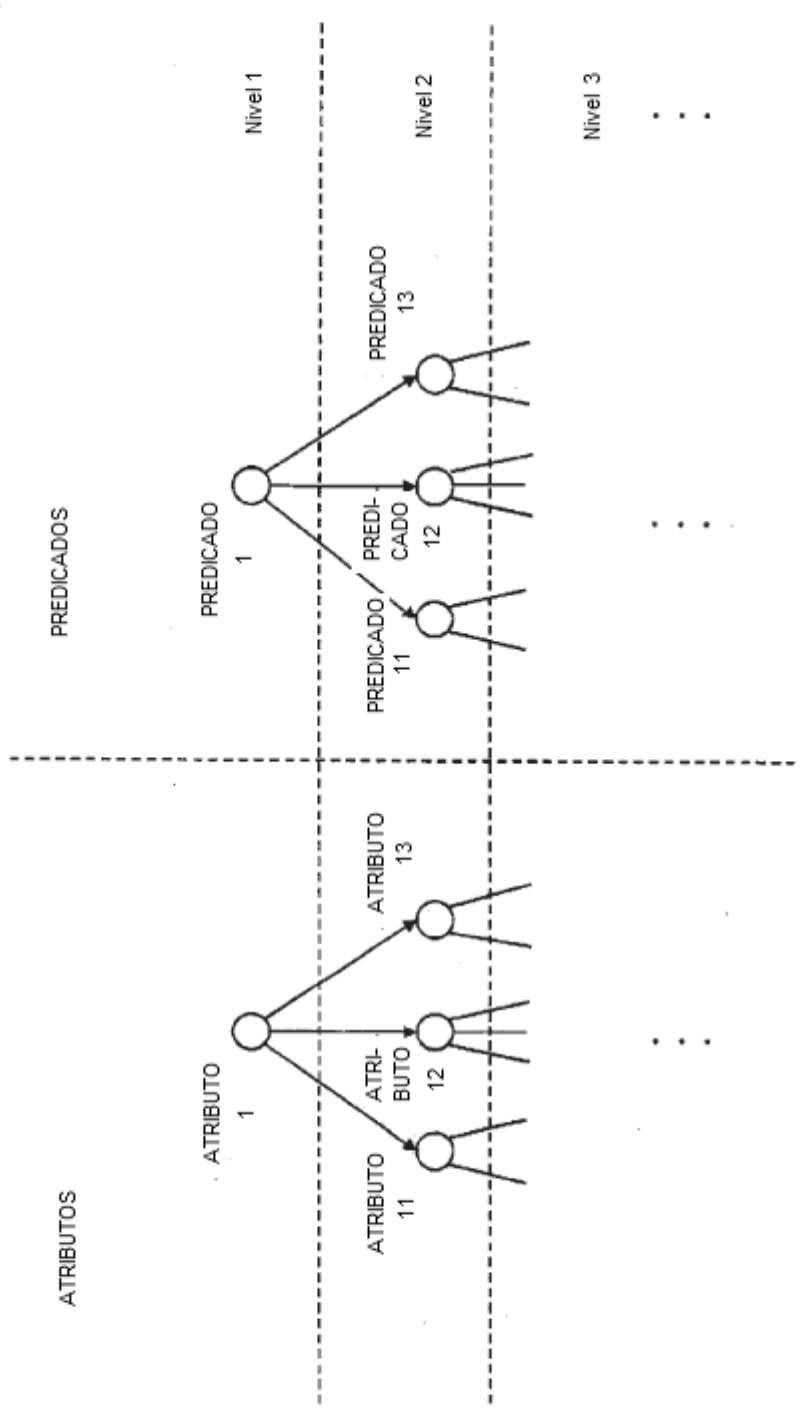

PREDICADOS
ATRIBUTOS
Nivel 1
Nivel 2
Nivel 3
PREDICADO 1
PREDICADO 11
PREDI-CADO 12
PREDICADO 13
ATRIBUTO 1
ATRIBUTO 11
ATRI-BUTO 12
ATRIBUTO 13

Fig. 4

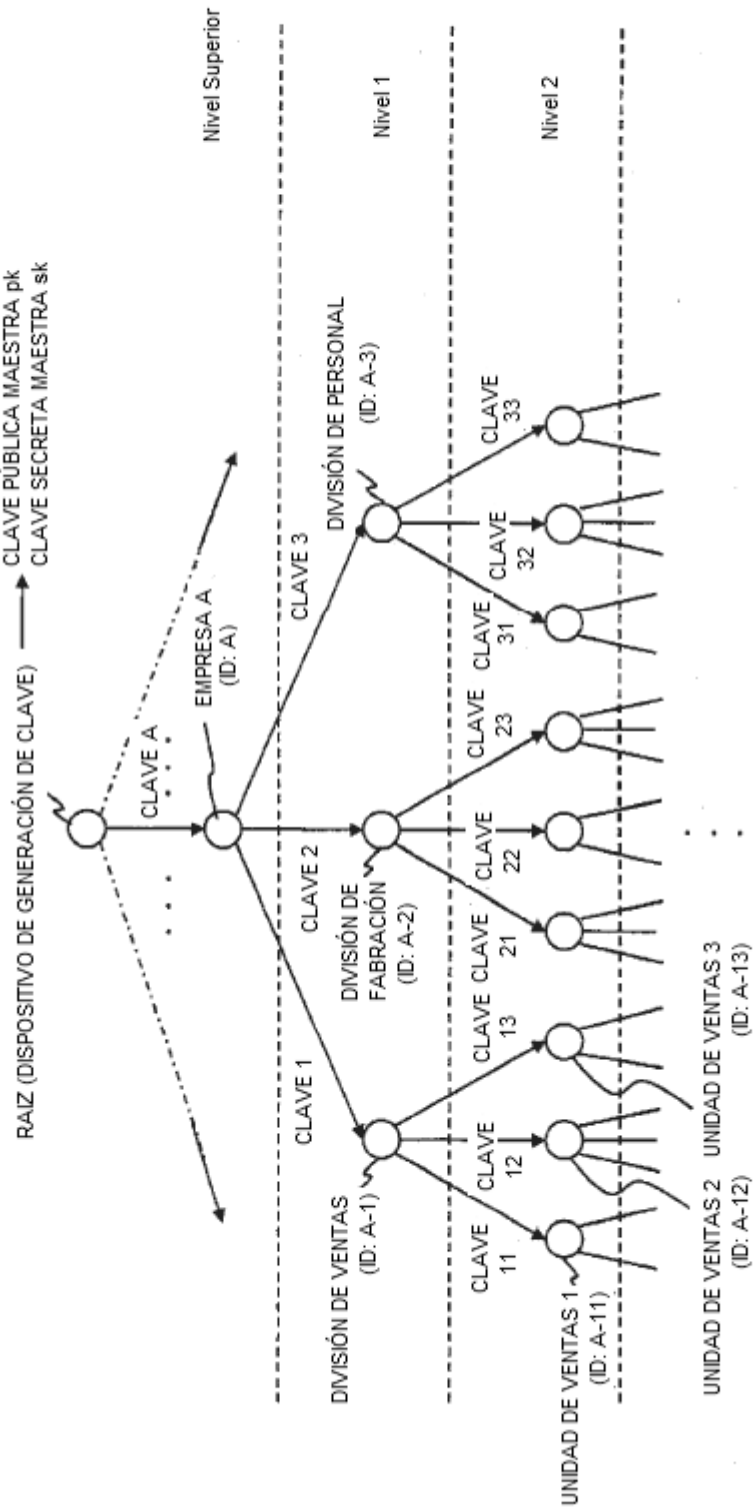

RAIZ (DISPOSITIVO DE GENERACIÓN DE CLAVE)
CLAVE PÚBLICA MAESTRA pk
CLAVE SECRETA MAESTRA sk
Nivel Superior
CLAVE A
EMPRESA A
(ID: A)
CLAVE 1
CLAVE 2
CLAVE 3
DIVISIÓN DE VENTAS
(ID: A-1)
DIVISIÓN DE
FABRACIÓN
(ID: A-2)
DIVISIÓN DE PERSONAL
(ID: A-3)
Nivel 1
Nivel 2
CLAVE
11
CLAVE
12
CLAVE
13
CLAVE
21
CLAVE
22
CLAVE
23
CLAVE
31
CLAVE
32
CLAVE
33
UNIDAD DE VENTAS 1
(ID: A-11)
UNIDAD DE VENTAS 2
(ID: A-12)
UNIDAD DE VENTAS 3
(ID: A-13)

