(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 699 535**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.12.2011 PCT/JP2011/078668**

(87) Fecha y número de publicación internacional: **16.08.2012 WO12108100**

(96) Fecha de presentación y número de la solicitud europea: **12.12.2011 E 11858018 (2)**

(97) Fecha y número de publicación de la concesión europea: **24.10.2018 EP 2675107**

(54) Título: **Sistema de procesamiento de cifrado, dispositivo de generación de claves, dispositivo de cifrado, dispositivo de desciframiento, dispositivo de delegación de claves, método de procesamiento de cifrado y programa de procesamiento de cifrado**

(30) Prioridad:

09.02.2011 JP 2011026216

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.02.2019

(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:

ELZABURU, S.L.P

DESCRIPCIÓN

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

Sector técnico

La presente invención se refiere a cifrado de predicados jerárquico (HPE, hierarchical predicate encryption). La invención se define en las reivindicaciones adjuntas.

Antecedentes de la técnica

La bibliografía no de patentes 21 discute HPE para productos escalares. La bibliografía no de patentes 18 discute cifrado funcional.

Lista de referencias

Bibliografía no de patentes

Bibliografía no de patentes 1: Beimel, A., Secure schemes for secret sharing and key distribution. PhD Thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

Bibliografía no de patentes 2: Bethencourt, J., Sahai, A., Waters, B.: ciphertext-policy attribute-based encryption En: 2007 IEEE Symposium on Security and Privacy, páginas 321·34 IEEE Press (2007)

Bibliografía no de patentes 3: Boneh, D., Boyen, X.: Efficient selective-ID secure identity based encryption without random oracles. En: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004 LNCS, volumen 3027, paginas 223·38. Springer Heidelberg (2004)

Bibliografía no de patentes 4: Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. En: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, volumen 3152, páginas 443·59. Springer Heidelberg (2004)

Bibliografía no de patentes 5: Boneh, D., Boyen, X., Goh, E.: Hierarchical identity based encryption with constant size ciphertext. En: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, volumen 3494, páginas 440·56. Springer Heidelberg (2005)

Bibliografía no de patentes 6: Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. En: Kilian, J.(ed.) CRYPTO 2001. LNCS, volumen 2139, páginas 213·29. Springer Heidelberg (2001)

Bibliografía no de patentes 7: Boneh, D., Hamburg, M.: Generalized identity based and broadcast encryption scheme. En: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, volumen 5350, páginas 455·70. Springer Heidelberg (2008)

Bibliografía no de patentes 8: Boneh, D., Katz, J., Improved efficiency for CCA-secure cryptosystems built using identity based encryption. RSA-CT 2005, LNCS, Springer Verlag (2005)

Bibliografía no de patentes 9: Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. En: Vadhan, S.P. (ed.) TCC 2007. LNCS, volumen 4392, páginas 535· 54. Springer Heidelberg (2007)

Bibliografía no de patentes 10: Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). En: Dwork, C. (ed.) CRYPTO 2006. LNCS, volumen 4117, páginas 290·07. Springer Heidelberg (2006)

Bibliografía no de patentes 11: Canetti, R., Halevi S., Katz J.: Chosen-ciphertext security from identity-based encryption. EUROCRYPT 2004, LNCS, Springer-Verlag (2004)

Bibliografía no de patentes 12: Cocks, C.: An identity based encryption scheme based on quadratic residues. En: Honary,B. (ed.) IMA Int. Conf. LNCS, volumen 2260, páginas 360· 63. Springer Heidelberg (2001)

Bibliografía no de patentes 13: Gentry, C.: Practical identity-based encryption without random oracles. En: Vaudenay, S.(ed.) EUROCRYPT 2006. LNCS, volumen 4004, páginas 445· 64. Springer Heidelberg (2006)

Bibliografía no de patentes 14: Gentry, C., Halevi, S.: Hierarchical identity-based encryption with polynomially many levels. En: Reingold, O. (ed.) TCC 2009. LNCS, volumen 5444, páginas 437· 56. Springer Heidelberg (2009)

Bibliografía no de patentes 15: Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. En: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, volumen 2501, páginas 548· 66. Springer Heidelberg (2002)

Bibliografía no de patentes 16: 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 89·8, ACM (2006)

Bibliografía no de patentes 17: Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. En: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, volumen 4965, páginas 146· 62. Springer Heidelberg (2008)

Bibliografía no de patentes 18: Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, EUROCRYPT 2010. LNCS, Springer Heidelberg (2010)

Bibliografía no de patentes 19: Lewko, A.B., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertexts. En: Micciancio, D. (ed.) TCC 2010. LNCS, volumen 5978, páginas 455· 79. Springer Heidelberg (2010)

Bibliografía no de patentes 20: Okamoto, T., Takashima, K.: Homomorphic encryption and signatures from vector decomposition. En: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, volumen 5209, páginas 57·4. Springer Heidelberg (2008)

Bibliografía no de patentes 21: Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products, In:ASIACRYPT 2009, Springer Heidelberg (2009).

Bibliografía no de patentes 22: Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. En: ACM Conference on Computer and Communication Security 2007, páginas 195·03, ACM (2007)

Bibliografía no de patentes 23: Pirretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure attribute-based systems. En: ACM Conference on Computer and Communication Security 2006, páginas 99·12, ACM (2006)

Bibliografía no de patentes 24: Sahai, A., Waters, B.: Fuzzy identity-based encryption. En: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, volumen 494, páginas 457· 73. Springer Heidelberg (2005)

Bibliografía no de patentes 25: Shi, E., Waters, B.: Delegating capability in predicate encryption system. En: Aceto, L., Damgaard, I., Goldberg, L.A., Halldorsson, M.M., Ingolfsdottir, A., Walukiewicz, I. (eds.) ICALP (2) 2008. LNCS, volumen 5126, páginas 560.578. Springer Heidelberg (2008)

Bibliografía no de patentes 26: Waters, B.: Efficient identity based encryption without random oracles. Eurocrypt 2005, LNCS, volumen 3152, páginas 443·59. Springer Verlag, (2005)

Bibliografía no de patentes 27: Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. ePrint, IACR, http://eprint.iacr.org/2008/290.

Bibliografía no de patentes 28: Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. En: Halevi, S. (ed.) CRYPTO 2009. LNCS, volumen 5677, páginas 619· 36. Springer Heidelberg (2009)

Descripción de la invención

Problema técnico

En un esquema HPE para productos escalares, discutido en la bibliografía no de patentes 21, se construyen procesos criptográficos utilizando un espacio grande. Por lo tanto, cuando se implementa este esquema HPE para productos escalares, los tamaños de las claves podrían ser grandes, afectando negativamente a la eficiencia de las operaciones, etc.

Un objetivo de la presente invención es dar a conocer un esquema HPE para productos escalares con una mayor eficiencia de las operaciones y similares.

Solución al problema

Un sistema de procesamiento criptográfico acorde con esta invención es un sistema de procesamiento criptográfico que realiza un proceso criptográfico utilizando una base B_t y una base B^*_t para cada número entero t de t = 1, ..., L+1 (siendo L un número entero igual o mayor que 1), el sistema de procesamiento criptográfico, e incluye

un dispositivo de cifrado que genera, como un texto cifrado ct, un vector en el que está incorporada información de atributo en un vector de base de la base B_t para por lo menos algún número entero t de t = 1, ..., L;

un dispositivo de desciframiento que utiliza, como clave de desciframiento sk_L, un vector en el que está incorporada información de predicado $\vec{v}_t$ en un vector de base de la base B^*_t para cada número entero t de t = 1, ..., L, realiza una operación de emparejamiento sobre el texto cifrado ct generado por el dispositivo de cifrado y la clave de desciframiento sk_L, y descifra el texto cifrado ct; y

un dispositivo de delegación de claves que genera una clave de desciframiento de nivel inferior sk_{L+1} de la clave de desciframiento sk_L, en base a un vector en el que la información de predicado $\vec{v}_{L+1}$ está incorporada en un vector de base de una base B^*_{L+1}, y a la clave de desciframiento sk_L utilizada en el dispositivo de desciframiento.

Resultados ventajosos de la invención

En un sistema de procesamiento criptográfico acorde con la presente invención, se construye una estructura jerárquica utilizando una serie de espacios. Por lo tanto, los tamaños de las claves pueden ser pequeños, mejorando de ese modo la eficiencia de las operaciones.

Breve descripción de los dibujos

La figura 1 es un diagrama para explicar una noción de "delegación (delegación jerárquica)";

la figura 2 es un diagrama para explicar una delegación con salto de nivel;

la figura 3 es un diagrama que muestra estructuras jerárquicas de información de atributo e información de predicado;

la figura 4 es un diagrama que muestra un ejemplo de cifrado jerárquico basado en identidad;

la figura 5 es un diagrama para explicar una base y un vector de la base;

la figura 6 es un diagrama para explicar un ejemplo de un método para implementar una estructura jerárquica en espacios vectoriales;

la figura 7 es un diagrama de configuración de un sistema de procesamiento criptográfico 10 que ejecuta algoritmos de un esquema HPE para productos escalares;

la figura 8 es un diagrama de bloques funcionales que muestra funciones de un dispositivo de generación de claves 100;

la figura 9 es un diagrama de bloques funcionales que muestra funciones de un dispositivo de cifrado 200;

la figura 10 es un diagrama de bloques funcionales que muestra funciones de un dispositivo de desciframiento 300;

la figura 11 es un diagrama de bloques funcionales que muestra funciones de un dispositivo de delegación de claves 400;

la figura 12 es un diagrama de flujo que muestra un proceso de un algoritmo Setup;

la figura 13 es un diagrama de flujo que muestra un proceso de un algoritmo KeyGen;

la figura 14 es un diagrama de flujo que muestra un proceso de un algoritmo Enc;

la figura 15 es un diagrama de flujo que muestra un proceso de un algoritmo Dec;

la figura 16 es un diagrama de flujo que muestra un proceso de un algoritmo $Delegate_L$;

la figura 17 es un diagrama de flujo que muestra un proceso de un algoritmo KeyGen;

la figura 18 es un diagrama de flujo que muestra un proceso del algoritmo Dec;

la figura 19 es un diagrama de flujo que muestra un proceso del algoritmo $Delegate_L$; y

la figura 20 es un diagrama que muestra un ejemplo de una configuración de hardware del dispositivo de generación de claves 100, el dispositivo de cifrado 200 y el dispositivo de desciframiento 300.

Descripción de realizaciones preferidas

A continuación se describirán realizaciones de la invención haciendo referencia a los dibujos.

En la siguiente descripción, un dispositivo de procesamiento es una CPU 911 o similar que se describirá más adelante. Un dispositivo de almacenamiento es una ROM 913, una RAM 914, un disco magnético 920 o similar, que se describirá más adelante. Un dispositivo de comunicación es una placa de comunicación 915 o similar, que se describirá más adelante. Un dispositivo de entrada es un teclado 902, la placa de comunicación 915 o similar, que se describirá más adelante. Un dispositivo de salida es la RAM 914, el disco magnético 920, la placa de comunicación 915, una LCD 901 o similar, que se describirá más adelante. 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 las notaciones que se van a utilizar en la siguiente descripción.

Cuando A es una distribución o variable aleatoria, la fórmula 101 denota que y se selecciona aleatoriamente desde A de acuerdo con 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 denota que y se selecciona uniformemente desde A. Es decir, y es un número aleatorio uniforme en la fórmula 102.

[Formula 102]

$$y \xleftarrow{U} A$$

La fórmula 103 denota que y es un conjunto, definido o sustituido por z.

[Fórmula 103]

$$y := z$$

Cuando a es un valor fijo, la fórmula 104 denota que una máquina (algoritmo) A entrega a sobre una entrada x.

[Fórmula 104]

$$A(x) \to a$$

por ejemplo,

$$A(x) \to 1$$

La fórmula 105, es decir, F_q, denota un campo finito de orden q.

[Formula 105]

$$\mathbb{F}_q$$

[Fórmula 105]

$$\mathbb{F}_q$$

Un símbolo de vector denota una representación vectorial sobre el campo finito F_q, es decir, fórmula 106.

[Fórmula 106]

$\vec{x}$ denota

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

La fórmula 107 denota el producto escalar, mostrado en la fórmula 109, de dos vectores $\vec{x}$ y $\vec{v}$ mostrados en la fórmula 108.

[Fórmula 107]

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

[Fórmula 108]

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

[Fórmula 109]

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

X^T denota la traspuesta de una matriz X.

Para una base B y una base B* mostradas en la fórmula 110, se define la fórmula 111.

[Fórmula 110]

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

[Fórmula 111]

$$(x_1, \ldots, x_N)_{\mathbb{B}} := \sum_{i=1}^{N} x_i b_i,$$
$$(y_1, \ldots, y_N)_{\mathbb{B}^*} := \sum_{i=1}^{N} y_i b_i^*$$

$\vec{e}_{t,j}$ denota un vector de la base ortonormal mostrado en la fórmula 112.

[Fórmula 112]

$$\vec{e}_{t,j} : (\overbrace{0 \cdots 0}^{j-1}, 1, \overbrace{0 \cdots 0}^{n_t - j}) \in \mathbb{F}_q^{n_t} \text{ para } j = 1, \ldots, n_t$$

Se definen las fórmulas 113 a 117.

[Fórmula 113]

$$((\vec{x}_0)_{\mathbb{B}_0^*}, \ldots, (\vec{x}_d)_{\mathbb{B}_d^*}) + ((\vec{y}_0)_{\mathbb{B}_0^*}, \ldots, (\vec{y}_d)_{\mathbb{B}_d^*})$$
$$:= ((\vec{x}_0 + \vec{y}_0)_{\mathbb{B}_0^*}, \ldots, (\vec{x}_d + \vec{y}_d)_{\mathbb{B}_d^*})$$

[Fórmula 114]

$$(\vec{x})_{\mathbb{B}_t^*} := ((\vec{0})_{\mathbb{B}_0^*}, \ldots, (\vec{0})_{\mathbb{B}_{t-1}^*}, (\vec{x})_{\mathbb{B}_t^*}, (\vec{0})_{\mathbb{B}_{t+1}^*}, \ldots, (\vec{0})_{\mathbb{B}_d^*})$$

[Fórmula 115]

$$((\vec{x}_i)_{\mathbb{B}_i^*}, (\vec{x}_j)_{\mathbb{B}_j^*}) := ((\vec{x}_i)_{\mathbb{B}_i^*} + (\vec{x}_j)_{\mathbb{B}_j^*}$$

[**Fórmula** 116]

$$((\vec{x}_0)_{\mathbb{B}_0^*},(\vec{x}_t)_{\mathbb{B}_t^*};t=1,...,L):=((\vec{x}_0)_{\mathbb{B}_0^*},...,\ (\vec{x}_L)_{\mathbb{B}_L^*})$$

[Fórmula 117]

$$e(c,k^*):=\prod_{t=0}^{d}e(c_t,k_t^*),$$

donde

$$c:=(c_0\in\langle\mathbb{B}_0\rangle,...,c_d\in\langle\mathbb{B}_d\rangle),$$

$$k^*:=(k_{L,0}^*\in\langle\mathbb{B}_0^*\rangle,...,k_d^*\in\langle\mathbb{B}_d^*\rangle)$$

Para la fórmula 118, se define la fórmula 119.

[Fórmula 118]

$$k^*:=((\vec{x}_0)_{\mathbb{B}_0^*},...,(\vec{x}_d)_{\mathbb{B}_d^*})$$

[Fórmula 119]

$$[k^*]^L:=((\vec{x}_0)_{\mathbb{B}_0^*},...,(\vec{x}_L)_{\mathbb{B}_L^*},(\vec{0})_{\mathbb{B}_{L+1}^*},...,(\vec{0})_{\mathbb{B}_d^*}),$$

$$[k^*]_L:=((\vec{0})_{\mathbb{B}_0^*},...,(\vec{0})_{\mathbb{B}_L^*},(\vec{x}_{L+1})_{\mathbb{B}_{L+1}^*},...,(\vec{x}_d)_{\mathbb{B}_d^*})$$

En la siguiente descripción, nt en F_q^{nt} denota n_t.

Análogamente, (v→1, ..., v→L) en una clave secreta $sk_{(v\rightarrow 1,\ ...,\ v\rightarrow L)}$ denota ($\vec{v}_1$, ..., $\vec{v}_L$), y (v→1, ..., v→L+1) en una clave secreta $sk_{(v\rightarrow 1,\ ...,\ v\rightarrow L+1)}$ denota ($\vec{v}_1$, ..., $\vec{v}_{L+1}$).

Análogamente, cuando se muestra "δi,j" como un superíndice, δi,j denota $\delta_{i,j}$.

Cuando "→" que representa un vector está acoplado a un subíndice o un superíndice, este "→" está acoplado como un superíndice a dicho subíndice o superíndice.

En la siguiente descripción, un proceso criptográfico incluye un proceso de cifrado, un proceso de desciframiento, un proceso de generación de claves y un proceso de delegación de claves.

Primera realización

En esta realización, se describirán conceptos básicos para implementar "HPE para productos escalares" y construcciones de "HPE para productos escalares".

En primer lugar, se describirá la noción de HPE para productos escalares. Para describir la noción de HPE para productos escalares, se describirá en primer lugar la noción de "delegación", junto con la noción de "delegación jerárquica". A continuación, se describirá el "cifrado de predicados (PE, predicate encryption) para productos escalares". Después, se describirá "HPE para productos escalares", que es un tipo de PE para productos escalares con la noción de delegación jerárquica. Además, para reforzar la comprensión del HPE para productos escalares, se describirá un ejemplo de aplicación de HPE para productos escalares.

En segundo lugar, se describirá HPE para productos escalares en espacios vectoriales. En esta realización y en las siguientes, HPE y un mecanismo de encapsulamiento de claves de predicado jerárquico (HPKEM, hierarchical predicate key encapsulation mechanism) se implementan en espacios vectoriales. En primer lugar se describirá una "base" y un "vector de la base". A continuación, se describirá "PE para productos escalares en espacios vectoriales".

Después, se describirá un "método para implementar una estructura jerárquica en espacios vectoriales". Además, para reforzar la comprensión, se describirá un ejemplo de implementación de la estructura jerárquica.

En tercer lugar, se describirán "espacios vectoriales de emparejamientos duales (DPVS, dual pairing vector spaces)", que tienen estructuras matemáticas ricas para implementar HPE para productos escalares.

En cuarto lugar, se describirán construcciones básicas de un "esquema HPE para productos escalares" de acuerdo con esta realización. A continuación, se describirán construcciones básicas de un "sistema de procesamiento criptográfico 10" que implementa HPE. Después, se describirá en detalle el esquema HPE y el sistema de procesamiento criptográfico 10, de acuerdo con esta realización.

<1. HPE para productos escalares>

<1-1. Noción de delegación (delegación jerárquica)>

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

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

En la figura 1, una raíz (dispositivo de generación de claves) genera claves secretas para usuarios de un primer nivel (nivel 1) utilizando una clave secreta maestra. Es decir, la raíz genera claves 1, 2 y 3 para usuarios de primer nivel 1, 2 y 3, respectivamente. A continuación, utilizando la clave 1, por ejemplo, el usuario 1 puede generar claves 11, 12 y 13 para usuarios 11, 12 y 13, respectivamente, que son usuarios de nivel inferior (segundo nivel) del usuario 1. Las claves 11, 12 y 13 que poseen los usuarios 11, 12 y 13 tienen capacidades más limitadas que la clave 1 que posee el usuario 1. Las capacidades limitadas significan que los textos cifrados que pueden ser descifrados por dicha clave secreta están limitados. Es decir, una clave secreta de nivel inferior puede descifrar solamente algunos textos cifrados que pueden ser descifrados por una clave secreta de nivel superior. Esto significa que las claves 11, 12 y 13 que poseen los usuarios 11, 12 y 13 pueden descifrar solamente algunos de los textos cifrados que pueden ser descifrados por la clave 1 que posee el usuario 1. Generalmente, las claves 11, 12 y 13 pueden descifrar respectivamente textos cifrados diferentes. Por otra parte, un texto cifrado que puede ser descifrado por las claves 11, 12 o 13 puede ser descifrado por la clave 1.

Tal como se muestra en la figura 1, cada clave secreta se proporciona para un nivel específico. Esto se describe como "jerárquico". Es decir, tal como se muestra en la figura 1, la generación jerárquica de claves de nivel inferior se denomina "delegación jerárquica".

En la figura 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. Sin embargo, tal como se muestra en la figura 2, la raíz puede generar no solamente las claves secretas para los usuarios de primer nivel, sino asimismo las claves secretas para los usuarios de segundo nivel o de nivel inferior. Análogamente, los usuarios de primer nivel pueden generar no solamente las claves secretas para los usuarios de segundo nivel, sino asimismo las claves secretas para los usuarios de tercer nivel o de nivel inferior. Es decir, la raíz o cada usuario pueden generar las claves secretas para niveles inferiores al nivel de su propia clave secreta.

<1-2. PE para productos escalares>

A continuación, se describirá "PE para productos escalares".

PE es un esquema criptográfico en el que un texto cifrado se puede descifrar si el resultado de introducir una información de atributo x en una información de predicado f_v es 1 (verdadero) ($f_v(x) = 1$). Generalmente, la información de atributo x está incorporada en un texto cifrado, y la información de predicado f_v está incorporada en una clave secreta. Es decir, en PE, un texto cifrado c cifrado en base a la información de atributo x es descifrado por una clave secreta SK_f generada en base a la información de predicado f_v. 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 tiene que introducir en 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) ($f_v(x) = 1$).

PE se discute en detalle en la bibliografía no de patentes 17.

PE para productos escalares es un tipo de PE en el que $f_v(x) = 1$ si el producto escalar de una información de atributo x y una información de predicado f_v es un valor predeterminado. Es decir, un texto cifrado c cifrado por la información de atributo x puede ser descifrado por una clave secreta SK_f generada en base a la información de predicado f_v si y sólo si el producto escalar de la información de atributo x por la información de predicado f_v es un valor predeterminado.

En la primera realización, se asume como una regla general que $f_v(x) = 1$ si el producto escalar de la información de atributo x por la información de predicado f_v es 0.

<1-3. HPE para productos escalares>

HPE para productos escalares (HPKEM para productos escalares) es un tipo de "PE para productos escalares" con la noción descrita anteriormente de "delegación jerárquica".

En HPE para productos escalares, la información de atributo y la información de predicado tienen estructuras jerárquicas, para incorporar un sistema de delegación jerárquica en PE para productos escalares.

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

En la figura 3, una información de atributo y una información de predicado con los mismos numerales de referencia se corresponden entre sí (es decir, su producto escalar es 0). Es decir, el producto escalar de un atributo 1 y un predicado 1 es 0, el producto escalar de un atributo 11 y un predicado 11 es 0, el producto escalar de un atributo 12 y un predicado 12 es 0, y el producto escalar de un atributo 13 y un predicado 13 es 0. Esto significa que un texto cifrado c1, cifrado con el atributo 1, puede ser descifrado por una clave secreta k1 generada en base al predicado 1. Un texto cifrado c11, cifrado por el atributo 11, puede ser descifrado por una clave secreta k11 generada en base al predicado 11. Lo mismo se puede decir del atributo 12 y el predicado 12, así como del atributo 13 y el predicado 13.

Tal como se ha descrito anteriormente, HPE para productos escalares tiene el sistema de delegación jerárquica. Por lo tanto, la clave secreta k11 se puede generar en base al predicado 11 y a la clave secreta k1 generada en base al predicado 1. Es decir, un usuario que tiene la clave secreta de nivel superior k1 puede generar su clave secreta de nivel inferior k11 a partir de la clave secreta k1 y el predicado de nivel inferior 11. Análogamente, una clave secreta k12 se puede generar a partir de la clave secreta k1 y del predicado 12, y una clave secreta k13 se puede generar a partir de la clave secreta k1 y del predicado 13.

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

<1-4. Ejemplo de aplicación de HPE para productos escalares>

La figura 4 es un diagrama que muestra un ejemplo de cifrado jerárquico basado en identidad (HIBE, hierarchical identity-based encryption), que es un ejemplo de aplicación del esquema HPE para productos escalares que se describe más adelante. HIBE es un proceso criptográfico en el que la noción de jerarquía se aplica a cifrado basado en identidad (IBE, identity-based encryption). IBE es un tipo de PE, concretamente, PE por coincidencia, que permite que un texto cifrado sea descifrado si un ID incluido en el texto cifrado coincide con un ID incluido en una clave secreta.

En el ejemplo mostrado en la figura 4, en base a una clave secreta maestra sk y a un ID "A" de la compañía A, una raíz (dispositivo de generación de claves) genera una clave secreta (clave A) correspondiente al ID "A". Por ejemplo, en base a la clave A y al ID de cada división, un administrador de seguridad de la compañía A genera una clave secreta correspondiente a dicho ID. Por ejemplo, el administrador de seguridad genera una clave secreta (clave 1) correspondiente a un ID "A-1" de una división de ventas. A continuación, en base a la clave secreta de cada división y al ID de cada unidad perteneciente a dicha división, por ejemplo, un administrador de cada división genera una clave secreta correspondiente a dicho ID. Por ejemplo, un administrador de la división de ventas genera una clave secreta (clave 11) correspondiente a un ID "A-11" de la unidad de ventas 1.

En este caso, un texto cifrado, cifrado por el ID "A-11" de la unidad de ventas 1, puede ser descifrado por la clave 11, que es la clave secreta correspondiente al ID "A-11" de la unidad de ventas 1. Sin embargo, un texto cifrado, cifrado por el ID de una unidad de ventas 2 o de una unidad de ventas 3, no puede ser descifrado por la clave 11. Asimismo, un texto cifrado, cifrado por el ID de la división de ventas, no puede ser descifrado por la clave 11.

Un texto cifrado, cifrado por el ID "A-1" de la división de ventas, puede ser descifrado por la clave 1, que es la clave secreta correspondiente al ID "A-1" de la división de ventas. Asimismo, un texto cifrado, cifrado por el ID de una unidad perteneciente a la división de ventas, puede ser descifrado por la clave 1. Es decir, un texto cifrado, cifrado por el ID de la unidad de ventas 1, 2 o 3, puede ser descifrado por la clave 1. Sin embargo, un texto cifrado, cifrado por el ID de la división de fabricación (ID: A-2) o de una división de personal (ID: A-3), no puede ser descifrado por la clave 1. Asimismo, un texto cifrado, cifrado por el ID de la compañía A, no puede ser descifrado por la clave 1.

Un texto cifrado, cifrado por el ID "A" de la compañía A, puede ser descifrado por la clave A que es la clave secreta correspondiente al ID "A" de la compañía A. Asimismo, un texto cifrado, cifrado por el ID de cada división perteneciente a la compañía A o el ID de una unidad perteneciente a cada división, puede ser descifrado por la clave A.

HPE para productos escalares se puede adaptar a diversas aplicaciones a parte de IBE. En particular, los procesos criptográficos que se describen más adelante no se limitan a una clase de pruebas de paridad, de tal modo que se pueden aplicar a un gran número de aplicaciones. Por ejemplo, con respecto a cifrado con capacidad de búsqueda o similar, que es un tipo de PE para productos escalares, los procesos criptográficos permiten que las aplicaciones que no se pueden implementar con PE convencional tengan el sistema de delegación, tal como limitando un rango de búsqueda en cada nivel mediante la utilización de 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, tal como cifrado con capacidad de búsqueda e IBE.

<2. HPE para productos escalares en espacios vectoriales>

HPKEM y HPE se implementan en espacios vectoriales de alta dimensión denominados espacios vectoriales de emparejamientos duales (DPVS, dual pairing vector spaces) que se describen más adelante. Por lo tanto, se describirá HPE para productos escalares en espacios vectoriales.

<2-1. Base y vector de la base>

En primer lugar, se explicarán brevemente una "base" y un "vector de la base" que se van a utilizar para explicar un espacio vectorial.

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

La figura 5 muestra un vector v de un espacio vectorial bidimensional. El vector v es $c_1a_1 + c_2a_2$. Además, el vector v es $y_1b_1 + y_2b_2$. En este caso, a_1 y a_2 se denominan vectores de la base en una base A, y se representan como base A: = (a_1, a_2). b_1 y b_2 se denominan vectores de la base en una base B, y se representan como base B: = (b_1, b_2). c_1, c_2, y_1 y y_2 son coeficientes de respectivos vectores de la base. La figura 5 muestra un espacio vectorial bidimensional, de tal modo que existen dos vectores de la base en cada base. En un espacio vectorial N-dimensional, existe en un número N de vectores de la base en cada base.

<2-2. PE para productos escalares en espacios vectoriales>

A continuación se describirá PE para productos escalares en espacios vectoriales.

Tal como se ha descrito anteriormente, PE para productos escalares es un tipo de PE en el que $f_v(x) = 1$ si el producto escalar de la información de atributo x por 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, es decir, un vector de atributo x y un vector de predicado $\vec{v}$, su predicado del producto escalar se define tal como se muestra en la fórmula 120.

[Fórmula 120]

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 PE en el que el resultado de introducir la información de atributo x en la información de predicado f_v es 1 (verdadero) si el producto escalar del vector de atributo $\vec{x}$ por el vector de predicado $\vec{v}$ (es decir, la suma de los productos escalares elemento a elemento) es 0, y el resultado de introducir la información de atributo x en la información de predicado f_v es 0 (falso) si el producto escalar 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 espacios vectoriales>

A continuación se describirá un método para implementar una estructura jerárquica en espacios vectoriales.

La figura 6 es un diagrama para explicar un ejemplo del método para implementar una estructura jerárquica en espacios vectoriales.

Se discutirá en este caso un número d (d es un número entero igual o mayor que 1) de espacios vectoriales. Cada espacio vectorial es un espacio vectorial de alta dimensión (N_t-dimensional (t = 1, ..., d)). Es decir, existe un número N_t de vectores de la base c_i (i = 1, ..., N_t) en una base predeterminada C_t (t = 1, ..., d) en cada espacio vectorial.

Una base C_1 es un espacio para establecer información de atributo e información de predicado de un primer nivel. Una base C_2 es un espacio para establecer información de atributo e información de predicado de un segundo nivel. Análogamente, una base C_L es un espacio para establecer información de atributo e información de predicado de un L-ésimo nivel. Por lo tanto, en este caso se pueden representar d niveles.

Una clave secreta para el L-ésimo nivel se genera no solamente estableciendo la información de predicado del L-ésimo nivel utilizando la base C_L, sino asimismo estableciendo la información de predicado de los primero a (L -1)-ésimo niveles utilizando las bases C_1 a C_{L-1}. Es decir, en una clave secreta de nivel inferior, se establece asimismo la información de predicado que se tiene que establecer en una clave secreta de nivel superior. Esta disposición permite que la información de predicado tenga una estructura jerárquica. A continuación, utilizando la estructura jerárquica de la información de predicado, se construye un sistema de delegación en PE para productos escalares.

En la siguiente descripción, se utiliza un formato de jerarquía $\vec{n}$: = (d; N_1, ..., N_d) para denotar una estructura jerárquica en un espacio vectorial, donde d es un valor que representa la profundidad de niveles descrita anteriormente, y N_i (i = 1, ..., d) es un valor que representa el número de dimensiones, es decir, el número de vectores de la base, que se asigna a cada nivel i.

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

La estructura jerárquica se explicará utilizando un ejemplo simple. Se proporcionará una explicación utilizando un ejemplo en el que existen tres niveles, y cada nivel está asignado a un espacio bidimensional. Es decir, $\vec{n}$: = (d; N_1, ..., N_d) = (3; 2, 2, 2).

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 a 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 ($\vec{v}_1$, $\vec{v}_2$). Análogamente, 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 a 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 mediante ($\vec{v}_1$, (0, 0), (0, 0)). Por lo tanto, la clave secreta de primer nivel sk_1 puede descifrar un texto cifrado, cifrado mediante 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. Donde "*" denota un valor arbitrario.

Análogamente, 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 mediante ($\vec{v}_1$, $\vec{v}_2$, (0, 0)). Por lo tanto, la clave secreta de segundo nivel sk_2 puede descifrar un texto cifrado, cifrado mediante 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 $\vec{v}_2 \cdot \vec{x}_2 = 0$.

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

<3. Espacios vectoriales de emparejamientos duales (DPVS)>

En primer lugar se describirán grupos de emparejamientos bilineales simétricos.