Fig. 5

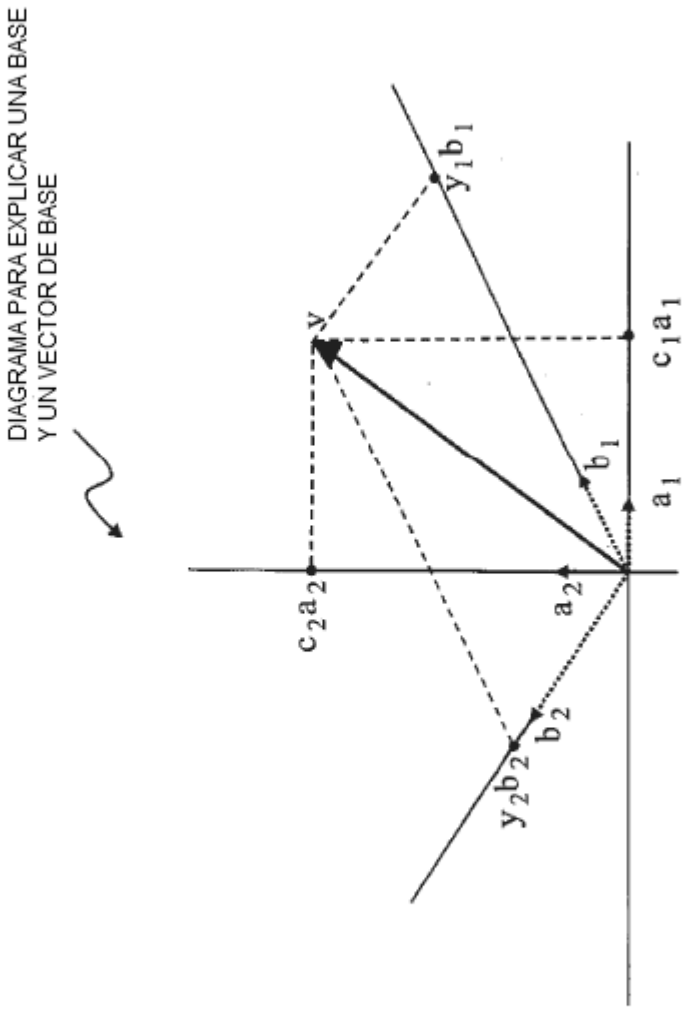


DIAGRAMA PARA EXPLICAR UNA BASE
Y UN VECTOR DE BASE
y
y_1b_1
c_1a_1
b_1
a_1
c_2a_2
a_2
b_2
y_2b_2

Fig. 6

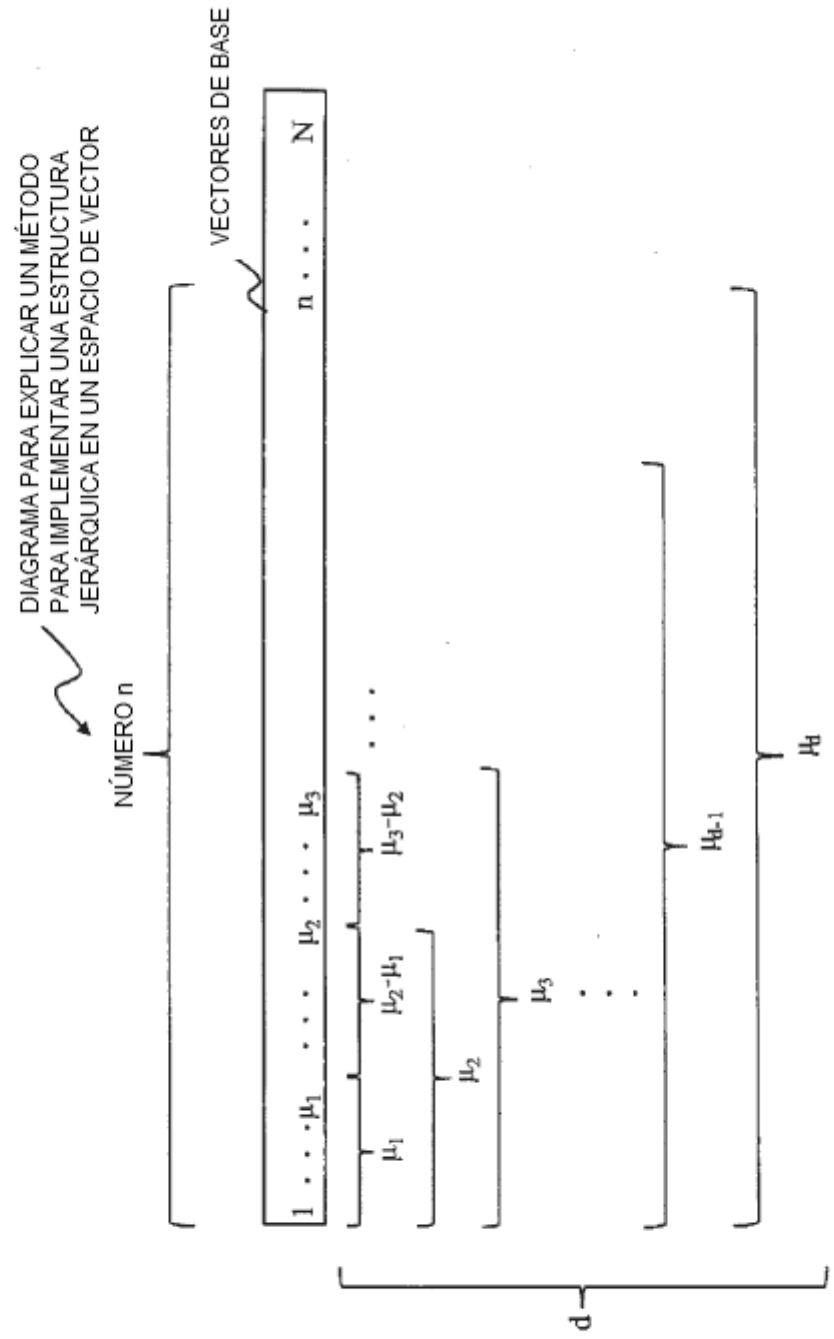


DIAGRAMA PARA EXPLICAR UN MÉTODO PARA IMPLEMENTAR UNA ESTRUCTURA JERÁRQUICA EN UN ESPACIO DE VECTOR
NÚMERO n
VECTORES DE BASE
1 . . . μ1 . . . μ2 . . . μ3 n . . . N
μ1
μ2-μ1
μ3-μ2
μ2
μ3
μH-1
μH
d