Los grupos de emparejamientos bilineales simétricos (q, G, G^T, g, e) son una tupla de un número primo q, un grupo aditivo cíclico G de orden q, un grupo multiplicativo cíclico G^T de orden q, $g \neq 0 \in G$, y un emparejamiento bilineal no degenerado computable en tiempo polinomial e: $G \times G \rightarrow G_T$. El emparejamiento bilineal no degenerado es $e(sg, tg) = e(g, g)^{st}$ y $e(g,g) \neq 1$.

En la siguiente descripción, la fórmula 121 es un algoritmo que toma 1^λ como entrada y entrega valores de parámetro $param_G$: = (q, G, G_T, g, e) de grupos de emparejamientos bilineales con un parámetro de seguridad λ.

[Fórmula 121]

$$\mathcal{G}_{\mathrm{bpg}}$$

A continuación se describirán los espacios vectoriales de emparejamientos duales.

Se pueden construir espacios vectoriales de emparejamientos duales (q, V, G_T, A, e) mediante un producto directo de los grupos de emparejamientos bilineales simétricos ($param_G$:=(q, G, G_T, g, e)). Los espacios vectoriales de emparejamientos duales (q, V, G_T, A, e) son tuplas de un número primo q, un espacio vectorial N-dimensional V sobre F_q mostrado en la fórmula 122, un grupo cíclico G_T de orden q y una base canónica A: = (a_1, ..., a_N) del espacio V, y tienen las siguientes operaciones (1) y (2). En este caso, a_i es tal como se muestra en la fórmula 123.

[Fórmula 122]

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

[Fórmula 123]

$$a_i := (\overbrace{0,\ldots,0}^{i-1}, g, \overbrace{0,\ldots,0}^{N-i})$$

Operación (1): emparejamiento bilineal no degenerado

Se define un emparejamiento en el espacio V mediante la fórmula 124.

[Fórmula 124]

$$e(x,y) := \prod_{i=1}^{N} e(G_i, H_i) \in \mathbb{G}_T$$

donde

$$(G_1,\ldots,G_N) := x \in \mathbb{V},$$
$$(H_1,\ldots,H_N) := y \in \mathbb{V}$$

Este es bilineal no degenerado, es decir, e(sx, ty) = $e(x, y)^{st}$ y si e(x, y) = 1 para todo y∈V, entonces x = 0. Para todo i y j, $e(a_i, a_j) = e(g, g)^{\delta_{i,j}}$, donde $\delta_{i,j}$ = 1 si i = j, y $\delta_{i,j}$ = 0 si i ≠ j, y e(g, g) ≠ 1∈G_T.

Operación (2): mapas de distorsión

Transformaciones lineales $\phi_{i,j}$ sobre el espacio V mostrado en la fórmula 125 pueden conseguir la fórmula 126.

[Fórmula 125]

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

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

[Fórmula 126]

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

donde

$$(g_1,\ldots g_N) := x.$$

Las transformaciones lineales $\phi_{i,j}$ se denominarán mapas de distorsión.

En la siguiente descripción, la fórmula 127 es un algoritmo que toma una entrada 1^{λ} ($\lambda \in$ números naturales), $N \in$ números naturales, y valores de parámetros $param_G$: = (q, G, G_T, g, e) de grupos de emparejamientos bilineales, y entrega valores del parámetros $param_V$: = (q, V, G_T, A, e) de espacios vectoriales de emparejamientos duales con un parámetro de seguridad λ y un espacio N-dimensional V.

[Fórmula 127]

$$\mathcal{G}_{\mathrm{dpvs}}$$

Aquí, la descripción se dirigirá a un caso en el que se construyen espacios vectoriales de emparejamientos duales utilizando los grupos de emparejamientos bilineales simétricos descritos anteriormente. Los espacios vectoriales de emparejamientos duales se pueden construir asimismo utilizando grupos de emparejamientos bilineales asimétricos. La siguiente descripción se puede adaptar fácilmente a un caso en el que se construyen espacios vectoriales de emparejamientos duales utilizando grupos de emparejamientos bilineales asimétricos.

<4. Construcción de HPE y sistema de procesamiento criptográfico 10>

<4-1. Construcción básica de HPE para productos escalares>

Se describirá brevemente una construcción del esquema HPE para productos escalares.

El esquema HPE para productos escalares incluye cinco algoritmos probabilísticos computables en tiempo polinomial: Setup, keyGen, 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 $\vec{n}$: = (d; N_0, ..., N_d), y entrega una clave pública maestra pk y una clave secreta maestra sk. La clave secreta maestra sk es una clave de nivel superior.

(KeyGen)

El algoritmo KeyGen toma como entrada la clave pública maestra pk, la clave secreta maestra sk y vectores de predicado ($\vec{v}_1$, ..., $\vec{v}_L$) (1 ≤ L ≤ d), y entrega una clave secreta de L-ésimo nivel $sk_{(\vec{v}_1, \ldots, \vec{v}_L)}$.

(Enc)

El algoritmo Enc toma como entrada la clave pública maestra pk, vectores de atributo ($\vec{x}_1$, ..., $\vec{x}_h$) (1 ≤ h ≤d) y un mensaje m, y entrega un texto cifrado ct (texto encriptado). Es decir, el algoritmo Enc entrega el texto cifrado ct conteniendo el mensaje n y cifrado mediante los vectores de atributo ($\vec{x}_1$, ..., $\vec{x}_h$).

(Dec)

El algoritmo Dec toma como entrada la clave pública maestra pk, la clave secreta de L-ésimo nivel $sk_{(\vec{v}_1, \ldots, \vec{v}_L)}$ y el texto cifrado ct, y entrega el mensaje m o un símbolo diferenciado $\perp$. El símbolo diferenciado $\perp$ es información que indica fallo de desciframiento. Es decir, el algoritmo Dec descifra el texto cifrado ct mediante la clave secreta de L-ésimo nivel, y extrae el mensaje m. En caso de fallo de desciframiento, el algoritmo Dec entrega el símbolo diferenciado $\perp$.

(DelegatedL)

$Delegate_L$ toma como entrada la clave pública maestra pk, la clave secreta de L-ésimo nivel $sk_{(\vec{v}_1, \ldots, \vec{v}_L)}$ y un vector de predicado de nivel (L + 1)-ésimo $\vec{v}_{L+1}$ (L+1 ≤ d), y entrega una clave secreta (L + 1)-ésima $sk_{(\vec{v}_1, \ldots, \vec{v}_{L+1})}$ Es decir, el algoritmo $Delegate_L$ entrega una clave secreta de nivel inferior.

<4-2. Sistema de procesamiento criptográfico 10>

Se describirá el sistema de procesamiento criptográfico 10 que ejecuta los algoritmos del esquema HPE para productos escalares.

La figura 7 es un diagrama de configuración del sistema de procesamiento criptográfico 10 que ejecuta los algoritmos del esquema HPE para productos escalares.

El sistema de procesamiento criptográfico 10 incluye un dispositivo de generación de claves 100, un dispositivo de cifrado 200, un dispositivo de desciframiento 300 y un dispositivo de delegación de claves 400. La descripción se proporcionará en este caso asumiendo que el dispositivo de desciframiento 300 incluye el dispositivo de delegación de claves 400. Sin embargo, el dispositivo de delegación de claves 400 se puede disponer por separado del dispositivo de desciframiento 300.

El dispositivo de generación de claves 100 ejecuta el algoritmo Setup tomando como entrada un parámetro de seguridad λ y un formato de jerarquía $\vec{n}$: = (d; N_0, ..., N_d), y genera una clave pública maestra pk y una clave secreta maestra sk. A continuación, el dispositivo de generación de claves 100 hace pública la clave pública maestra pk generada. El dispositivo de generación de claves 100 ejecuta asimismo el algoritmo KeyGen tomando como entrada la clave pública maestra pk, la clave secreta maestra sk y vectores de predicado ($\vec{v}_1$, ..., $\vec{v}_L$)(1 ≤ L ≤ d), genera una clave secreta de L-ésimo nivel $sk_{(\vec{v}_1, ..., \vec{v}_L)}$ y proporciona secretamente la clave secreta de L-ésimo nivel al dispositivo de desciframiento de nivel L-ésimo 300.

El dispositivo de cifrado 200 ejecuta el algoritmo Enc tomando como entrada la clave pública maestra pk, vectores de atributo ($\vec{x}_1$, ..., $\vec{x}_h$) (1 ≤ h ≤ d) y un mensaje m, y genera un texto cifrado ct. El dispositivo de cifrado 200 transmite el texto cifrado generado ct al dispositivo de desciframiento 300.

El dispositivo de desciframiento 300 ejecuta el algoritmo Dec tomando como entrada la clave pública maestra pk, la clave secreta de L-ésimo nivel $sk_{(\vec{v}_1, ..., \vec{v}_L)}$ y el texto cifrado ct, y entrega el mensaje m o el símbolo diferenciado $\perp$.

El dispositivo de delegación de claves 400 ejecuta el algoritmo $Delegate_L$ tomando como entrada la clave pública maestra pk, la clave secreta de L-ésimo nivel $sk_{(\vec{v}_1, ..., \vec{v}_L)}$ y un vector de predicado de (L + 1)-ésimo nivel $\vec{v}_{L+1}$ (L + 1 ≤ d), y genera una clave secreta de (L + 1)-ésimo nivel $sk_{(\vec{v}_1, ..., \vec{v}_{L+1})}$ y proporciona secretamente la clave secreta de (L + 1)-ésimo nivel al dispositivo de desciframiento 300 de (L + 1)-ésimo nivel.

<4-3. Detalles del esquema HPE para productos escalares y sistema de procesamiento criptográfico 10>

Haciendo referencia a las figuras 8 a 16, la descripción se dirigirá al esquema HPE para productos escalares de acuerdo con la primera realización. La descripción se dirigirá asimismo a funciones y operaciones del sistema de procesamiento criptográfico 10 que implementa el esquema HPE para productos escalares.

La figura 8 es un diagrama de bloques funcionales que muestra funciones del dispositivo de generación de claves 100. La figura 9 es un diagrama de bloques funcionales que muestra funciones del dispositivo de cifrado 200. La figura 10 es un diagrama de bloques funcionales que muestra funciones del dispositivo de desciframiento 300. La figura 11 es un diagrama de bloques funcionales que muestra funciones del dispositivo de delegación de claves 400.

Las figuras 12 y 13 son diagramas de flujo que muestran operaciones del dispositivo de generación de claves 100. La figura 12 es un diagrama de flujo que muestra un proceso del algoritmo Setup. La figura 13 es un diagrama de flujo que muestra un proceso del algoritmo KeyGen. La figura 14 es un diagrama de flujo que muestra operaciones del dispositivo de cifrado 200 y muestra un proceso del algoritmo Enc. La figura 15 es un diagrama de flujo que muestra operaciones del dispositivo de desciframiento 300 y muestra un proceso del algoritmo Dec. La figura 16 es un diagrama de flujo que muestra operaciones del dispositivo de delegación de claves 400 y muestra un proceso del algoritmo $Delegate_L$.

En la siguiente descripción, un subíndice "dec" significa "desciframiento". El subíndice "dec" indica un elemento de desciframiento utilizado para descifrar un texto cifrado. Un subíndice "ran" significa "aleatorización". El subíndice "ran" indica un elemento de aleatorización para aleatorizar el coeficiente de un vector de la base predeterminado de una clave de desciframiento de nivel inferior. Un subíndice "del" significa "delegación". El subíndice "del" indica un elemento de delegación para generar una clave de desciframiento de nivel inferior.

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

Tal como se muestra en la figura 8, el dispositivo de generación de claves 100 incluye una unidad de generación de claves maestras 110, una unidad de almacenamiento de claves maestras 120, una unidad de introducción de información 130 (primera unidad de introducción de información), una unidad de generación de claves de desciframiento 140 y una unidad de distribución de claves 150 (unidad de transmisión de claves de desciframiento).

La unidad de generación de claves de desciframiento 140 incluye una unidad de generación de números aleatorios 141, una unidad de generación de elementos de desciframiento 142, una unidad de generación de elementos de aleatorización 143 y una unidad de generación de elementos de delegación 144.

Haciendo referencia a la figura 12, se describirá en primer lugar el proceso del algoritmo Setup.

(S101: etapa de generación de base ortonormal)

Utilizando el dispositivo de procesamiento, la unidad de generación de claves maestras 110 calcula la fórmula 128, y genera aleatoriamente $param_{\vec{n}}$ así como una base B_t y una base B^*_t para cada número entero t de t = 0, ..., d.

[Fórmula 128]

(1) introducir

$$1^{\lambda}, \vec{n} := (d; \vec{n} := (d; n_1, ..., n_d, u_0, ..., u_d, w_0, ..., w_d, z_0, ..., z_d)),$$
$$N_0 := 1 + u_0 + 1 + w_0 + z_0;\ N_t := n_t + u_t + w_t + z_t (t = 1, ..., d)$$

(2) $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, g, e) \xleftarrow{R} \mathcal{G}_{\mathsf{bpg}}(1^{\lambda})$

(3) $\psi \xleftarrow{U} \mathbb{F}_q^{\times},$

Se ejecutan las etapas (4) a (8) para cada t de t= 0,...,d.

(4) $\mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^{\lambda}, N_t, \mathsf{param}_{\mathbb{G}})$

(5) $X_t := (\chi_{t,i,j})_{i,j} \xleftarrow{U} GL(N_t, \mathbb{F}_q)$

(6) $(\nu_{t,i,j})_{i,j} := \psi \cdot (X_t^{\mathrm{T}})^{-1}$

(7) $\mathbb{B}_t := (b_{t,1}, \ldots, b_{t,N_t})$

(8) $\mathbb{B}_t^* := (b_{t,1}^*, \ldots, b_{t,N_t}^*)$

(9) $\mathsf{param}_n^{\rightarrow} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,\ldots,d}, g_T)$

Es decir, la unidad de generación de claves maestras 110 ejecuta las etapas siguientes.

(1) Utilizando el dispositivo de entrada, la unidad de generación de claves maestras 110 introduce un parámetro de seguridad $\lambda(1^{\lambda})$ y un formato de atributo $n^{\rightarrow}$: = (d; n_1, ..., n_d, u_0, ..., u_d, w_0, ..., w_d, z_0, ..., z_d), donde d es un número entero igual o mayor que 1, n_t es un número entero igual o mayor que 1 para cada número entero t de t = 1, ..., d, y u_t, w_t, z_t son números enteros iguales o mayores que 1 para cada número entero t de t = 0, ..., d. La unidad de generación de claves maestras 110 establece asimismo N_0: = $1+u_0+1+w_0+z_0$ y N_t: = $n_t+u_t+w_t+z_t$ para cada número entero t de t = 1, ..., d.

(2) Utilizando el dispositivo de procesamiento, la unidad de generación de claves maestras 110 ejecuta el algoritmo G_{bpg} tomando como entrada el parámetro de seguridad $\lambda(1^{\lambda})$ introducido en (1), y genera aleatoriamente valores de parámetro $param_G$: = (q, G, G_T, g, e) de grupos de emparejamientos bilineales.

(3) utilizando el dispositivo de procesamiento, la unidad de generación de claves maestras 110 genera un número aleatorio ψ.

A continuación, la unidad de generación de claves maestras 110 ejecuta las siguientes etapas (4) a (8) para cada número entero t de t = 0, ..., d.

(4) Utilizando el dispositivo de procesamiento, la unidad de generación de claves maestras 110 ejecuta el algoritmo G_{dpvs} tomando como entrada el parámetro de seguridad $\lambda(1^{\lambda})$ y N_t introducido en (1) y los valores de $param_G$: = (q, G, G_T, g, e) generados en (2), y genera valores del parámetro $param_{Vt}$: = (q, V_t, G_T, A_t, e) de espacios vectoriales de emparejamientos duales.

(5) Utilizando el dispositivo de procesamiento, la unidad de generación de claves maestras 110 genera aleatoriamente una transformación lineal X_t: = $(\chi_{t,i,j})_{i,j}$ tomando como entrada N_t establecido en (1) y F_q. Se debe

observar que GL significa lineal general. Es decir, GL es un grupo lineal general, un conjunto de matrices cuadradas con determinantes distintos de cero, y un grupo bajo la multiplicación. $(\chi_{t,i,j})_{i,j}$ denota una matriz asociada con los subíndices i, j de la matriz $\chi_{t,i,j}$, donde i, j = 1, ..., N_t.