Fig. 7

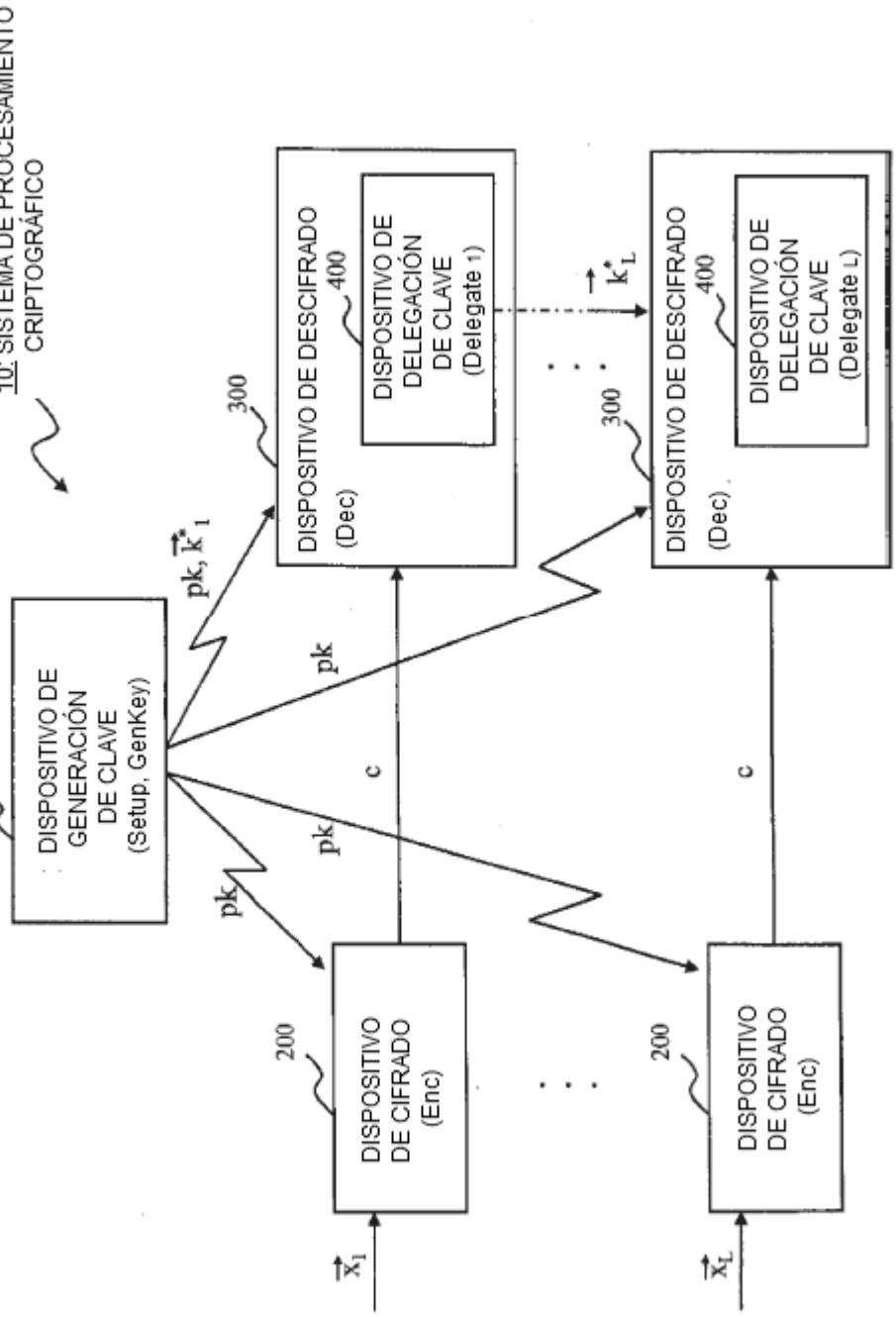

10: SISTEMA DE PROCESAMIENTO CRIPTOGRÁFICO
100
DISPOSITIVO DE GENERACIÓN DE CLAVE (Setup, GenKey)
pk
pk
pk
c
c
pk, $\vec{k}_1$
300
DISPOSITIVO DE DESCIFRADO (Dec)
400
DISPOSITIVO DE DELEGACIÓN DE CLAVE (Delegate 1)
300
DISPOSITIVO DE DESCIFRADO (Dec)
400
DISPOSITIVO DE DELEGACIÓN DE CLAVE (Delegate L)
$\vec{k}_L$
200
DISPOSITIVO DE CIFRADO (Enc)
200
DISPOSITIVO DE CIFRADO (Enc)
$\vec{x}_1$
$\vec{x}_L$

Fig. 8

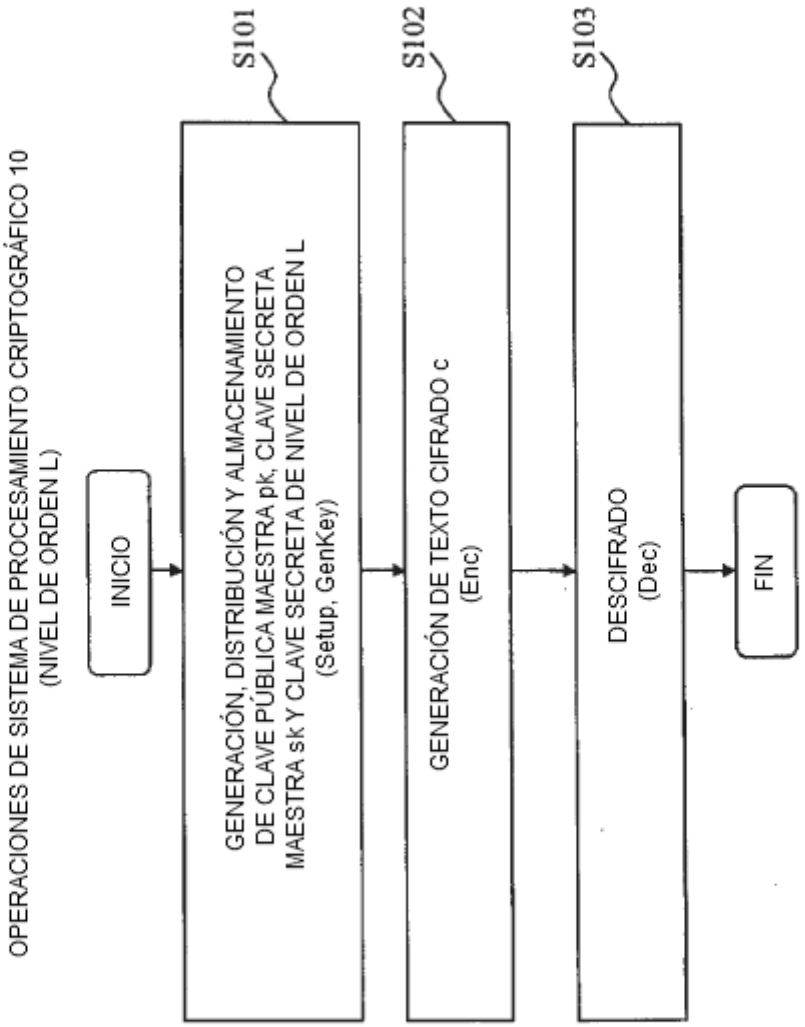

OPERACIONES DE SISTEMA DE PROCESAMIENTO CRIPTOGRÁFICO 10
(NIVEL DE ORDEN L)
INICIO
S101
GENERACIÓN, DISTRIBUCIÓN Y ALMACENAMIENTO DE CLAVE PÚBLICA MAESTRA pk, CLAVE SECRETA MAESTRA sk Y CLAVE SECRETA DE NIVEL DE ORDEN L
(Setup, GenKey)
S102
GENERACIÓN DE TEXTO CIFRADO c
(Enc)
S103
DESCIFRADO
(Dec)
FIN

Fig. 9

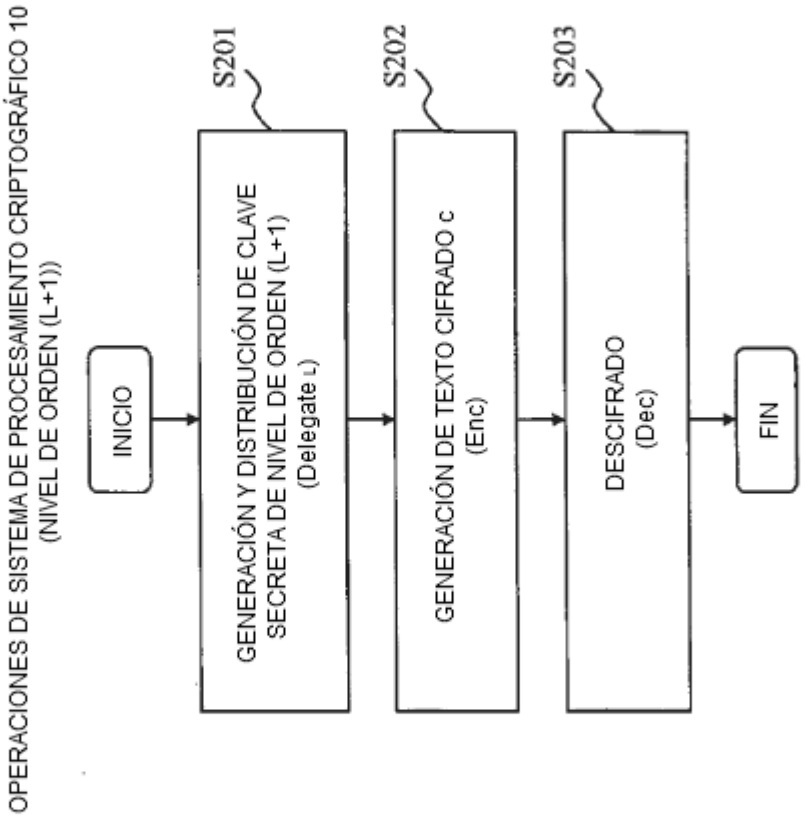

OPERACIONES DE SISTEMA DE PROCESAMIENTO CRIPTOGRÁFICO 10
(NIVEL DE ORDEN (L+1))
INICIO
S201
GENERACIÓN Y DISTRIBUCIÓN DE CLAVE SECRETA DE NIVEL DE ORDEN (L+1)
(Delegate L)
S202
GENERACIÓN DE TEXTO CIFRADO c
(Enc)
S203
DESCIFRADO
(Dec)
FIN

Fig. 10

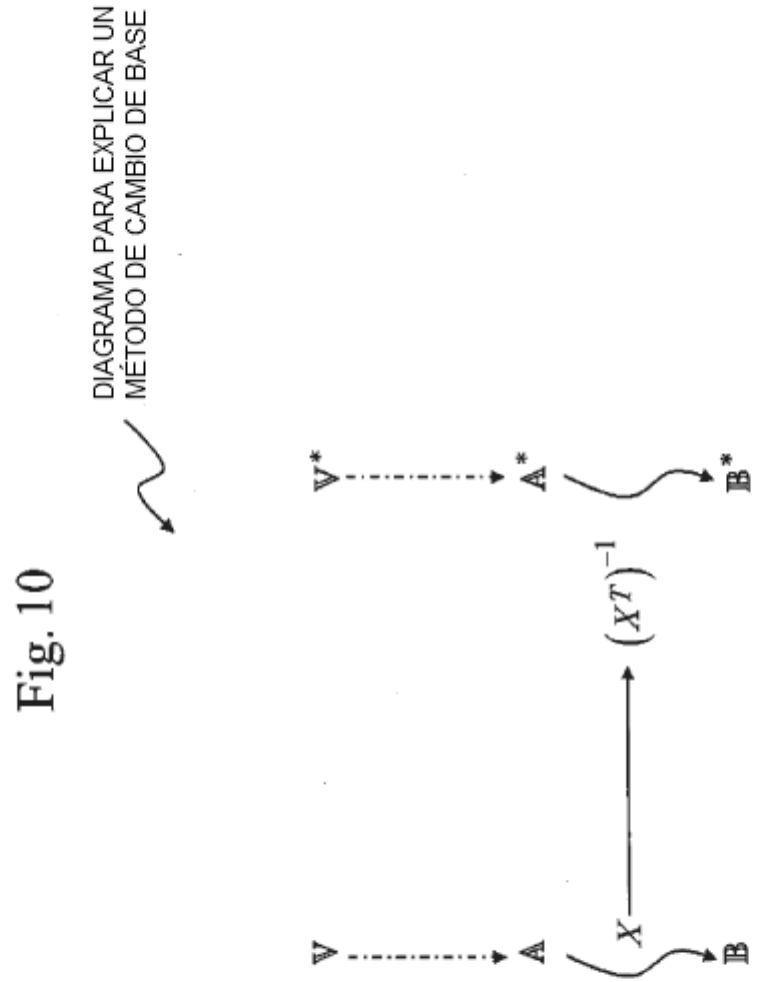


DIAGRAMA PARA EXPLICAR UN MÉTODO DE CAMBIO DE BASE
V
A
B
X
$(X^T)^{-1}$
V*
A*
B*

Fig. 11

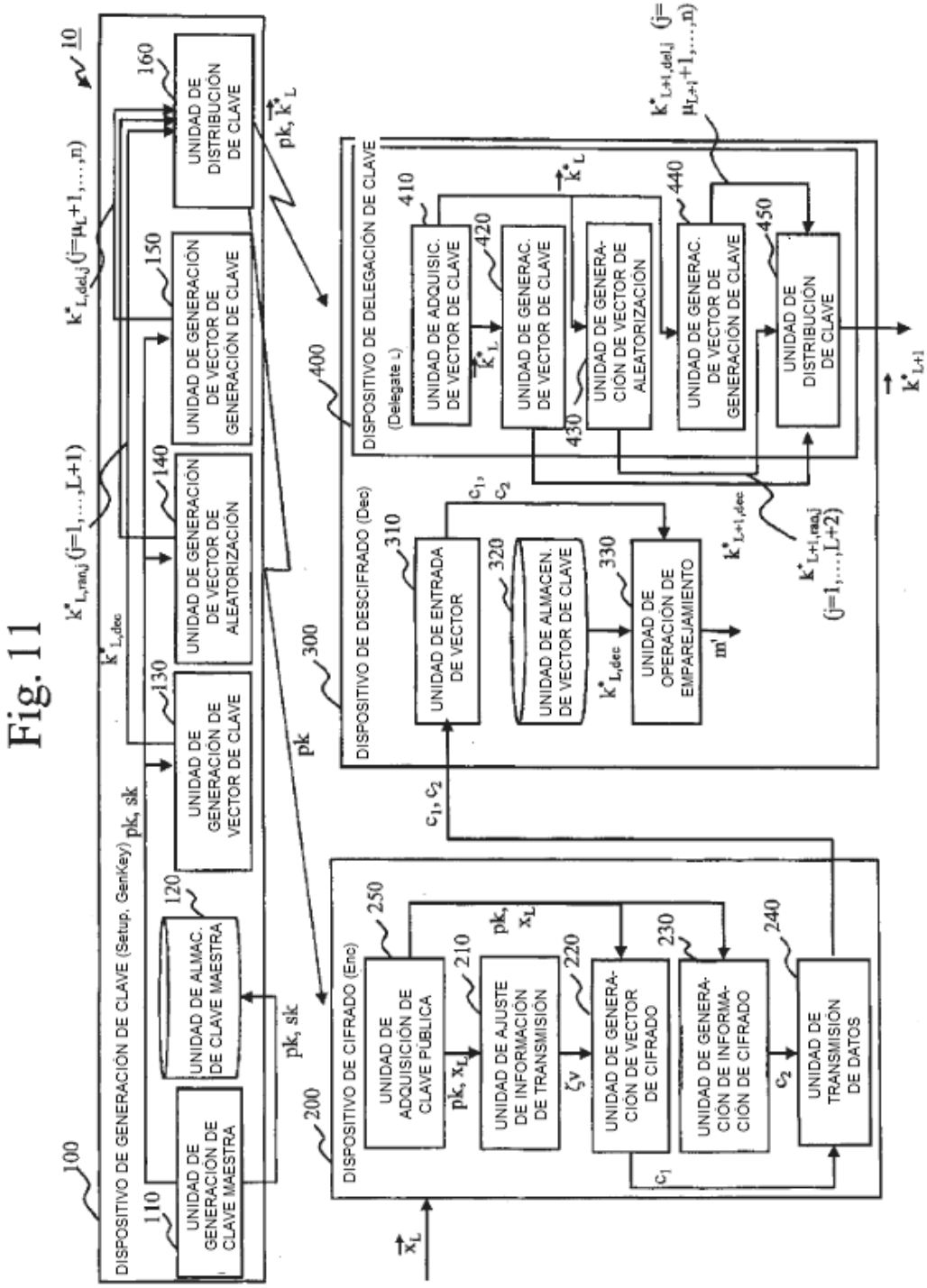

DISPOSITIVO DE GENERACIÓN DE CLAVE (Setup, GenKey)
UNIDAD DE GENERACIÓN DE CLAVE MAESTRA
UNIDAD DE ALMAC. DE CLAVE MAESTRA
UNIDAD DE GENERACIÓN DE VECTOR DE CLAVE
UNIDAD DE GENERACIÓN DE ALEATORIZACIÓN
UNIDAD DE GENERACIÓN DE VECTOR DE GENERACIÓN DE CLAVE
UNIDAD DE DISTRIBUCIÓN DE CLAVE
DISPOSITIVO DE CIFRADO (Enc)
UNIDAD DE ADQUISICIÓN DE CLAVE PÚBLICA
UNIDAD DE AJUSTE DE INFORMACIÓN DE TRANSMISIÓN
UNIDAD DE GENERACIÓN DE VECTOR DE CIFRADO
UNIDAD DE GENERACIÓN DE INFORMACIÓN DE CIFRADO
UNIDAD DE TRANSMISIÓN DE DATOS
DISPOSITIVO DE DESCIFRADO (Dec)
UNIDAD DE ENTRADA DE VECTOR
UNIDAD DE ALMACEN. DE VECTOR DE CLAVE
UNIDAD DE OPERACIÓN DE EMPAREJAMIENTO
DISPOSITIVO DE DELEGACIÓN DE CLAVE (Delegate)
UNIDAD DE ADQUISIC. DE VECTOR DE CLAVE
UNIDAD DE GENERAC. DE VECTOR DE CLAVE
UNIDAD DE GENERACIÓN DE VECTOR DE ALEATORIZACIÓN
UNIDAD DE GENERAC. DE VECTOR DE GENERACIÓN DE CLAVE
UNIDAD DE DISTRIBUCIÓN DE CLAVE
pk, sk
pk
pk, k*L
k*L,deL,j (j=μL+1,...,n)
k*L,ranj (j=1,...,L+1)
k*L,dec
k*L
k*L+1,delj (j=μL+1,...,n)
k*L+1,ranj (j=1,...,L+2)
k*L+1,dec
k*L+1
c1, c2
m'
xL
pk, xL
ζv
c1
c2
100
110
120
130
140
150
160
200
210
220
230
240
250
300
310
320
330
400
410
420
430
440
450