(6) Utilizando el dispositivo de procesamiento y en base al número aleatorio ψ y a la transformación lineal X_t, la unidad de generación de claves maestras 110 genera $(v_{t,i,j})_{i,j}$: = ψ. $(X_t^T)^{-1}$. Como en el caso de $(\chi_{t,i,j})_{i,j}$, $(v_{t,i,j})_{i,j}$ denota una matriz asociada con los subíndices i, j de la matriz $v_{t,i,j}$, donde i, j = 1, ..., N_t.

(7) Utilizando el dispositivo de procesamiento y en base a la transformación lineal X_t generada (5), la unidad de generación de claves maestras 110 genera la base B_t a partir de la base ortonormal A_t generada en (4).

(8) Utilizando el dispositivo de procesamiento y en base a $(v_{t,i,j})_{i,j}$ generada en (6), la unidad de generación de claves maestras 110 genera la base B^*_t a partir de la base ortonormal A_t generada en (4).

(9) Utilizando el dispositivo de procesamiento, la unidad de generación de claves maestras 110 establece $e(g,g)^{\psi}$ en g_T. La unidad de generación de claves maestras 110 establece asimismo $\{param_{Vt}\}_{t=0,...,d}$ generado en (4) y g_T en $param_{n\rightarrow}$, donde $g_T=e(b_{t,i}, b^*_{t,i})$ para cada número entero t de t = 0, ..., d y cada número entero i de i = 1, ..., N_t.

Resumiendo, en (S101), la unidad de generación de claves maestras 110 ejecuta el algoritmo G_{ob} mostrado en la fórmula 129, y genera $param_{n\rightarrow}$ así como la base B_t y la base B^*_t para cada número entero t de t = 0, ..., d.

[Fórmula 129]

$$\mathcal{G}_{\mathsf{ob}}(1^{\lambda}, \vec{n} := (d; \vec{n} := (d; n_1,...,n_d, u_0,...,u_d, w_0,...,w_d, z_0,...,z_d)):$$
$$N_0 := 1+u_0+1+w_0+z_0,\ N_t := n_t+u_t+w_t+z_t \quad \text{for } t=1,..,d,$$
$$\mathsf{param}_{\mathbb{G}} := (q,\mathbb{G},\mathbb{G}_T,g,e) \xleftarrow{R} \mathcal{G}_{\mathsf{bpg}}(1^{\lambda}),$$
$$\psi \xleftarrow{U} \mathbb{F}_q^{\times},$$
$$\text{Para } t=0,\ldots,d,$$
$$\mathsf{param}_{\mathbb{V}_t} := (q,\mathbb{V}_t,\mathbb{G}_T,\mathbb{A}_t,e) := \mathcal{G}_{\mathsf{dpvs}}(1^{\lambda}, N_t, \mathsf{param}_{\mathbb{G}}),$$
$$X_t := (\chi_{t,i,j})_{i,j} \xleftarrow{U} GL(N_t,\mathbb{F}_q), \quad (v_{t,i,j})_{i,j} := \psi\cdot(X_t^{\mathrm{T}})^{-1},$$
$$b_{t,i} := (\chi_{t,i,1},\cdots,\chi_{t,i,N_t})_{\mathbb{A}_t} = \sum_{j=1}^{N_t}\chi_{t,i,j}a_{t,j},\ \mathbb{B}_t := (b_{t,1},\ldots,b_{t,N_t}),$$
$$b^*_{t,i} := (v_{t,i,1},\cdots,v_{t,i,N_t})_{\mathbb{A}_t} = \sum_{j=1}^{N_t}v_{t,i,j}a_{t,j},\quad \mathbb{B}^*_t := (b^*_{t,1},\ldots,b^*_{t,N_t}),$$
$$g_T := e(g,g)^{\psi},\quad \mathsf{param}^{-}_{n} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,\ldots,d}, g_T)$$
$$\text{devuelve } (\mathsf{param}^{-}_{n}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d}).$$

(S102: etapa de generación de clave pública maestra)

Utilizando el dispositivo de procesamiento, la unidad de generación de claves maestras 110 genera una base parcial $B^\wedge_0$ de la base B_0 y una base parcial $B^\wedge_t$ de la base B_t para cada número entero t de t = 1, ..., d, tal como se muestra en la fórmula 130.

[Fórmula 130]

$$\hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,1+u_0+1}, b_{0,1+u_0+1+w_0+1},\ldots, b_{0,1+u_0+1+w_0+z_0}),$$
$$\hat{\mathbb{B}}_t := (b_{t,1},..,b_{t,n_t}, b_{t,n_t+u_t+w_t+1},\ldots, b_{t,n_t+u_t+w_t+z_t}) \quad \text{para } t=1,..,d$$

La unidad de generación de claves maestras 110 designa, como una clave pública maestra pk, una combinación de la base parcial generada $B^\wedge_0$ y una base parcial $B^\wedge_t$, el parámetro de seguridad $\lambda(1^{\lambda})$ introducido en (S101), y $param_{n\rightarrow}$, los vectores de la base $b^*_{0,1+u0+1+1,\ ...,}$ $b^*_{0,1+u0+1+w0}$ (donde u0 y w0 denotan respectivamente u_0 y w_0), y los

vectores de la base $b^*_{t,nt+ut+1}$, ..., $b^*_{t,nt+ut+wt}$ (donde nt, ut y wt denotan respectivamente n_t, u_t y w_t) para cada número entero t de t = 1, ..., d generado en (S101).

(S103: etapa de generación de clave secreta maestra)

Utilizando el dispositivo de procesamiento, la unidad de generación de claves maestras 110 genera una base parcial $B^{\wedge *}_0$ de la base B^*_0 y una base parcial $B^{\wedge *}_t$ de la base B^*_t para cada número entero t de t = 1, ..., d, tal como se muestra en la fórmula 131.

[Fórmula 131]

$$\hat{\mathbb{B}}^*_0 := (b^*_{0,1}, b^*_{0,1+u_0+1}),$$

$$\hat{\mathbb{B}}^*_t := (b^*_{t,1},..,b^*_{t,n_t}) \quad \text{para } t = 1,..,d$$

La unidad de generación de claves maestras 110 designa la base parcial $B^{\wedge *}_0$ y la base parcial $B^{\wedge *}_t$ generadas como una clave secreta maestra.

(S104: etapa de almacenamiento de clave maestra)

La unidad de almacenamiento de claves maestras 120 almacena la clave pública maestra pk generada en (S102) en el dispositivo de almacenamiento. La unidad de almacenamiento de claves maestras 120 almacena asimismo la clave secreta maestra sk generada en (S103) en el dispositivo de almacenamiento.

Resumiendo, en (S101) a (S103), el dispositivo de generación de claves 100 ejecuta el algoritmo Setup mostrado en la fórmula 132, y genera la clave pública maestra pk y la clave secreta maestra sk. A continuación, en (S104), el dispositivo de generación de claves 100 almacena la clave pública maestra pk y la clave secreta maestra sk generadas, en el dispositivo de almacenamiento.

La clave pública maestra pk se hace pública por medio de una red, por ejemplo, para que esté disponible para el dispositivo de desciframiento 300.

[Fórmula 132]

$$\begin{aligned}
&\text{Setup}(1^\lambda,\ \vec{n} := (d; n_1,...,n_d, u_0,...,u_d, w_0,...,w_d, z_0,...,z_d)) : \\
&\quad (\text{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,...,d}) \xleftarrow{R} \mathcal{G}_{\text{ob}}(1^\lambda, \vec{n}), \\
&\quad \hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,1+u_0+1}, b_{0,1+u_0+1+w_0+1},..., b_{0,1+u_0+1+w_0+z_0}), \\
&\quad \hat{\mathbb{B}}_t := (b_{t,1},..,b_{t,n_t}, b_{t,n_t+u_t+w_t+1},..., b_{t,n_t+u_t+w_t+z_t}) \text{ para } t = 1,..,d, \\
&\quad \hat{\mathbb{B}}^*_0 := (b^*_{0,1}, b^*_{0,1+u_0+1}), \\
&\quad \hat{\mathbb{B}}^*_t := (b^*_{t,1},..,b^*_{t,n_t}) \text{ para } t = 1,..,d, \\
&\quad \text{pk} := (1^\lambda, \text{param}_{\vec{n}}, \{\hat{\mathbb{B}}_t\}_{t=0,...,d}, \\
&\qquad\quad b^*_{0,1+u_0+1+1},..., b^*_{0,1+u_0+1+w_0}, \{b^*_{t,n_t+u_t+1},..., b^*_{t,n_t+u_t+w_t}\}_{t=1,...,d}), \\
&\quad \text{sk} := \{\hat{\mathbb{B}}^*_t\}_{t=0,...,d}, \\
&\quad \text{devuelve pk, sk.}
\end{aligned}$$

Haciendo referencia a la figura 13, se describirá a continuación el proceso del algoritmo KeyGen ejecutado por el dispositivo de generación de claves 100.

(S201: etapa de introducción de información)

Utilizando el dispositivo de entrada, la unidad de introducción de información 130 introduce información de predicado ($\vec{v}_1$, ..., $\vec{v}_L$): = (($v_{1,i}$ (i = 1, ..., n_1)), ..., ($v_{L,i}$ (i = 1, ..., n_L))). Como información de predicado, se introduce un atributo de un usuario de una clave.

(S202: etapa de generación de números aleatorios)

Utilizando el dispositivo de procesamiento, la unidad de generación de números aleatorios 141 genera un número aleatorio ψ, números aleatorios $s_{dec,t}$, $s_{ran,j,t}$ (t = 1, ..., L), números aleatorios $\theta_{dec,t}$, $\theta_{ran,j,t}$, $\vec{\eta}_{dec,t}$, $\vec{\eta}_{ran,j,t}$ (t = 0, ..., L), números aleatorios $s_{ran,(\tau,\iota),t}$, $s_{del,(\tau,\iota),t}$ (t = 1, ..., L+1) y números aleatorios $\theta_{ran,(\tau,\iota),t}$, $\theta_{del,(\tau,\iota),t}$, $\vec{\eta}_{ran,(\tau,\iota),t}$, $\vec{\eta}_{del,(\tau,\iota),t}$ (t=0,...,L+1) para cada número entero j, τ, ι de j = 1, ..., 2L, τ de τ = L+1, ..., d y (τ,ι) = (τ,1),..., (τ,n_τ), tal como se muestra en la fórmula 133.

[Fórmula 133]

$$\text{para } j=1,...,2L;\ \tau=L+1,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau);$$

$$\psi, s_{\mathrm{dec},t}, s_{\mathrm{ran},j,t} \xleftarrow{\mathrm{U}} \mathbb{F}_q \ (t=1,...,L),$$

$$\theta_{\mathrm{dec},t}, \theta_{\mathrm{ran},j,t} \xleftarrow{\mathrm{U}} \mathbb{F}_q \ (t=0,...,L),$$

$$\vec{\eta}_{\mathrm{dec},t} := (\eta_{\mathrm{dec},t,1},...,\eta_{\mathrm{dec},t,w_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_t} \ (t=0,...,L),$$

$$\vec{\eta}_{\mathrm{ran},j,t} := (\eta_{\mathrm{ran},j,t,1},...,\eta_{\mathrm{ran},j,t,w_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_t} \ (t=0,...,L),$$

$$s_{\mathrm{ran},(\tau,\iota),t}, s_{\mathrm{del},(\tau,\iota),t} \xleftarrow{\mathrm{U}} \mathbb{F}_q \ (t=1,...,L+1),$$

$$\theta_{\mathrm{ran},(\tau,\iota),t}, \theta_{\mathrm{del},(\tau,\iota),t} \xleftarrow{\mathrm{U}} \mathbb{F}_q \ (t=0,...,L+1),$$

$$\vec{\eta}_{\mathrm{ran},(\tau,\iota),t} := (\eta_{\mathrm{ran},(\tau,\iota),t,1},...,\eta_{\mathrm{ran},(\tau,\iota),t,w_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_t} \ (t=0,...,L+1),$$

$$\vec{\eta}_{\mathrm{del},(\tau,\iota),t} := (\eta_{\mathrm{del},(\tau,\iota),t,1},...,\eta_{\mathrm{del},(\tau,\iota),t,w_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_t} \ (t=0,...,L+1)$$

Asimismo, $s_{dec,0}$, $s_{ran,j,0}$, $s_{ran,(\tau,\iota),0}$ y $s_{del,(\tau,\iota),0}$ se establecen tal como se muestra en la fórmula 134.

[Fórmula 134]

$$s_{\mathrm{dec},0} := \sum_{t=1}^{L} s_{\mathrm{dec},t},$$

$$s_{\mathrm{ran},j,0} := \sum_{t=1}^{L} s_{\mathrm{ran},j,t},$$

$$s_{\mathrm{ran},(\tau,\iota),0} := \sum_{t=1}^{L+1} s_{\mathrm{ran},(\tau,\iota),t},$$

$$s_{\mathrm{del},(\tau,\iota),0} := \sum_{t=1}^{L+1} s_{\mathrm{del},(\tau,\iota),t}$$

(S203: etapa de generación de elemento de desciframiento)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de desciframiento 142 genera un elemento de desciframiento $k^*_{L,dec}$ que es un elemento de una clave de desciframiento sk_L, tal como se muestra en la fórmula 135.

[Fórmula 135]

$$k^*_{L,\mathrm{dec}} := (\ (-s_{\mathrm{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathrm{dec},0}, 0^{z_0})_{\mathbb{B}^*_0},$$

$$(s_{\mathrm{dec},t}\ \vec{e}_{t,1} + \theta_{\mathrm{dec},t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{dec},t}, 0^{z_t})_{\mathbb{B}^*_t} : t=1,...,L)$$

Tal como se ha descrito anteriormente, para la base B y la base B* mostradas en la fórmula 110, se define la fórmula 111. De este modo, la fórmula 135 denota que los coeficientes de vectores de base de la base B^*_0 y la base B^*_t (t = 1, ..., L) se ajustan tal como se describe a continuación para generar el elemento de desciframiento de $k^*_{L,dec}$.

En primer lugar, la descripción se dirigirá a la base B^*_0. Para simplificar la notación, un vector de la base $b^*_{0,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{0,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{0,1}$, ..., $b^*_{0,3}$.

$-s_{dec,0}$ se ajusta como un coeficiente de un vector de la base 1, de la base B^*_0. 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+1, ..., $1+u_0$. 1 se ajusta como un coeficiente de un vector de la base $1+u_0+1$. $\eta_{dec,0,1}$, ..., $\eta_{dec,0,w0}$ (donde w0 denota w_0) se ajustan respectivamente como coeficientes de vectores de base $1+u_0+1+1$, ..., $1+u_0+1+w_0$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $1+u_0+1+w_0+1$, ..., $1+u_0+1+w_0+z_0$.

A continuación, la descripción se dirigirá a la base B^*_t (t = 1, ..., L). Para simplificar la notación, un vector de la base $b^*_{t,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{t,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{t,1}$, ..., $b^*_{t,3}$.

$s_{dec,t}+\theta_{dec,t}v_{t,1}$ se ajusta como un coeficiente de un vector de la base 1, de la base B^*_t (t = 1, ..., L). $\theta_{dec,t}v_{t,2}$, ..., $\theta_{dec,t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 2, ..., n_t. 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{dec,t,1}$, ..., $\eta_{dec,t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., $n_t+u_t+w_t$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_t+u_t+w_t+1$, ..., $n_t+u_t+w_t+z_t$.

(S204: etapa de generación del primer elemento de aleatorización)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de aleatorización 143 genera un primer elemento de aleatorización $k^*_{L,ran,j}$ que es un elemento de la clave de desciframiento sk_L, para cada número entero j de j=1, ..., 2L, tal como se muestra en la fórmula 136.

[Fórmula 136]

$$k^*_{L,\mathrm{ran},j} := (\ (-s_{\mathrm{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},j,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathrm{ran},j,t}\ \vec{e}_{t,1} + \theta_{\mathrm{ran},j,t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,...,L)$$

Tal como se ha descrito anteriormente, para la base B y la base B* mostradas en la fórmula 110, se define la fórmula 111. De este modo, la fórmula 136 denota que los coeficientes de vectores de base de la base B^*_0 y la base B^*_t (t = 1, ..., L) se ajustan tal como se describe a continuación para generar el primer elemento de aleatorización $k^*_{L,ran,j}$.