Fig. 12

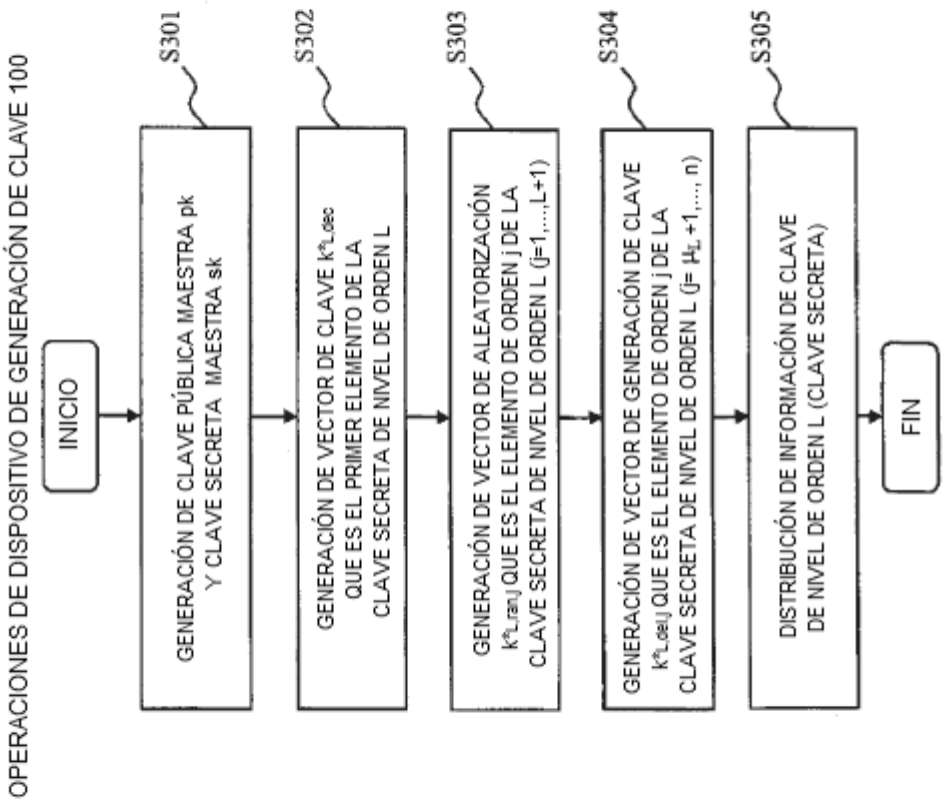

OPERACIONES DE DISPOSITIVO DE GENERACIÓN DE CLAVE 100
INICIO
S301
GENERACIÓN DE CLAVE PÚBLICA MAESTRA pk
Y CLAVE SECRETA MAESTRA sk
S302
GENERACIÓN DE VECTOR DE CLAVE k*L,dec
QUE ES EL PRIMER ELEMENTO DE LA
CLAVE SECRETA DE NIVEL DE ORDEN L
S303
GENERACIÓN DE VECTOR DE ALEATORIZACIÓN
k*L,ranj QUE ES EL ELEMENTO DE ORDEN j DE LA
CLAVE SECRETA DE NIVEL DE ORDEN L (j=1,...,L+1)
S304
GENERACIÓN DE VECTOR DE GENERACIÓN DE CLAVE
k*L,decj QUE ES EL ELEMENTO DE ORDEN j DE LA
CLAVE SECRETA DE NIVEL DE ORDEN L (j= μL +1,..., n)
S305
DISTRIBUCIÓN DE INFORMACIÓN DE CLAVE
DE NIVEL DE ORDEN L (CLAVE SECRETA)
FIN

Fig. 13

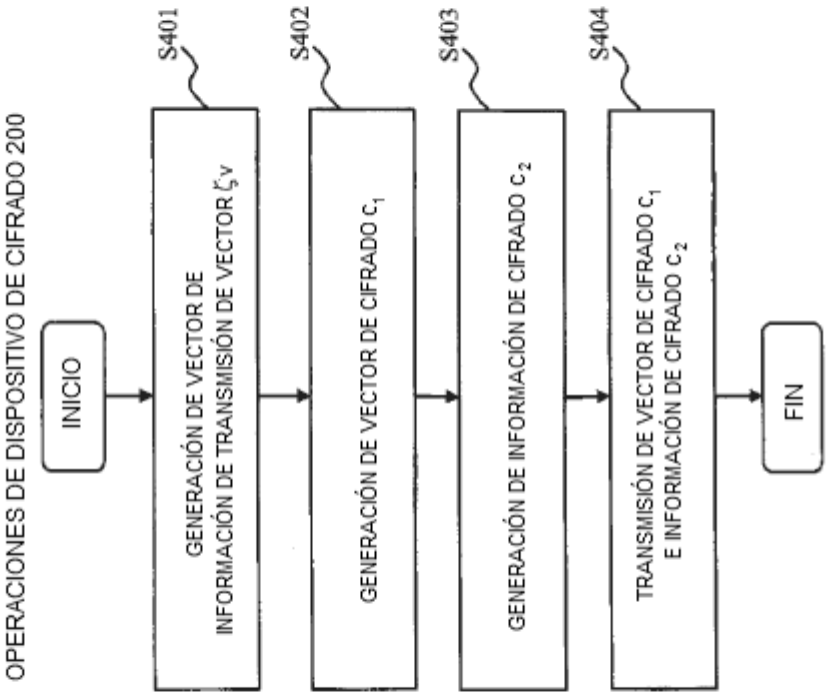

OPERACIONES DE DISPOSITIVO DE CIFRADO 200
INICIO
S401
GENERACIÓN DE VECTOR DE INFORMACIÓN DE TRANSMISIÓN DE VECTOR ζv
S402
GENERACIÓN DE VECTOR DE CIFRADO c1
S403
GENERACIÓN DE INFORMACIÓN DE CIFRADO c2
S404
TRANSMISIÓN DE VECTOR DE CIFRADO c1 E INFORMACIÓN DE CIFRADO c2
FIN

Fig. 14

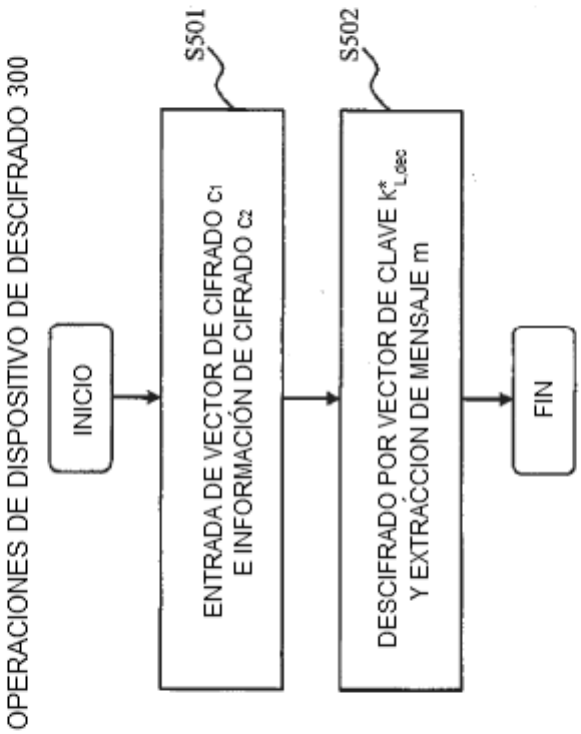

OPERACIONES DE DISPOSITIVO DE DESCIFRADO 300
INICIO
S501
ENTRADA DE VECTOR DE CIFRADO c1
E INFORMACIÓN DE CIFRADO c2
S502
DESCIFRADO POR VECTOR DE CLAVE k*Ldec
Y EXTRACCION DE MENSAJE m
FIN

Fig. 15

OPERACIONES DE DISPOSITIVO DE DELEGACIÓN DE CLAVE 400

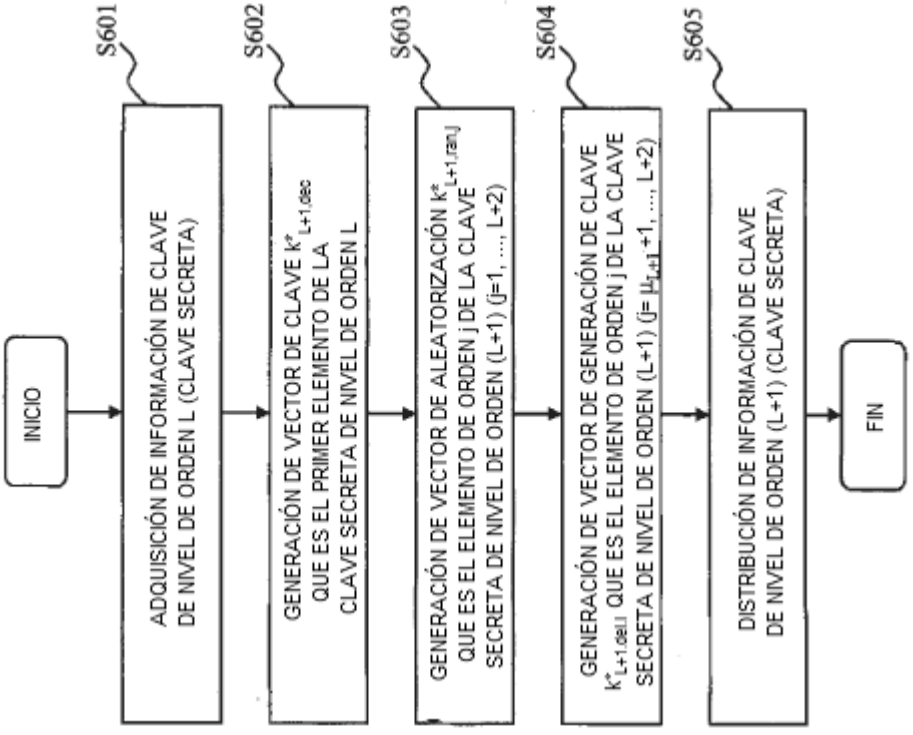


Fig. 16

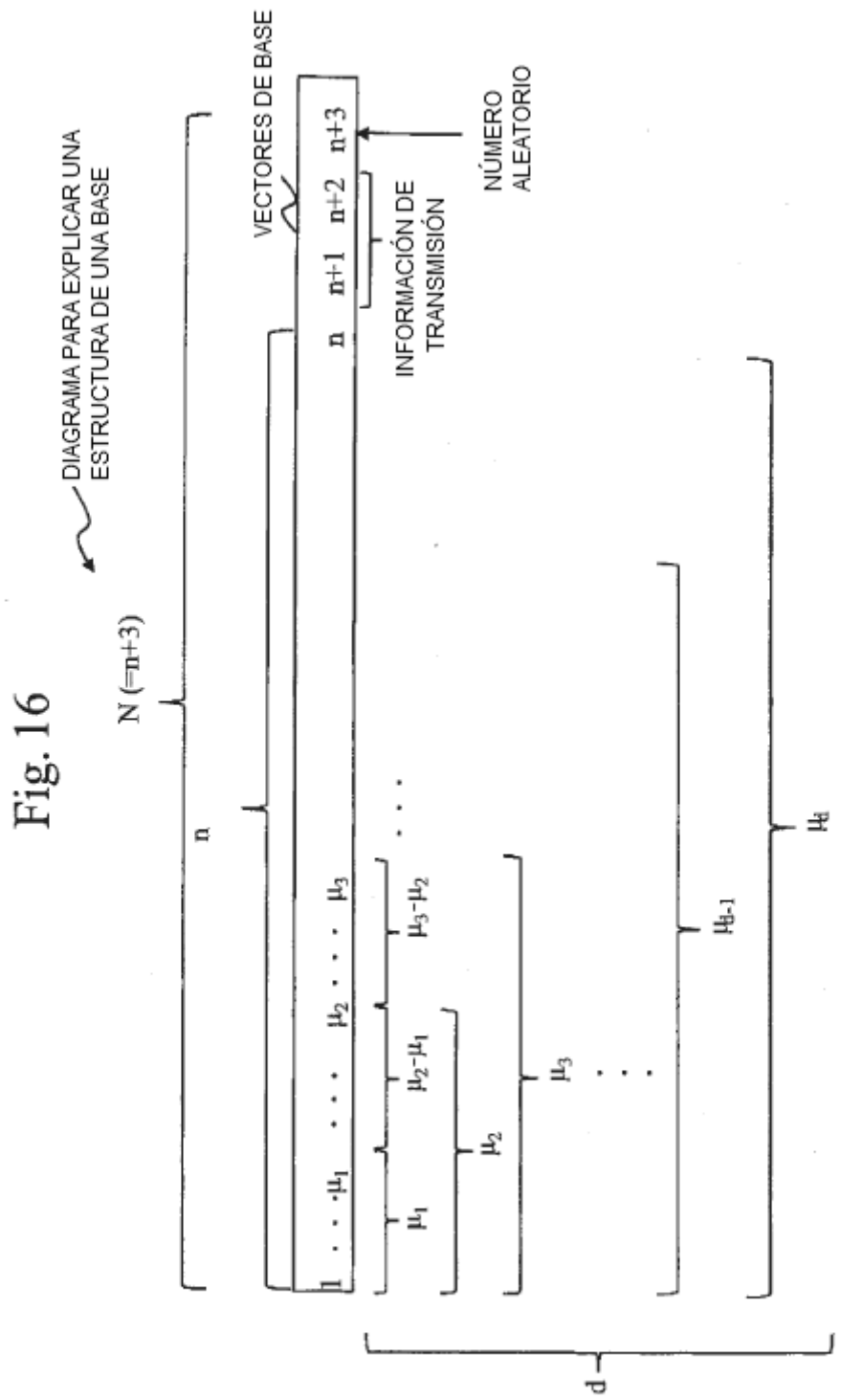


DIAGRAMA PARA EXPLICAR UNA ESTRUCTURA DE UNA BASE
N (=n+3)
n
VECTORES DE BASE
n n+1 n+2 n+3
INFORMACIÓN DE TRANSMISIÓN
NÚMERO ALEATORIO
1 . . . μ1 . . . . μ2 . . . . μ3
μ1
μ2-μ1
μ3-μ2
μ2
μ3
μd-1
μd
d