En primer lugar, la descripción se dirigirá a la base B^*_0. Para simplificar la notación, un vector de la base $b^*_{0,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{0,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{0,1}$, ..., $b^*_{0,3}$.

$-s_{ran,j,0}$ se ajusta como un coeficiente de un vector de la base 1, de la base de B^*_0. 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+1, ..., $1+u_0+1$. $\eta_{ran,j,0,1}$, ..., $\eta_{ran,j,0,w0}$ (donde w0 denota w_0) se ajustan respectivamente como coeficientes de vectores de base $1+u_0+1+1$, ..., $1+u_0+1+w_0$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $1+u_0+1+w_0+1$, ..., $1+u_0+1+w_0+z_0$.

A continuación, la descripción se dirigirá a la base B^*_t (t = 1, ..., L). Para simplificar la notación, un vector de la base $b^*_{t,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{t,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{t,1}$, ..., $b^*_{t,3}$.

$s_{ran,j,t}+\theta_{ran,j,t}v_{t,1}$ se ajusta como un coeficiente de un vector de la base 1, de la base B^*_t (t = 1, ..., L). $\theta_{ran,j,t}v_{t,2}$, ..., $\theta_{ran,j,t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 2, ..., n_t. 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{ran,j,t,1}$, ..., $\eta_{ran,j,t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., $n_t+u_t+w_t$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_t+u_t+w_t+1$, ..., $n_t+u_t+w_t+z_t$.

(S205: etapa de generación del segundo elemento de aleatorización)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de aleatorización 143 genera un segundo elemento de aleatorización $k^*_{L,ran,(\tau,\iota)}$ que es un elemento de la clave de desciframiento sk_L, para cada número entero τ de τ = L+1, ..., d y cada número entero ι de ι = 1, ,.., n_τ con respecto a cada número entero τ, tal como se muestra en la fórmula 137.

[Formula 137]

$$k^*_{L,\mathrm{ran},(\tau,\iota)} := (\ (-s_{\mathrm{ran},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathrm{ran},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathrm{ran},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{ran},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L$$
$$(s_{\mathrm{ran},(\tau,\iota),L+1}\ \vec{e}_{\tau,1},\ 0^{u_\tau}, \vec{\eta}_{\mathrm{ran},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau})$$

Tal como se ha descrito anteriormente, para la base B y la base B* mostradas en la fórmula 110, se define la fórmula 111. Por lo tanto, la fórmula 137 denota que los coeficientes de vectores de base de la base B^*_0, la base B^*_t (t = 1, ..., L) y una base B^*_τ se ajustan tal como se describe a continuación para generar el segundo elemento de aleatorización $k^*_{L,\mathrm{ran},(\tau,\iota)}$.

En primer lugar, la descripción se dirigirá a la base B^*_0. Para simplificar la notación, un vector de la base $b^*_{0,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{0,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{0,1}$, ..., $b^*_{0,3}$.

$-s_{\mathrm{ran},(\tau,\iota),0}$ se ajusta como un coeficiente de un vector de la base 1, de la base B^*_0. 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+1, ..., $1+u_0+1$. $\eta_{\mathrm{ran},(\tau,\iota),0,1}$, ..., $\eta_{\mathrm{ran},(\tau,\iota),0,w0}$ (donde w0 denota w_0) se ajustan respectivamente como coeficientes de vectores de base $1+u_0+1+1$, ..., $1+u_0+1+w_0$,. 0 se ajusta como un coeficiente de cada uno de los vectores de base $1+u_0+1+w_0+1$, ..., $1+u_0+1+w_0+z_0$.

A continuación, la descripción se dirigirá a la base B^*_t (t = 1, ..., L). Para simplificar la notación, un vector de la base $b^*_{t,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{t,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{t,1}$, ..., $b^*_{t,3}$.

$s_{\mathrm{ran},(\tau,\iota),t}+\theta_{\mathrm{ran},(\tau,\iota),t}v_{t,1}$ se ajusta como un coeficiente de un vector de base 1 de la base B^*_t (t = 1, ..., L). $\theta_{\mathrm{ran},(\tau,\iota),t}v_{t,2}$, ..., $\theta_{\mathrm{ran},(\tau,\iota),t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 2, ..., n_t. 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{\mathrm{ran},(\tau,\iota),t,1}$, ..., $\eta_{\mathrm{ran},(\tau,\iota),t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., $n_t+u_t+w_t$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_t+u_t+w_t+1$, ..., $n_t+u_t+w_t+z_t$.

A continuación, la descripción se dirigirá a la base B^*_τ. Para simplificar la notación, un vector de la base $b^*_{\tau,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{\tau,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{\tau,1}$, ..., $b^*_{\tau,3}$.

$s_{\mathrm{ran},(\tau,\iota),L+1}$ se ajusta como un coeficiente de un vector de base 1 de la base B^*_τ. 0 se ajusta como un coeficiente de cada uno de los vectores de base 2, ..., n_τ, ..., $n_\tau+u_\tau$. $\eta_{\mathrm{ran},(\tau,\iota),L+1,1}$, ..., $\eta_{\mathrm{ran},(\tau,\iota),L+1,w\tau}$ (donde wτ denota w_τ) se ajustan respectivamente como coeficientes de vectores de base $n_\tau+u_\tau+1$, ..., $n_\tau+u_\tau+w_\tau$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_\tau+u_\tau+w_\tau+1$, ..., $n_\tau+u_\tau+w_\tau+z_\tau$.

(S206: etapa de generación de elemento de delegación)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de delegación 144 genera un elemento de delegación $k^*_{L,\mathrm{del},(\tau,\iota)}$ que es un elemento de la clave de desciframiento sk_L, para cada número entero τ de τ = L+1, ..., d y cada número entero ι de ι = 1, ,.., n_τ con respecto a cada número entero τ, tal como se muestra en la fórmula 138.

[Fórmula 138]

$$k^*_{L,\mathrm{del},(\tau,\iota)} := (\ (-s_{\mathrm{del},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{del},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathrm{del},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathrm{del},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{del},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L$$
$$(s_{\mathrm{del},(\tau,\iota),L+1}\ \vec{e}_{\tau,1} + \psi\vec{e}_{\tau,t}, 0^{u_\tau}, \vec{\eta}_{\mathrm{del},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau})$$

Tal como se ha descrito anteriormente, para la base B y la base B* mostradas en la fórmula 110, se define la fórmula 111. De este modo, la fórmula 138 denota que los coeficientes de vectores de base de la base B^*_0 y la base B^*_t (t = 1, ..., L) se ajustan tal como se describe a continuación para generar el elemento de delegación de $k^*_{L,\mathrm{del},(\tau,\iota)}$.

En primer lugar, la descripción se dirigirá a la base B^*_0. Para simplificar la notación, un vector de la base $b^*_{0,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{0,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{0,1}$, ..., $b^*_{0,3}$.

$-s_{del,(\tau,\iota),0}$ se ajusta como un coeficiente de un vector de la base 1 cuando la base B^*_0, 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+1, ..., $1+u_0+1$. $\eta_{del,(\tau,\iota),0,1}$, ..., $\eta_{del,(\tau,\iota),0,w0}$ (donde w0 denota w_0) se ajustan respectivamente como coeficientes de vectores de base $1+u_0+1+1$, ..., $1+u_0+1+w_0$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $1+u_0+1+w_0+1$, ..., $1+u_0+1+w_0+z_0$.

A continuación, la descripción se dirigirá a la base B^*_t (t = 1, ..., L). Para simplificar la notación, un vector de la base $b^*_{t,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{t,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{t,1}$, ..., $b^*_{t,3}$.

$s_{del,(\tau,\iota),t}+\theta_{del,(\tau,\iota),t}v_{t,1}$ se ajusta como un coeficiente de un vector de base 1 de la base B^*_t (t = 1, ..., L). $\theta_{del,(\tau,\iota),t}v_{t,2}$, ..., $\theta_{del,(\tau,\iota),t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 2, ..., n_t. 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{del,(\tau,\iota),t,1}$, ..., $\eta_{del,(\tau,\iota),t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., $n_t+u_t+w_t$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_t+u_t+w_t+1$, ..., $n_t+u_t+w_t+z_t$.

A continuación, la descripción se dirigirá a la base B^*_τ. Para simplificar la notación, un vector de la base $b^*_{\tau,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{\tau,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{\tau,1}$, ..., $b^*_{\tau,3}$.

$s_{del,(\tau,\iota),L+1}\vec{e}_{\tau,1}+\psi\vec{e}_{\tau,\iota}$ se ajusta como un coeficiente de cada uno de los vectores de base 1, ..., n_τ de la base B^*_τ. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_\tau+1$, ..., $n_\tau+u_\tau$. $\eta_{del,(\tau,\iota),L+1,1}$, ..., $\eta_{del,(\tau,\iota),L+1,w\tau}$ (donde $w\tau$ denota w_τ) se ajustan respectivamente como coeficientes de vectores de base $n_\tau+u_\tau+1$, ..., $n_\tau+u_\tau+w_\tau$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_\tau+u_\tau+w_\tau+1$, ..., $n_\tau+u_\tau+w_\tau+z_\tau$.

(S207: etapa de distribución de clave)

Utilizando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de distribución de claves 150 proporciona secretamente al dispositivo de desciframiento 300 la clave de desciframiento sk_L que tiene elementos del elemento de desciframiento $k^*_{L,dec}$, el primer elemento de aleatorización $k^*_{L,ran,j}$ (j = 1, ..., 2L), el segundo elemento de aleatorización $k^*_{L,ran,(\tau,\iota)}$ (τ = L+1, ..., d; $(\tau,\iota) = (\tau,1), ..., (\tau,n_\tau)$) y el elemento de delegación $k^*_{L,del,(\tau,\iota)}$ (τ = L+1, ..., d; $(\tau,\iota) = (\tau,1), ..., (\tau,n_\tau)$). Es obvio que la clave de desciframiento sk_L se puede proporcionar al dispositivo de desciframiento 300 mediante otros métodos.

Resumiendo, en (S201) a (S206), el dispositivo de generación de claves 100 ejecuta el algoritmo KeyGen mostrado en las fórmulas 139 y 140, y genera la clave de desciframiento sk_L. A continuación, en (S207), el dispositivo de generación de claves 100 proporciona la clave de desciframiento sk_L generada al dispositivo de desciframiento 300.

[Fórmula 139]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,...,\vec{v}_L) \coloneqq (v_{1,1},...,v_{1,n_1}),...,\ (v_{L,1},...,v_{L,n_L})):$$

para $j=1,...,2L;\ \tau=L+1,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau);$

$$\psi, s_{\mathsf{dec},t}, s_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q\ \ (t=1,...,L);$$

$$\theta_{\mathsf{dec},t}, \theta_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \ \vec{\eta}_{\mathsf{dec},t},\ \ \vec{\eta}_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t}\ \ (t=0,...,L);$$

$$s_{\mathsf{ran},(\tau,\iota),t}, s_{\mathsf{del},(\tau,\iota),t} \xleftarrow{\mathsf{U}} \mathbb{F}_q\ \ (t=1,...,L+1);$$

$$\theta_{\mathsf{ran},(\tau,\iota),t}, \theta_{\mathsf{del},(\tau,\iota),t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \ \vec{\eta}_{\mathsf{ran},(\tau,\iota),t},\ \ \vec{\eta}_{\mathsf{del},(\tau,\iota),t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t},$$
$$(t=0,...,L+1);$$

$$s_{\mathsf{dec},0} \coloneqq \sum_{t=1}^{L} s_{\mathsf{dec},t},\ \ s_{\mathsf{ran},j,0} \coloneqq \sum_{t=1}^{L} s_{\mathsf{ran},j,t},$$

$$s_{\mathsf{ran},(\tau,\iota),0} \coloneqq \sum_{t=1}^{L+1} s_{\mathsf{ran},(\tau,\iota),t},\ \ s_{\mathsf{del},(\tau,\iota),0} \coloneqq \sum_{t=1}^{L+1} s_{\mathsf{del},(\tau,\iota),t},$$

[Fórmula 140]

$$k^*_{L,\mathrm{dec}} := (\ (-s_{\mathrm{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathrm{dec},0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathrm{dec},t}\ \vec{e}_{t,1} + \theta_{\mathrm{dec},t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{dec},t}, 0^{z_t})_{\mathbb{B}^*_t} : t = 1,\ldots,L),$$

$$k^*_{L,\mathrm{ran},j} := (\ (-s_{\mathrm{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},j,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathrm{ran},j,t}\ \vec{e}_{t,1} + \theta_{\mathrm{ran},j,t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L),$$

$$k^*_{L,\mathrm{ran},(\tau,\iota)} := (\ (-s_{\mathrm{ran},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathrm{ran},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathrm{ran},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{ran},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L$$
$$(s_{\mathrm{ran},(\tau,\iota),L+1}\ \vec{e}_{\tau,1}, 0^{u_\tau}, \vec{\eta}_{\mathrm{ran},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathrm{del},(\tau,\iota)} := (\ (-s_{\mathrm{del},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{del},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathrm{del},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathrm{del},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{del},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L$$
$$(s_{\mathrm{del},(\tau,\iota),L+1}\ \vec{e}_{\tau,1} + \psi\vec{e}_{\tau,\iota}, 0^{u_\tau}, \vec{\eta}_{\mathrm{del},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$\mathsf{sk}_L := (k^*_{L,\mathrm{dec}}, \{k^*_{L,\mathrm{ran},j}\}_{j=1,\ldots,2L},$$
$$\{k^*_{L,\mathrm{ran},(\tau,\iota)}\}_{\tau=L+1,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)},$$
$$\{k^*_{L,\mathrm{del},(\tau,\iota)}\}_{\tau=L+1,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}),$$

devuelve sk_L.

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

Tal como se muestra en la figura 9, el dispositivo de cifrado 200 incluye una unidad de adquisición de clave pública maestra 210, una unidad de introducción de información 220 (segunda unidad de introducción de información), una unidad de generación de texto cifrado 230 y una unidad de transmisión de datos 240.

La unidad de introducción de información 220 incluye una unidad de introducción de información de atributos 221 y una unidad de introducción de mensajes 222. La unidad de generación de texto cifrado 230 incluye una unidad de generación de números aleatorios 231, una unidad de generación de texto cifrado c1 232, y una unidad de generación de texto cifrado c2 233.

Haciendo referencia a la figura 14, se describirá el proceso del algoritmo Enc ejecutado por el dispositivo de cifrado 200.

(S301: etapa de adquisición de clave pública maestra)

Utilizando el dispositivo de comunicación y por medio de la red, por ejemplo, la unidad de adquisición de clave pública maestra 210 obtiene la clave pública maestra pk generada por el dispositivo de generación de claves 100.

(S302: etapa de introducción de información)

Utilizando el dispositivo de entrada, la unidad de introducción de información de atributos 221 introduce información de atributo ($\vec{x}_1, \ldots, \vec{x}_L$): = (($x_{1,i}$ (i = 1, ..., n_1)), ...,($x_{L,i}$ (i = 1, ...,n_L))). Como información de atributo, se introduce un atributo de una persona que puede descifrar un mensaje cifrado.

Utilizando el dispositivo de entrada, la unidad de introducción de mensajes 222 introduce un mensaje m que se tiene que cifrar.

(S303: etapa de generación de números aleatorios)

Utilizando el dispositivo de procesamiento, la unidad de generación de números aleatorios 231 genera números aleatorios ($\vec{x}_{L+1},...,\vec{x}_d$): = (($x_{L+1,i}$ (i = 1, ..., n_{L+1})), ..., ($x_{d,i}$ (i = 1, ..., n_d))) y números aleatorios ω, ζ, $\vec{\phi}_t$ (t = 0, ..., d), tal como se muestra en la fórmula 141.

[Fórmula 141]

$$(\vec{x}_{L+1},\ldots,\vec{x}_d) := ((x_{L+1,1},\ldots,x_{L+1,n_{L+1}}),\ldots,(x_{d,1},\ldots,x_{d,n_d}))$$

$$\xleftarrow{U} \mathbb{F}_q^{n_{L+1}} \times \cdots \times \mathbb{F}_q^{n_d},$$

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

$$\vec{\varphi}_t := (\varphi_{t,1},\ldots,\varphi_{t,z_t}) \xleftarrow{U} \mathbb{F}_q^{z_t} \quad (t = 0,\ldots,d)$$

(S304: etapa de generación de texto cifrado c1)

Utilizando el dispositivo de procesamiento, la unidad de generación de texto cifrado c1 232 genera un texto cifrado c_1 que es un elemento de un texto cifrado ct, tal como se muestra en la fórmula 142.

[Fórmula 142]

$$c_1 := ((\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t} : t = 1,\ldots,d)$$

Tal como se ha descrito anteriormente, para la base B y la base B* mostradas en la fórmula 110, se define la fórmula 111. Por lo tanto, la fórmula 142 denota que los coeficientes de vectores de base de la base B_0 y la base B_t (t = 1, ..., d) se ajustan tal como se describe a continuación para generar el texto cifrado c_1.

En primer lugar, la descripción se dirigirá a la base B_0. Para simplificar la notación, un vector de la base $b_{0,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b_{0,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b_{0,1}$, ..., $b_{0,3}$.

ω se ajusta como un coeficiente de un vector de base 1 de la base de B_0. 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+1, ..., 1+u_0. ζ se ajusta como un coeficiente de un vector de la base 1+u_0+1. 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+u_0+1+1, ..., 1+u_0+1+w_0. $\phi_{0,1}$, ..., $\phi_{0,z0}$ (donde z0 denota z_0) se ajustan respectivamente como coeficientes de vectores de base 1+u_0+1+w_0+1, ..., 1+u_0+1+w_0+z_0.

A continuación, la descripción se dirigirá a la base B_t (t = 1, ..., d). Para simplificar la notación, un vector de la base $b_{t,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b_{t,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b_{t,1}$, ..., $b_{t,3}$.

$\omega x_{t,1}$, ..., $\omega x_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 1, ..., n_t de la base B_t (t = 1, ..., d). 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t+w_t. $\phi_{t,1}$, ..., $\phi_{t,zt}$ (donde zt denota z_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+w_t+1, ..., n_t+u_t+w_t+z_t.

(S305: etapa de generación de texto cifrado c2)

Utilizando el dispositivo de procesamiento, la unidad de generación 233 de texto cifrado c2 genera un texto cifrado c_2 que es un elemento del texto cifrado ct, tal como se muestra en la fórmula 143.

[Fórmula 143]

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

(S306: etapa de transmisión de datos)

Utilizando el dispositivo de comunicación y por medio de la red, por ejemplo, la unidad de transmisión de datos 240 transmite al dispositivo de desciframiento 300 el texto cifrado ct utilizando el texto cifrado c_1 y el texto cifrado c_2. Es obvio que el texto cifrado ct se puede transmitir al dispositivo de desciframiento 300 mediante otros métodos.

Resumiendo, en (S301) a (S305), el dispositivo de cifrado 200 ejecuta el algoritmo Enc mostrado en la fórmula 144, y genera el texto cifrado ct. A continuación, en (S306), el dispositivo de cifrado 200 transmite el texto cifrado generado ct al dispositivo de desciframiento 300.

[Fórmula 144]

$$\mathsf{Enc}(\mathsf{pk}, m \in \mathbb{G}_T, (\vec{x}_1,\ldots,\vec{x}_L) := ((x_{1,1},\ldots,x_{1,n_1}),\ldots,(x_{L,1},\ldots,x_{L,n_L})):$$

$$(\vec{x}_{L+1},\ldots,\vec{x}_d) \xleftarrow{\cup} \mathbb{F}_q^{n_{L+1}} \times \cdots \times \mathbb{F}_q^{n_d};$$

$$\omega, \zeta \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\varphi}_t \xleftarrow{\cup} \mathbb{F}_q^{z_t}\ (t = 0,\ldots,d),$$

$$c_1 := (\ (\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t}\ : t = 1,\ldots,d),$$

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

$$\mathsf{ct} := (c_1, c_2),$$

devuelve ct.

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

Tal como se muestra en la figura 10, el dispositivo de desciframiento 300 incluye una unidad de adquisición de clave de desciframiento 310, una unidad de recepción de datos 320, una unidad de operación de emparejamiento 330 y una unidad de computación de mensajes 340.

Haciendo referencia a la figura 15, se describirá el proceso del algoritmo Dec ejecutado por el dispositivo de desciframiento 300.

(S401: etapa de adquisición de clave de desciframiento)

Utilizando el dispositivo de comunicación y por medio de la red, por ejemplo, la unidad de adquisición de clave de desciframiento 310 obtiene la clave de desciframiento sk_L. La unidad de adquisición de clave de desciframiento 310 obtiene asimismo la clave pública maestra pk generada por el dispositivo de generación de claves 100.

(S402: etapa de recepción de datos)

Utilizando el dispositivo de comunicación y por medio de la red, por ejemplo, la unidad de recepción de datos 320 recibe el texto cifrado ct transmitido por el dispositivo de cifrado 200.

(S403: etapa de operación de emparejamiento)

Utilizando el dispositivo de procesamiento, la unidad de operación de emparejamiento 330 realiza una operación de emparejamiento mostrada en la fórmula 145, y computa una clave de sesión $K = g_T^{\zeta}$.

[Fórmula 145]

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

Si el producto escalar de ($\vec{v}_1$, ..., $\vec{v}_L$) y ($\vec{x}_1$, ..., $\vec{x}_L$) es 0, la clave de sesión K se computa mediante la fórmula de computación 145.

(S404: etapa de computación de mensaje)

Utilizando el dispositivo de procesamiento, la unidad de computación de mensajes 340 computa un mensaje m'(= m) dividiendo el texto cifrado c2 por la clave de sesión K.

En resumen, en (S401) a (S404), el dispositivo de desciframiento 300 ejecuta el algoritmo Dec mostrado en la fórmula 146 y computa el mensaje m' (= m).

[Fórmula 146]

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

devuelve m'.

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

Tal como se muestra en la figura 11, el dispositivo de delegación de claves 400 incluye una unidad de adquisición de clave de desciframiento 410, una unidad de introducción de información 420 (tercera unidad de introducción de información), una unidad de generación de claves de delegación 430 y una unidad de distribución de claves 440 (unidad de transmisión de claves de delegación).

La unidad de generación de claves de delegación 430 incluye una unidad de generación de números aleatorios 431, una unidad de generación de elementos de desciframiento de nivel inferior 432, una unidad de generación de elementos de aleatorización de nivel inferior 433 y una unidad de generación de elementos de delegación de nivel inferior 434.

Haciendo referencia a la figura 16, se describirá el proceso del algoritmo $\mathsf{Delegate}_L$ ejecutado por el dispositivo de delegación de claves 400.

(S501: etapa de adquisición de clave de desciframiento)

Utilizando el dispositivo de comunicación y por medio de la red, por ejemplo, la unidad de adquisición de clave de desciframiento 410 obtiene la clave de desciframiento sk_L. La unidad de adquisición de clave de desciframiento 410 obtiene asimismo la clave pública maestra pk generada por el dispositivo de generación de claves 100.

(S502: etapa de introducción de información)

Utilizando el dispositivo de entrada, la unidad de introducción de información 420 introduce información de predicado $\vec{v}_{L+1}$: = ($v_{L+1,i}$ (i = 1, ..., n_{L+1})). Como información de predicado, se introduce un atributo de una persona a la que se delega la clave.

(S503: etapa de generación de números aleatorios)

Utilizando el dispositivo de procesamiento, la unidad de generación de números aleatorios 431 genera números aleatorios $\alpha_{\mathsf{dec},j}$, σ_{dec}, $\alpha_{\mathsf{ran},j',j}$, $\sigma_{\mathsf{ran},j'}$, $\alpha_{\mathsf{ran},(\tau,\iota),j}$, $\sigma_{\mathsf{ran},(\tau,\iota)}$, $\phi_{\mathsf{ran},(\tau,\iota)}$, $\alpha_{\mathsf{del},(\tau,\iota),j}$, $\sigma_{\mathsf{del},(\tau,\iota)}$, $\phi_{\mathsf{del},(\tau,\iota)}$, ψ', $\eta_{\mathsf{dec},(t,i)}$, $\eta_{\mathsf{ran},j',(t,i)}$, $\eta_{\mathsf{ran},(\tau,\iota),(t,i)}$, $\eta_{\mathsf{del},(\tau,\iota),(t,i)}$ para cada número entero j, j', 1, t, t, i de j = 1, ..., 2L, j' = 1, ..., 2(L+1), τ = L+2, ..., d, (τ,ι) = (τ,1), ..., (τ,n_τ), t = 0, ..., L+1, τ, (t,i) = (t,1), ..., (t,n_t), tal como se muestra en la fórmula 147.

[Fórmula 147]

$$\text{para } j = 1,\ldots,2L;\ j' = 1,\ldots,2(L+1);\ \tau = L+2,\ldots,d;\ (\tau,\iota) = (\tau,1),\ldots,(\tau,n_\tau);$$
$$t = 0,\ldots,L+1,\tau;\ (t,i) = (t,1),\ldots,(t,w_t);$$
$$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota),j},\sigma_{\mathsf{ran},(\tau,\iota)},$$
$$\phi_{\mathsf{ran},(\tau,\iota)},\ \alpha_{\mathsf{del},(\tau,\iota),j},\ \sigma_{\mathsf{del},(\tau,\iota)},\ \phi_{\mathsf{del},(\tau,\iota)},\ \psi',$$
$$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota),(t,i)} \xleftarrow{\mathsf{U}} \mathbb{F}_q$$

(S504: etapa de generación de elemento de desciframiento de nivel inferior)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de desciframiento de nivel inferior 432 genera un elemento de desciframiento de nivel inferior $k^*_{L+1,\mathsf{dec}}$ que es un elemento de una clave de delegación sk_{L+1}, tal como se muestra en la fórmula 148.

[Fórmula 148]

$$k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + \sum_{j=1}^{2L} \alpha_{\mathsf{dec},j} k^*_{L,\mathsf{ran},j}$$
$$+ \sigma_{\mathsf{dec}} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)}\right) + \sum_{i=1}^{w_t} \eta_{\mathsf{dec},(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{dec},(t,i)} b^*_{t,n_t+u_t+i}$$

(S505: etapa de generación del primer elemento de aleatorización de nivel inferior)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de aleatorización de nivel inferior 433 genera un primer elemento de aleatorización de nivel inferior $k^*_{L+1,ran,j'}$ que es un elemento de la clave de delegación sk_{L+1}, para cada número entero j' de j' = 1, ..., 2(L+1), tal como se muestra en la fórmula 149.

[Fórmula 149]

$$k^*_{L+1,\mathrm{ran},j'} := \sum_{j=1}^{2L} \alpha_{\mathrm{ran},j',j} k^*_{L,\mathrm{ran},j} + \sigma_{\mathrm{ran},j'} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)} \right) + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(t,i)} b^*_{t,n_t+u_t+i}$$

(S506: etapa de generación del segundo elemento de aleatorización de nivel inferior)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de aleatorización de nivel inferior 433 genera un segundo elemento de aleatorización de nivel inferior $k^*_{L+1,ran,(\tau,\iota)}$ que es un elemento de la clave de delegación sk_{L+1}, para cada número entero τ de τ = L+2, ..., d y cada número entero ι de ι = 1, ..., n_τ con respecto a cada número entero τ, tal como se muestra en la fórmula 150.

[Fórmula 150]

$$k^*_{L+1,\mathrm{ran},(\tau,\iota)} := \sum_{j=1}^{2L} \alpha_{\mathrm{ran},(\tau,\iota),j} k^*_{L,\mathrm{ran},j} + \sigma_{\mathrm{ran},(\tau,\iota)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)} \right) + \phi_{\mathrm{ran},(\tau,\iota)} k^*_{L,\mathrm{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{ran},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}$$

(S507: etapa de generación de elemento de delegación de nivel inferior)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de delegación de nivel inferior 434 genera un elemento de delegación de nivel inferior $k^*_{L+1,del,(\tau,\iota)}$ que es un elemento de la clave de delegación sk_{L+1} para cada número entero τ de τ = L+2, ..., d y cada número entero ι de ι = 1, ..., n_τ, con respecto a cada número entero τ, tal como se muestra en la fórmula 151.

[Fórmula 151]

$$k^*_{L+1,\mathrm{del},(\tau,\iota)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del},(\tau,\iota),j} k^*_{L,\mathrm{ran},j} + \sigma_{\mathrm{del},(\tau,\iota)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)} \right) + \psi' k^*_{L,\mathrm{del},(\tau,\iota)} + \phi_{\mathrm{del},(\tau,\iota)} k^*_{L,\mathrm{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$

(S508: etapa de distribución de clave)

Utilizando el dispositivo de comunicación, y a través de la red, por ejemplo, la unidad de distribución de claves 150 proporciona secretamente al dispositivo de desciframiento de nivel inferior 300 la clave de delegación sk_{L+1} (clave de desciframiento de nivel inferior) que tiene elementos del elemento de desciframiento de nivel inferior $k^*_{L+1,dec}$, el primer elemento de aleatorización de nivel inferior $k^*_{L+1,ran,j'}$ (j' = 1, ..., 2(L+1)), el segundo elemento de aleatorización de nivel inferior $k^*_{L+1,ran,(\tau,\iota)}$ (τ = L+2, ..., d; (τ,ι) = (τ,1), ..., (τ,n_τ)) y el elemento de delegación de nivel inferior $k^*_{L+1,del,(\tau,\iota)}$ (τ = L+2, ..., d; (τ,ι) = (τ,1), ..., (τ,n_τ)). Es obvio que la clave de delegación sk_{L+1} se puede proporcionar al dispositivo de desciframiento de nivel inferior 300 mediante otros métodos.

Resumiendo, en (S501) a (S507), el dispositivo de delegación de claves 400 ejecuta el algoritmo $Delegate_L$ mostrado en las fórmulas 152 y 153, y genera la clave de delegación de sk_{L+1}. A continuación, en (S508), el dispositivo de delegación de claves 400 proporciona la clave de delegación generada sk_{L+1} al dispositivo de desciframiento de nivel inferior 300.

[Fórmula 152]

$$\mathsf{Delegate}_L(\mathsf{pk},\mathsf{sk}_L,\vec{v}_{L+1} := (v_{L+1,1},\ldots,v_{L+1,n_{L+1}})):$$

$$\text{para } j=1,\ldots,2L;\ j'=1,\ldots,2(L+1);\ \tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau);$$

$$t=0,\ldots,L+1,\tau;\ (t,i)=(t,1),\ldots,(t,w_t);$$

$$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota),j},\ \sigma_{\mathsf{ran},(\tau,\iota)},$$

$$\phi_{\mathsf{ran},(\tau,\iota)},\ \alpha_{\mathsf{del},(\tau,\iota),j},\ \sigma_{\mathsf{del},(\tau,\iota)},\ \phi_{\mathsf{del},(\tau,\iota)},\ \psi',$$

$$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota),(t,i)} \xleftarrow{U} \mathbb{F}_q,$$

[Fórmula 153]

$$k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + \sum_{j=1}^{2L} \alpha_{\mathsf{dec},j}\, k^*_{L,\mathsf{ran},j}$$
$$+ \sigma_{\mathsf{dec}} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)}\Big) + \sum_{i=1}^{w_t} \eta_{\mathsf{dec},(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{dec},(t,i)} b^*_{t,n_t+u_t+i},$$
$$k^*_{L+1,\mathsf{ran},j'} := \sum_{j=1}^{2L} \alpha_{\mathsf{ran},j',j}\, k^*_{L,\mathsf{ran},j}$$
$$+ \sigma_{\mathsf{ran},j'} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)}\Big) + \sum_{i=1}^{w_t} \eta_{\mathsf{ran},j',(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{ran},j',(t,i)} b^*_{t,n_t+u_t+i},$$
$$k^*_{L+1,\mathsf{ran},(\tau,\iota)} := \sum_{j=1}^{2L} \alpha_{\mathsf{ran},(\tau,\iota),j}\, k^*_{L,\mathsf{ran},j}$$
$$+ \sigma_{\mathsf{ran},(\tau,\iota)} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)}\Big)$$
$$+ \phi_{\mathsf{ran},(\tau,\iota)} k^*_{L,\mathsf{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathsf{ran},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{ran},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathsf{ran},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$
$$k^*_{L+1,\mathsf{del},(\tau,\iota)} := \sum_{j=1}^{2L} \alpha_{\mathsf{del},(\tau,\iota),j}\, k^*_{L,\mathsf{ran},j}$$
$$+ \sigma_{\mathsf{del},(\tau,\iota)} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)}\Big) + \psi' k^*_{L,\mathsf{del},(\tau,\iota)}$$
$$+ \phi_{\mathsf{del},(\tau,\iota)} k^*_{L,\mathsf{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathsf{del},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{del},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathsf{del},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$
$$\mathsf{sk}_{L+1} := (k^*_{L+1,\mathsf{dec}}, \{k^*_{L+1,\mathsf{ran},j'}\}_{j'=1,\ldots,2(L+1)},$$
$$\{k^*_{L+1,\mathsf{ran},(\tau,\iota)}, k^*_{L+1,\mathsf{del},(\tau,\iota)}\}_{\tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}),$$

devuelve sk_{L+1}

Cuando el dispositivo de desciframiento de nivel inferior 300 ejecuta el algoritmo Dec utilizando la clave de delegación de sk_{L+1}, la clave de sesión K se computa en (S403) de la figura 15 mediante la computación de la fórmula 145 si el producto escalar de ($\vec{v}_1$, ..., $\vec{v}_{L+1}$) y ($\vec{x}_1$, ..., $\vec{x}_{L+1}$) es 0.