Fig. 17

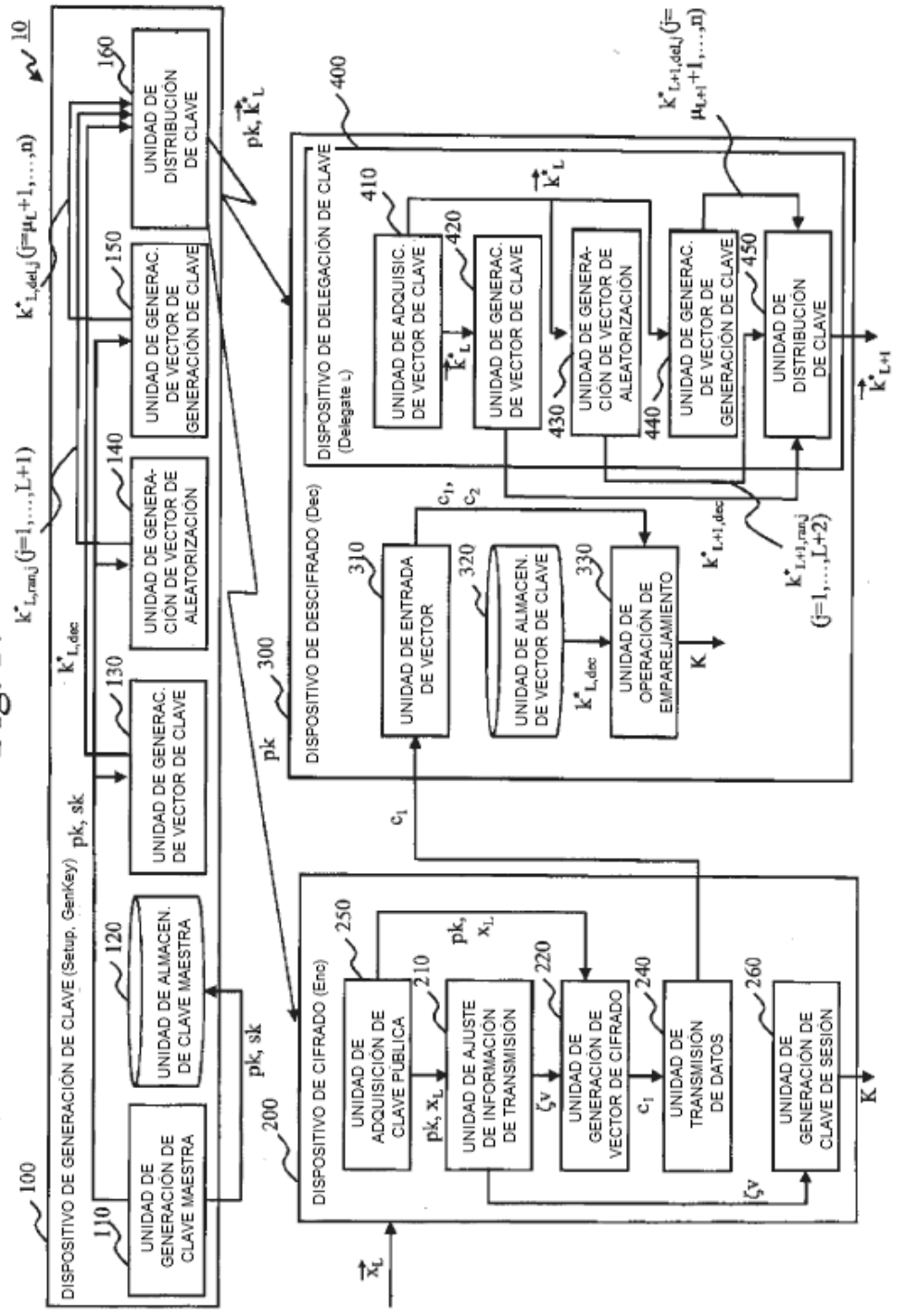

DISPOSITIVO DE GENERACIÓN DE CLAVE (Setup, GenKey)
UNIDAD DE GENERACIÓN DE CLAVE MAESTRA
UNIDAD DE ALMACEN. DE CLAVE MAESTRA
UNIDAD DE GENERAC. DE VECTOR DE CLAVE
UNIDAD DE GENERA-CIÓN DE VECTOR DE ALEATORIZACIÓN
UNIDAD DE GENERAC. DE VECTOR DE GENERACIÓN DE CLAVE
UNIDAD DE DISTRIBUCIÓN DE CLAVE
DISPOSITIVO DE CIFRADO (Enc)
UNIDAD DE ADQUISICIÓN DE CLAVE PÚBLICA
UNIDAD DE AJUSTE DE INFORMACIÓN DE TRANSMISIÓN
UNIDAD DE GENERACIÓN DE VECTOR DE CIFRADO
UNIDAD DE TRANSMISIÓN DE DATOS
UNIDAD DE GENERACIÓN DE CLAVE DE SESIÓN
DISPOSITIVO DE DESCIFRADO (Dec)
UNIDAD DE ENTRADA DE VECTOR
UNIDAD DE ALMACEN. DE VECTOR DE CLAVE
UNIDAD DE OPERACIÓN DE EMPAREJAMIENTO
DISPOSITIVO DE DELEGACIÓN DE CLAVE (Delegate L)
UNIDAD DE ADQUISIC. DE VECTOR DE CLAVE
UNIDAD DE GENERAC. DE VECTOR DE CLAVE
UNIDAD DE GENERA-CIÓN DE VECTOR DE ALEATORIZACIÓN
UNIDAD DE GENERAC. DE VECTOR DE GENERACIÓN DE CLAVE
UNIDAD DE DISTRIBUCIÓN DE CLAVE
pk, sk
pk
pk, x_L
ζv
c_1
c_2
K

Fig. 18

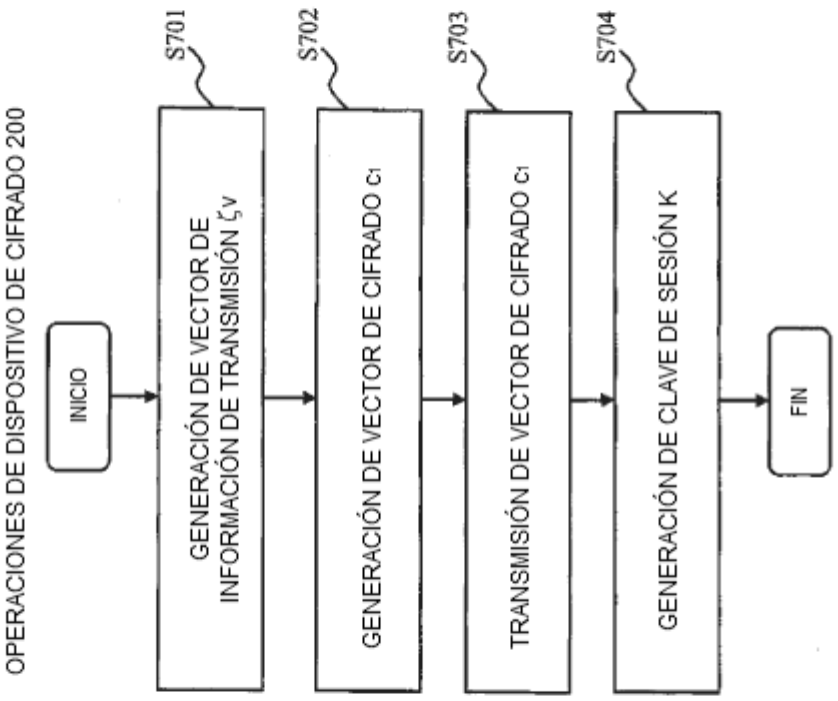

OPERACIONES DE DISPOSITIVO DE CIFRADO 200
INICIO
S701
GENERACIÓN DE VECTOR DE INFORMACIÓN DE TRANSMISIÓN ζv
S702
GENERACIÓN DE VECTOR DE CIFRADO c1
S703
TRANSMISIÓN DE VECTOR DE CIFRADO c1
S704
GENERACIÓN DE CLAVE DE SESIÓN K
FIN

Fig. 19

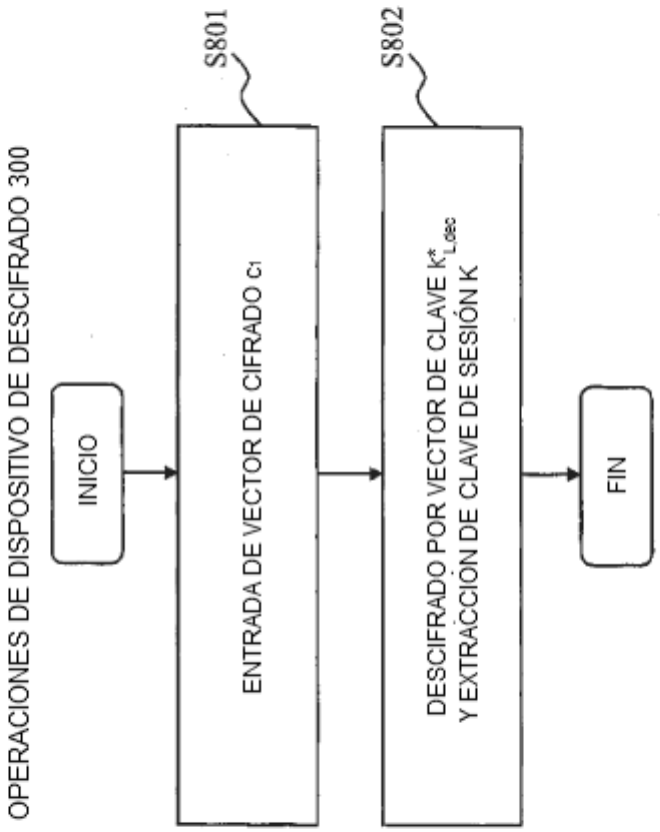

OPERACIONES DE DISPOSITIVO DE DESCIFRADO 300
INICIO
S801
ENTRADA DE VECTOR DE CIFRADO c1
S802
DESCIFRADO POR VECTOR DE CLAVE K*L,dec
Y EXTRACCIÓN DE CLAVE DE SESIÓN K
FIN