Tal como se ha descrito anteriormente, el sistema de procesamiento criptográfico 10 acorde con la primera realización implementa el esquema HPE para productos escalares de d niveles utilizando el número (d+1) de espacios N_t (t = 0, ..., d)-dimensionales. Los espacios requeridos para los procesos criptográficos al nivel L-ésimo (1 ≤ L ≤ d) son el número (L + 1) de espacios N_t (t = 0, ..., L)-dimensionales. Por lo tanto, los tamaños de las claves pueden ser pequeños, y se puede mejorar la eficiencia de las operaciones, etc. Se hacen pequeñas también las áreas de memoria y de registros y similares para almacenar claves.

En la descripción anterior, se proporcionan dimensiones u_t, w_t, y z_t (t = 0, ..., d) para una mayor seguridad. Por lo tanto, al precio de una seguridad reducida, se pueden omitir las dimensiones u_t, w_t y z_t (t = 0, ..., d) ajustando u_t, w_t y z_t (t = 0, ..., d) respectivamente a 0.

En la descripción anterior, $1+u_0+1+w_0+z_0$ se ajusta en N_0 y $n_t+u_t+w_t+z_t$ se ajusta en N_t. Sin embargo, $1+u_0+1+w_0+z_0$ puede ser sustituido por 1+1+1+1+1, de tal modo que 5 se ajusta en N_0, y $n_t+u_t+w_t+z_t$ puede ser sustituido por $n_t+n_t+n_t+1$, de tal modo que $3n_t+1$ se ajusta en N_t.

En este caso, el algoritmo Setup mostrado en la fórmula 132 se reescribe tal como se muestra en la fórmula 154. G_{ob} se reescribe tal como se muestra en la fórmula 155.

[Fórmula 154]

$$\mathsf{Setup}(1^\lambda,\ \vec{n} := (d; n_1,...,n_d):\ \ (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,...,d}) \xleftarrow{R} \mathcal{G}_{ob}(1^\lambda, \vec{n}),$$

$$\hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,3}, b_{0,5}),\ \hat{\mathbb{B}}_t := (b_{t,1},..,b_{t,n_t}, b_{t,3n_t+1}) \text{ para } t = 1,..,d,$$

$$\hat{\mathbb{B}}_0^* := (b_{0,1}^*, b_{0,3}^*),\ \hat{\mathbb{B}}_t^* := (b_{t,1}^*,..,b_{t,n_t}^*) \text{para } t = 1,..,d,$$

$$\mathsf{pk} := (1^\lambda, \mathsf{param}_{\vec{n}}, \{\hat{\mathbb{B}}_t\}_{t=0,...,d}, b_{0,4}^*, \{b_{t,2n_t+1}^*,...,b_{t,3n_t}^*\}_{t=1,...,d}),$$

$$\mathsf{sk} := \{\hat{\mathbb{B}}_t^*\}_{t=0,...,d},$$

devuelve pk, sk.

[Fórmula 155]

$$\mathcal{G}_{ob}(1^\lambda, \vec{n} := (d; n_1,...,n_d)):$$

$$N_0 := 5,\ N_t := 3n_t + 1\ (t = 1,...,d),$$

$$\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, g, e) \xleftarrow{R} \mathcal{G}_{bpg}(1^\lambda),$$

$$\psi \xleftarrow{U} \mathbb{F}_q^\times,$$

Para $t = 0,\ldots,d$,

$$\mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{dpvs}(1^\lambda, N_t, \mathsf{param}_{\mathbb{G}}),$$

$$X_t := (\chi_{t,i,j})_{i,j} \xleftarrow{U} GL(N_t, \mathbb{F}_q),\quad (\nu_{t,i,j})_{i,j} := \psi \cdot (X_t^{\mathrm{T}})^{-1},$$

$$b_{t,i} := (\chi_{t,i,1}, \cdots, \chi_{t,i,N_t})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \chi_{t,i,j} a_{t,j},\ \mathbb{B}_t := (b_{t,1},\ldots,b_{t,N_t}),$$

$$b_{t,i}^* := (\nu_{t,i,1}, \cdots, \nu_{t,i,N_t})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \nu_{t,i,j} a_{t,j},\ \mathbb{B}_t^* := (b_{t,1}^*,\ldots,b_{t,N_t}^*),$$

$$g_T := e(g,g)^\psi,\quad \mathsf{param}_{\vec{n}}^- := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=1,..,d}, g_T)$$

devuelve $(\mathsf{param}_{\vec{n}}^-, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,..,d})$.

El algoritmo KeyGen mostrado en las fórmulas 139 y 140 se reescribe tal como se muestra las fórmulas 156 y 157.

[Fórmula 156]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,...,\vec{v}_L) := (v_{1,1},...,v_{1,n_1}),...,\ (v_{L,1},...,v_{L,n_L})):$$

para $j=1,...,2L;\ \tau=L+1,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau);$

$$\psi, s_{\mathsf{dec},t}, s_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q\ (t=1,...,L);$$

$$\theta_{\mathsf{dec},t}, \theta_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\eta}_{\mathsf{dec},t},\ \vec{\eta}_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}\ (t=0,...,L);$$

$$s_{\mathsf{ran},(\tau,\iota),t}, s_{\mathsf{del},(\tau,\iota),t} \xleftarrow{\mathsf{U}} \mathbb{F}_q\ (t=1,...,L+1);$$

$$\theta_{\mathsf{ran},(\tau,\iota),t}, \theta_{\mathsf{del},(\tau,\iota),t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\eta}_{\mathsf{ran},(\tau,\iota),t},\ \vec{\eta}_{\mathsf{del},(\tau,\iota),t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t},$$
$$(t=0,...,L+1);$$

$$s_{\mathsf{dec},0} := \sum_{t=1}^{L} s_{\mathsf{dec},t},\ s_{\mathsf{ran},j,0} := \sum_{t=1}^{L} s_{\mathsf{ran},j,t},$$

$$s_{\mathsf{ran},(\tau,\iota),0} := \sum_{t=1}^{L+1} s_{\mathsf{ran},(\tau,\iota),t},\ s_{\mathsf{del},(\tau,\iota),0} := \sum_{t=1}^{L+1} s_{\mathsf{del},(\tau,\iota),t},$$

[Fórmula 157]

$$k^*_{L,\mathsf{dec}} := (\ (-s_{\mathsf{dec},0},0,1,\eta_{\mathsf{dec},0},0)_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{dec},t}\ \vec{e}_{t,1} + \theta_{\mathsf{dec},t}\vec{v}_t,\ 0^{n_t},\vec{\eta}_{\mathsf{dec},t},0)_{\mathbb{B}^*_t} : t=1,...,L),$$

$$k^*_{L,\mathsf{ran},j} := (\ (-s_{\mathsf{ran},j,0},0,0,\eta_{\mathsf{ran},j,0},0)_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{ran},j,t}\ \vec{e}_{t,1} + \theta_{\mathsf{ran},j,t}\vec{v}_t,\ 0^{n_t},\vec{\eta}_{\mathsf{ran},j,t},0)_{\mathbb{B}^*_t}$$
$$: t=1,...,L),$$

$$k^*_{L,\mathsf{ran},(\tau,\iota)} := (\ (-s_{\mathsf{ran},(\tau,\iota),0},0,0,\eta_{\mathsf{ran},(\tau,\iota),0},0)_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{ran},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathsf{ran},(\tau,\iota),t}\vec{v}_t,\ 0^{n_t},\vec{\eta}_{\mathsf{ran},(\tau,\iota),t},0)_{\mathbb{B}^*_t}$$
$$: t=1,...,L$$
$$(s_{\mathsf{ran},(\tau,\iota),L+1}\ \vec{e}_{\tau,1},\ 0^{n_\tau},\vec{\eta}_{\mathsf{ran},(\tau,\iota),L+1},0)_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,\iota)} := (\ (-s_{\mathsf{del},(\tau,\iota),0},0,0,\eta_{\mathsf{del},(\tau,\iota),0},0)_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{del},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathsf{del},(\tau,\iota),t}\vec{v}_t,\ 0^{n_t},\vec{\eta}_{\mathsf{del},(\tau,\iota),t},0)_{\mathbb{B}^*_t}$$
$$: t=1,...,L$$
$$(s_{\mathsf{del},(\tau,\iota),L+1}\ \vec{e}_{\tau,1} + \psi\vec{e}_{\tau,\iota},0^{n_\tau},\vec{\eta}_{\mathsf{del},(\tau,\iota),L+1},0)_{\mathbb{B}^*_\tau}),$$

$$\mathsf{sk}_L := (k^*_{L,\mathsf{dec}}, \{k^*_{L,\mathsf{ran},j}\}_{j=1,...,2L},$$
$$\{k^*_{L,\mathsf{ran},(\tau,\iota)}\}_{\tau=L+1,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau)},$$
$$\{k^*_{L,\mathsf{del},(\tau,\iota)}\}_{\tau=L+1,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau)}),$$

devuelve sk_L.

El algoritmo Enc mostrado en la fórmula 144 se reescribe tal como se muestra en la fórmula 158.

[Fórmula 158]

$$\mathsf{Enc}(\mathsf{pk}, m \in \mathbb{G}_T, (\vec{x}_1,\ldots,\vec{x}_L) := ((x_{1,1},\ldots,x_{1,n_1}),\ldots,(x_{L,1},\ldots,x_{L,n_L})):$$

$$(\vec{x}_{L+1},\ldots,\vec{x}_d) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_{L+1}} \times \cdots \times \mathbb{F}_q^{n_d};\ \ \omega,\zeta,\varphi_0,\ldots,\varphi_d \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$c_1 := (\ (\omega,0,\zeta,0,\varphi_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{n_t}, 0^{n_t}, \varphi_t)_{\mathbb{B}t} : t = 1,\ldots,d),$$

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

$$\mathsf{ct} := (c_1, c_2),$$

devuelve ct.

El algoritmo $\mathsf{Delegate}_L$ mostrado en las fórmulas 152 y 153 se reescribe tal como se muestra en las fórmulas 159 y 160.

[Fórmula 159]

$$\mathsf{Delegate}_L(\mathsf{pk}, \mathsf{sk}_L, \vec{v}_{L+1} := (v_{L+1,1},\ldots,v_{L+1,n_{L+1}})):$$

para $j = 1,\ldots,2L;\ j' = 1,\ldots,2(L+1);\ \tau = L+2,\ldots,d;\ (\tau,\iota) = (\tau,1),\ldots,(\tau,n_\tau);$

$t = 0,\ldots,L+1,\tau;\ (t,i) = (t,1),\ldots,(t,n_t);$

$$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota),j},\ \sigma_{\mathsf{ran},(\tau,\iota)},$$

$$\phi_{\mathsf{ran},(\tau,\iota)},\ \alpha_{\mathsf{del},(\tau,\iota),j},\ \sigma_{\mathsf{del},(\tau,\iota)},\ \phi_{\mathsf{del},(\tau,\iota)},\ \psi',$$

$$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota),(t,i)} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

[Fórmula 160]

$$k^*_{L+1,\mathrm{dec}} := k^*_{L,\mathrm{dec}} + \sum_{j=1}^{2L} \alpha_{\mathrm{dec},j}\, k^*_{L,\mathrm{ran},j}$$
$$+ \sigma_{\mathrm{dec}} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)}\Big) + \eta_{\mathrm{dec},(0,1)} b^*_{0,4}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathrm{dec},(t,i)} b^*_{t,2n_t+i},$$
$$k^*_{L+1,\mathrm{ran},j'} := \sum_{j=1}^{2L} \alpha_{\mathrm{ran},j',j}\, k^*_{L,\mathrm{ran},j}$$
$$+ \sigma_{\mathrm{ran},j'} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)}\Big) + \eta_{\mathrm{ran},j',(0,1)} b^*_{0,4}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathrm{ran},j',(t,i)} b^*_{t,2n_t+i},$$
$$k^*_{L+1,\mathrm{ran},(\tau,\iota)} := \sum_{j=1}^{2L} \alpha_{\mathrm{ran},(\tau,\iota),j}\, k^*_{L,\mathrm{ran},j}$$
$$+ \sigma_{\mathrm{ran},(\tau,\iota)} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)}\Big)$$
$$+ \phi_{\mathrm{ran},(\tau,\iota)} k^*_{L,\mathrm{ran},(\tau,\iota)} + \eta_{\mathrm{ran},(\tau,\iota),(0,1)} b^*_{0,4}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathrm{ran},(\tau,\iota),(t,i)} b^*_{t,2n_t+i}$$
$$+ \sum_{i=1}^{n_\tau} \eta_{\mathrm{ran},(\tau,\iota),(\tau,i)} b^*_{\tau,2n_\tau+i},$$
$$k^*_{L+1,\mathrm{del},(\tau,\iota)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del},(\tau,\iota),j}\, k^*_{L,\mathrm{ran},j}$$
$$+ \sigma_{\mathrm{del},(\tau,\iota)} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)}\Big) + \psi' k^*_{L,\mathrm{del},(\tau,\iota)}$$
$$+ \phi_{\mathrm{del},(\tau,\iota)} k^*_{L,\mathrm{ran},(\tau,\iota)} + \eta_{\mathrm{del},(\tau,\iota),(0,1)} b^*_{0,4}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathrm{del},(\tau,\iota),(t,i)} b^*_{t,2n_t+i}$$
$$+ \sum_{i=1}^{n_\tau} \eta_{\mathrm{del},(\tau,\iota),(\tau,i)} b^*_{\tau,2n_\tau+i},$$
$$\mathsf{sk}_{L+1} := \big(k^*_{L+1,\mathrm{dec}}, \{k^*_{L+1,\mathrm{ran},j'}\}_{j'=1,\ldots,2(L+1)},$$
$$\{k^*_{L+1,\mathrm{ran},(\tau,\iota)}, k^*_{L+1,\mathrm{del},(\tau,\iota)}\}_{\tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}\big),$$

devuelve sk_{L+1}

El algoritmo Dec mostrado en la fórmula 146 permanece igual.

El algoritmo Setup tiene que ser ejecutado una vez cuando se configura el sistema de procesamiento criptográfico 10, y no se tiene que ejecutar cada vez que se genera una clave de desciframiento. En la descripción anterior, el algoritmo Setup y el algoritmo KeyGen son ejecutados por el dispositivo de generación de claves 100. Sin embargo, el algoritmo Setup y el algoritmo KeyGen pueden ser ejecutados por dispositivos diferentes.

Segunda realización

En esta realización, se describirá una versión generalizada del esquema HPE para productos escalares discutido en la primera realización.

En el esquema HPE para productos escalares discutido en la primera realización, un texto cifrado ct puede ser descifrado mediante una clave de desciframiento, como regla general, si el producto escalar de una información de atributo ajustada en el texto cifrado ct y una información de predicado ajustada en la clave de desciframiento es 0.

Sin embargo, en el esquema HPE para productos escalares que se va discutir en la segunda realización, se puede disponer que el desciframiento es posible incluso si el producto escalar de la información de atributo ajustada en el texto cifrado ct y la información de predicado ajustada en la clave de desciframiento no es 0.