Fig. 20

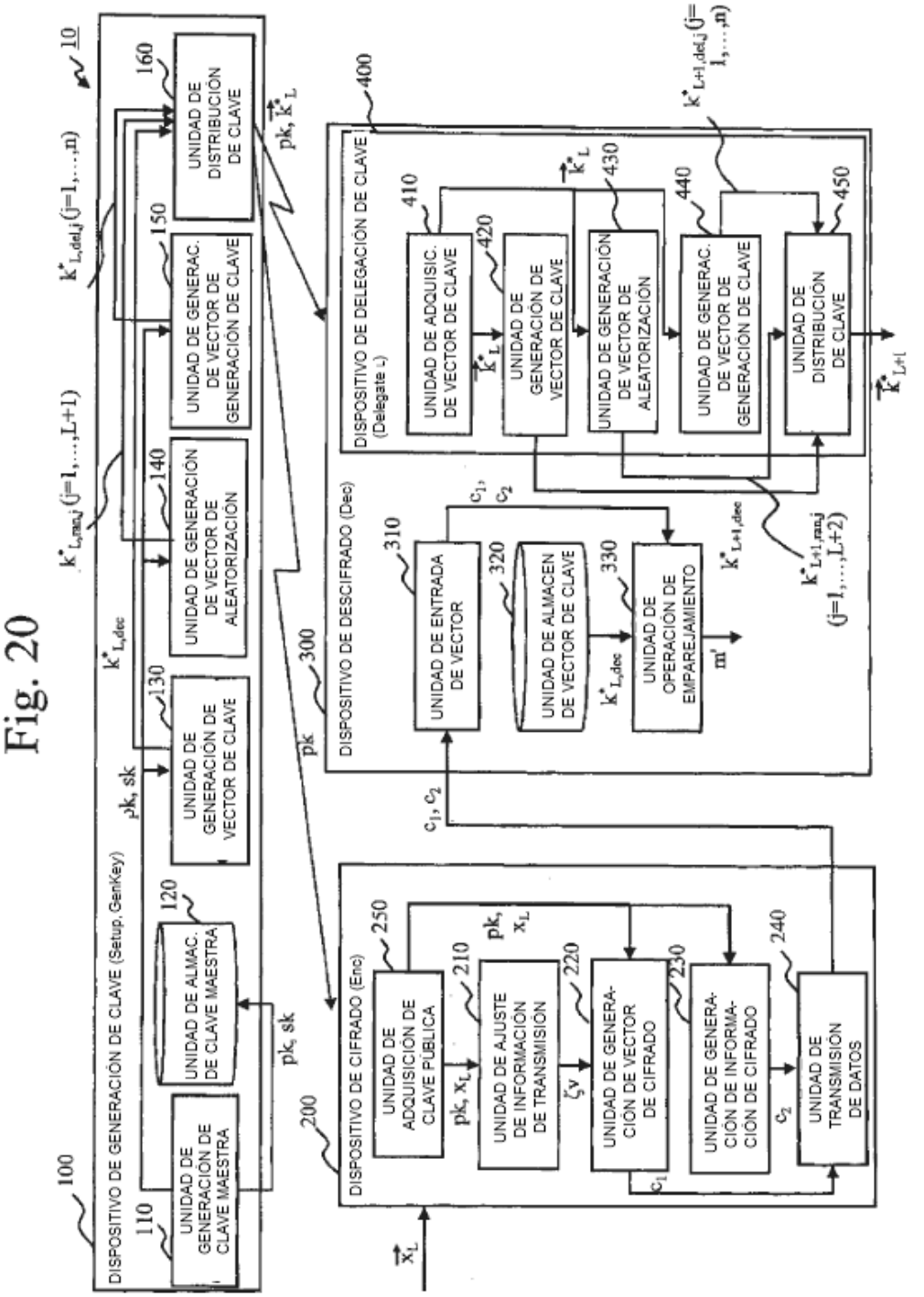
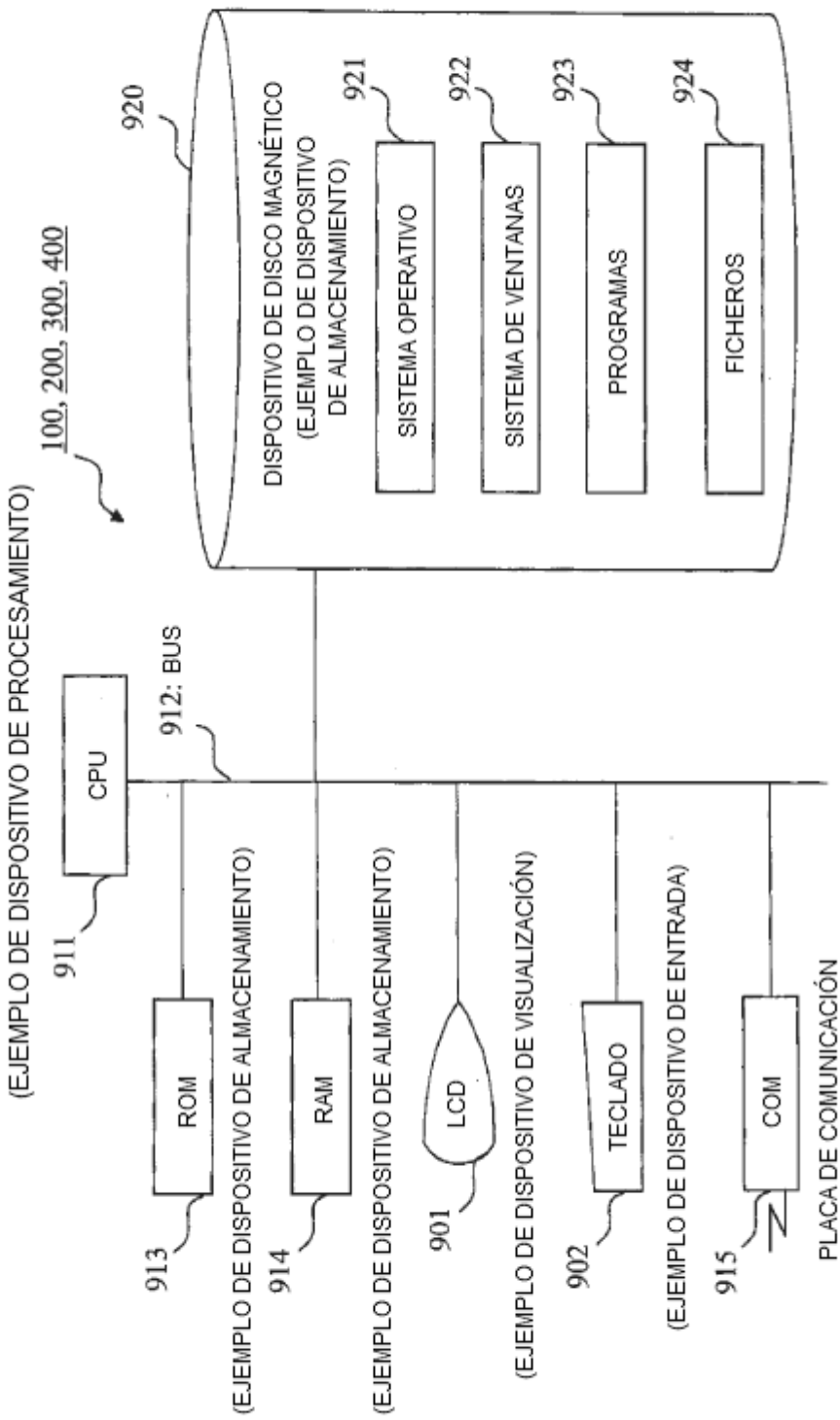

DISPOSITIVO DE GENERACIÓN DE CLAVE (Setup, GenKey)
UNIDAD DE GENERACIÓN DE CLAVE MAESTRA
UNIDAD DE ALMAC. DE CLAVE MAESTRA
UNIDAD DE GENERACIÓN DE VECTOR DE CLAVE
UNIDAD DE GENERACIÓN DE VECTOR DE ALEATORIZACIÓN
UNIDAD DE GENERAC. DE VECTOR DE GENERACIÓN DE CLAVE
UNIDAD DE DISTRIBUCIÓN DE CLAVE
DISPOSITIVO DE CIFRADO (Enc)
UNIDAD DE ADQUISICIÓN DE CLAVE PÚBLICA
UNIDAD DE AJUSTE DE INFORMACIÓN DE TRANSMISIÓN
UNIDAD DE GENERACIÓN DE VECTOR DE CIFRADO
UNIDAD DE GENERACIÓN DE INFORMACIÓN DE CIFRADO
UNIDAD DE TRANSMISIÓN DE DATOS
DISPOSITIVO DE DESCIFRADO (Dec)
UNIDAD DE ENTRADA DE VECTOR
UNIDAD DE ALMACEN DE VECTOR DE CLAVE
UNIDAD DE OPERACIÓN DE EMPAREJAMIENTO
DISPOSITIVO DE DELEGACIÓN DE CLAVE (Delegate -)
UNIDAD DE ADQUISIC. DE VECTOR DE CLAVE
UNIDAD DE GENERACIÓN DE VECTOR DE CLAVE
UNIDAD DE GENERACIÓN DE VECTOR DE ALEATORIZACIÓN
UNIDAD DE GENERAC. DE VECTOR DE GENERACIÓN DE CLAVE
UNIDAD DE DISTRIBUCIÓN DE CLAVE

Fig. 21


100, 200, 300, 400
(EJEMPLO DE DISPOSITIVO DE PROCESAMIENTO)
CPU
911
912: BUS
920
DISPOSITIVO DE DISCO MAGNÉTICO
(EJEMPLO DE DISPOSITIVO
DE ALMACENAMIENTO)
921
SISTEMA OPERATIVO
922
SISTEMA DE VENTANAS
923
PROGRAMAS
924
FICHEROS
ROM
913
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
RAM
914
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
LCD
901
(EJEMPLO DE DISPOSITIVO DE VISUALIZACIÓN)
TECLADO
902
(EJEMPLO DE DISPOSITIVO DE ENTRADA)
COM
915
PLACA DE COMUNICACIÓN