Específicamente, en la siguiente descripción, el desciframiento es posible si el producto escalar de la información de atributo $\vec{x}_t$ y la información de predicado $\vec{v}_t$ es 0 para cada número entero t de ρ_t (t = 1, ..., d) que tiene el valor de 0 y si el producto escalar de la información de atributo $\vec{x}_t$ y la información de predicado $\vec{v}_t$ no es 0 para cada número entero t de ρ_t (t = 1, ..., d) que tiene el valor de 1.

Con esta disposición, es posible ajustar una expresión condicional positiva (por ejemplo, información de atributo = información de predicado) o una expresión condicional negativa (información de atributo ≠ información de predicado), dependiendo del ajuste del valor de ρ_t (t = 1, ..., d).

Haciendo referencia a las figuras 17 y 19, se describirá el esquema HPE para productos escalares acorde con la segunda realización, y se describirán funciones y operaciones del sistema de procesamiento criptográfico 10 que implementa el esquema HPE para productos escalares.

La configuración funcional del sistema de procesamiento criptográfico 10 acorde con la segunda realización es la misma que la configuración funcional del sistema de procesamiento criptográfico 10 acorde con la primera realización mostrada en las figuras 8 a 11.

La figura 17 es un diagrama de flujo que muestra operaciones del dispositivo de generación de claves 100 y muestra un proceso del algoritmo KeyGen. La figura 18 es un diagrama de flujo que muestra operaciones del dispositivo de desciframiento 300 y muestra un proceso del algoritmo Dec. La figura 19 es un diagrama de flujo que muestra operaciones del dispositivo de delegación de claves 400 y muestra un proceso del algoritmo Delegate_L.

Los procesos del algoritmo Setup y del algoritmo Enc acorde con la segunda realización son iguales que los procesos del algoritmo Setup y el algoritmo Enc acordes con la primera realización, de tal modo que se omitirá la descripción. En el algoritmo Enc, sin embargo, un texto cifrado ct para transmitir al dispositivo de desciframiento 300 incluye no solo textos cifrados c_1 y c_2 sino asimismo información de atributo $\vec{x}_i$ (i = 1, ..., L).

Haciendo referencia a la figura 17, se describirá a continuación el proceso del algoritmo KeyGen ejecutado por el dispositivo de generación de claves 100.

(S601: etapa de introducción de información)

Utilizando el dispositivo de entrada, la unidad de introducción de información 130 introduce información de predicado $((\vec{v}_1,\rho_1), ..., (\vec{v}_L,\rho_L))$: = $((v_{1,i}\ (i = 1, ..., n_1), \rho_1 \in \{0,1\}), ..., (v_{L,i}\ (i = 1, ..., n_L), \rho_L \in \{0,1\}))$. Como información de predicado, se introduce un atributo de un usuario de una clave.

(S602: etapa de generación de números aleatorios)

Utilizando el dispositivo de procesamiento, la unidad de generación de números aleatorios 141 genera un número aleatorio ψ, números aleatorios $s_{dec,t}$, $s_{ran,j,t}$ (t = 1, ..., L), números aleatorios $\theta_{dec,t}$, $\theta_{ran,j,t}$, $\vec{\eta}_{dec,t}$, $\vec{\eta}_{ran,j,t}$, $\vec{\eta}_{ran,0,t}$, $\vec{\eta}_{del,0,t}$, $\vec{\eta}_{del,1,t}$ (t = 0, ..., L), números aleatorios $s_{ran,0,t}$, $s_{del,0,t}$, $s_{del,1,t}$ (t = 0, ..., L+1), números aleatorios $\theta_{ran,0,t}$, $\theta_{del,0,t}$, $\theta_{del,1,t}$ (t = 0, ..., L+1) y números aleatorios $\vec{\eta}_{ran,(\tau,\iota)}$, $\vec{\eta}_{del,0,(\tau,\iota)}$, $\vec{\eta}_{del,1,(\tau,\iota)}$ para cada uno de los números enteros j, τ, ι de j = 1, ..., 2L, τ = L+1, ..., d, (τ,ι) = (τ,1), ..., (τ,n_τ), tal como se456+

muestra en la fórmula 161.

[Fórmula 161]

$$\text{para} j=1,\ldots,2L;\ \tau=L+1,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau);$$

$$\psi, s_{\text{dec},t}, s_{\text{ran},j,t} \xleftarrow{U} \mathbb{F}_q\ (t=1,\ldots,L),$$

$$\theta_{\text{dec},t}, \theta_{\text{ran},j,t} \xleftarrow{U} \mathbb{F}_q\ (t=0,\ldots,L),$$

$$\vec{\eta}_{\text{dec},t} := (\eta_{\text{dec},t,1},\ldots,\eta_{\text{dec},t,w_t}) \xleftarrow{U} \mathbb{F}_q^{w_t}\ (t=0,\ldots,L),$$

$$\vec{\eta}_{\text{ran},j,t} := (\eta_{\text{ran},j,t,1},\ldots,\eta_{\text{ran},j,t,w_t}) \xleftarrow{U} \mathbb{F}_q^{w_t}\ (t=0,\ldots,L),$$

$$\vec{\eta}_{\text{ran},0,t} := (\eta_{\text{ran},0,t,1},\ldots,\eta_{\text{ran},0,t,w_t}) \xleftarrow{U} \mathbb{F}_q^{w_t}\ (t=0,\ldots,L),$$

$$\vec{\eta}_{\text{del},0,t} := (\eta_{\text{del},0,t,1},\ldots,\eta_{\text{del},0,t,w_t}) \xleftarrow{U} \mathbb{F}_q^{w_t}\ (t=0,\ldots,L),$$

$$\vec{\eta}_{\text{del},1,t} := (\eta_{\text{del},1,t,1},\ldots,\eta_{\text{del},1,t,w_t}) \xleftarrow{U} \mathbb{F}_q^{w_t}\ (t=0,\ldots,L),$$

$$s_{\text{ran},0,t}, s_{\text{del},0,t}, s_{\text{del},1,t} \xleftarrow{U} \mathbb{F}_q\ (t=1,\ldots,L+1),$$

$$\theta_{\text{ran},0,t}, \theta_{\text{del},0,t}, \theta_{\text{del},1,t} \xleftarrow{U} \mathbb{F}_q\ (t=0,\ldots,L+1),$$

$$\vec{\eta}_{\text{ran},0,(\tau,\iota)} := (\eta_{\text{ran},0,(\tau,\iota),1},\ldots,\eta_{\text{ran},0,(\tau,\iota),w_t}) \xleftarrow{U} \mathbb{F}_q^{w_t},$$

$$\vec{\eta}_{\text{del},0,(\tau,\iota)} := (\eta_{\text{del},0,(\tau,\iota),1},\ldots,\eta_{\text{del},0,(\tau,\iota),w_t}) \xleftarrow{U} \mathbb{F}_q^{w_t},$$

$$\vec{\eta}_{\text{del},1,(\tau,\iota)} := (\eta_{\text{del},1,(\tau,\iota),1},\ldots,\eta_{\text{del},1,(\tau,\iota),w_t}) \xleftarrow{U} \mathbb{F}_q^{w_t}$$

$s_{dec,0}$, $s_{ran,j,0}$, $s_{ran,0,0}$, $s_{del,0,0}$ y $s_{del,1,0}$ se ajustan tal como se muestra en la fórmula 162.

[Fórmula 162]

$$s_{\text{dec},0} := \sum_{t=1}^{L} s_{\text{dec},t},$$

$$s_{\text{ran},j,0} := \sum_{t=1}^{L} s_{\text{ran},j,t},$$

$$s_{\text{ran},0,0} := \sum_{t=1}^{L} s_{\text{ran},0,t},$$

$$s_{\text{del},0,0} := \sum_{t=1}^{L+1} s_{\text{del},0,t},$$

$$s_{\text{del},1,0} := \sum_{t=1}^{L+1} s_{\text{del},1,t}$$

(S603: etapa de generación de elemento de desciframiento)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de desciframiento 142 genera un elemento de desciframiento $k^*_{L,dec}$ que es un elemento de una clave de desciframiento sk_L, tal como se muestra en la fórmula 163.

[Fórmula 163]

$$k^*_{L,\mathrm{dec}} := (\ (-s_{\mathrm{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathrm{dec},0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathrm{dec},t}\vec{e}_{t,1} + \theta_{\mathrm{dec},t,}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{dec},t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathrm{dec},t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{dec},t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, ..., L)$$

Tal como se ha descrito anteriormente, para la base B y la base B* mostradas en la fórmula 110, se define la fórmula 111. De este modo, la fórmula 163 denota que los coeficientes de vectores de base de la base B^*_0 y la base B^*_t (t = 1, ..., L) se ajustan tal como se describe a continuación para generar el elemento de desciframiento de $k^*_{L,\mathrm{dec}}$.

En primer lugar, la descripción se dirigirá a la base B^*_0. Para simplificar la notación, un vector de la base $b^*_{0,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{0,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{0,1}$, ..., $b^*_{0,3}$.

$-s_{\mathrm{dec},0}$ se ajusta como un coeficiente de un vector de base 1 de la base B^*_0. 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+1, ..., $1+u_0$. 1 se ajusta como un coeficiente de un vector de la base $1+u_0+1$. $\eta_{\mathrm{dec},0,1}$, ..., $\eta_{\mathrm{dec},0,w0}$ (donde w0 denota w_0) se ajustan respectivamente como coeficientes de vectores de base $1+u_0+1+1$, ..., $1+u_0+1+w_0$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $1+u_0+1+w_0+1$, ..., $1+u_0+1+w_0+z_0$.

A continuación, la descripción se dirigirá a la base B^*_t (t = 1, ..., L). Para simplificar la notación, un vector de la base $b^*_{t,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{t,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{t,1}$, ..., $b^*_{t,3}$. Los ajustes de la base B^*_t (t = 1, ..., L) varían en función de si el valor de ρ_t es 0 o 1.

Cuando el valor de ρ_t es 0, $s_{\mathrm{dec},t}+\theta_{\mathrm{dec},t}v_{t,1}$ se ajusta como un coeficiente de un vector de base 1 de la base B^*_t (t = 1, ..., L). $\theta_{\mathrm{dec},t}v_{t,2}$, ..., $\theta_{\mathrm{dec},t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 2, ..., n_t. 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{\mathrm{dec},t,1}$, ..., $\eta_{\mathrm{dec},t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., $n_t+u_t+w_t$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_t+u_t+w_t+1$, ..., $n_t+u_t+w_t+z_t$.

Por otra parte, cuando el valor de ρ_t es 1, $s_{\mathrm{dec},t}v_{t,1}$, ..., $s_{\mathrm{dec},t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 1, ..., n_t de la base B^*_t (t = 1, ..., L) 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{\mathrm{dec},t,1}$, ..., $\eta_{\mathrm{dec},t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., $n_t+u_t+w_t$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_t+u_t+w_t+1$, ..., $n_t+u_t+w_t+z_t$.

(S604: etapa de generación del primer elemento de aleatorización)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de aleatorización 143 genera un primer elemento de aleatorización $k^*_{L,\mathrm{ran},j}$ que es un elemento de la clave de desciframiento sk_L, para cada número entero j de j=1, ..., 2L, tal como se muestra en la fórmula 164.

[Fórmula 164]

$$k^*_{L,\mathrm{ran},j} := (\ (-s_{\mathrm{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},j,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathrm{ran},j,t}\vec{e}_{t,1} + \theta_{\mathrm{ran},j,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathrm{ran},j,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, ..., L)$$

Tal como se ha descrito anteriormente, para la base B y la base B* mostradas en la fórmula 110, se define la fórmula 111. De este modo, la fórmula 164 denota que los coeficientes de vectores de base de la base B^*_0 y la base B^*_t (t = 1, ..., L) se ajustan tal como se describe a continuación para generar el primer elemento de aleatorización $k^*_{L,\mathrm{ran},j}$.

En primer lugar, la descripción se dirigirá a la base B^*_0. Para simplificar la notación, un vector de la base $b^*_{0,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{0,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{0,1}$, ..., $b^*_{0,3}$.

-$s_{ran,j,0}$ se ajusta como un coeficiente de un vector de la base 1, de la base de B^*_0. 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+1, ..., 1+u_0+1. $\eta_{ran,j,0,1}$, ..., $\eta_{ran,j,0,w0}$ (donde w0 denota w_0) se ajustan respectivamente como coeficientes de vectores de base 1+u_0+1+1, ..., 1+u_0+1+w_0. 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+u_0+1+w_0+1, ..., 1+u_0+1+w_0+z_0.

A continuación, la descripción se dirigirá a la base B^*_t (t = 1, ..., L). Para simplificar la notación, un vector de la base $b^*_{t,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{t,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{t,1}$, ..., $b^*_{t,3}$. Los ajustes de la base B^*_t (t = 1, ..., L) varían en función de si el valor de ρ_t es 0 o 1.

Cuando el valor de ρ_t es 0, $s_{ran,j,t}$+$\theta_{ran,j,t}v_{t,1}$ se ajusta como un coeficiente de un vector de base 1 de la base B^*_t (t = 1, ..., L). $\theta_{ranj,t}v_{t,2}$, ..., $\theta_{ran,j,t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 2, ..., n_t. 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{ran,j,t,1}$, ..., $\eta_{ran,j,t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., n_t+u_t+w_t. 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+u_t+w_t+1, ..., n_t+u_t+w_t+z_t.

Por otra parte, cuando el valor de ρ_t es 1, $s_{ran,j,t}v_{t,1}$, ..., $s_{ran,j,t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 1, ..., n_t de la base B^*_t (t = 1, ..., L) 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{ran,j,t,1}$, ..., $\eta_{ran,j,t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., n_t+u_t+w_t. 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+u_t+w_t+1, ..., n_t+u_t+w_t+z_t.

(S605: etapa de generación del segundo elemento de aleatorización)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de aleatorización 143 genera un segundo elemento de aleatorización $k^*_{L,ran,(\tau,\iota,0)}$ que es un elemento de la clave de desciframiento sk_L, para cada número entero τ de τ = L+1, ..., d y cada número entero ι de ι = 1, ,.., n_τ con respecto a cada número entero τ, tal como se muestra en la fórmula 165.

[Fórmula 165]

$$k^*_{L,\mathrm{ran},(\tau,\iota,0)} := \Big((-s_{\mathrm{ran},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},0,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathrm{ran},0,t}\vec{e}_{t,1} + \theta_{\mathrm{ran},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{ran},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathrm{ran},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{ran},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathrm{ran},0,L+1}\vec{e}_{\tau,1}, 0^{u_\tau}, \vec{\eta}_{\mathrm{ran},0,(\tau,\iota)}, 0^{z_\tau})_{\mathbb{B}^*_\tau})$$

Tal como se ha descrito anteriormente, para la base B y la base B* mostradas en la fórmula 110, se define la fórmula 111. Por lo tanto, la fórmula 165 denota que los coeficientes de vectores de base de la base B^*_0, la base B^*_t (t = 1, ..., L) y la base B^*_τ se ajustan tal como se describe a continuación para generar el segundo elemento de aleatorización $k^*_{L,ran,(\tau,\iota,0)}$.

En primer lugar, la descripción se dirigirá a la base B^*_0. Para simplificar la notación, un vector de la base $b^*_{0,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{0,i}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{0,1}$, ..., $b^*_{0,3}$.

-$s_{ran,0,0}$ se ajusta como un coeficiente de un vector de la base 1, de la base de B^*_0. 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+1, ..., 1+u_0+1. $\eta_{ran,0,0,1}$, ..., $\eta_{ran,0,0,w0}$ (donde w0 denota w_0) se ajustan respectivamente como coeficientes de vectores de base 1+u_0+1+1, ..., 1+u_0+1+w_0. 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+u_0+1+w_0+1, ..., 1+u_0+1+w_0+z_0.

A continuación, la descripción se dirigirá a la base B^*_t (t = 1, ..., L). Para simplificar la notación, un vector de la base $b^*_{t,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{t,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{t,1}$, ..., $b^*_{t,3}$. Los ajustes de la base B^*_t (t = 1, ..., L) varían en función de si el valor de ρ_t es 0 o 1.

Cuando el valor de ρ_t es 0, $s_{ran,0,t}$+$\theta_{ran,0,t}v_{t,1}$ se ajusta como un coeficiente de un vector de base 1 de la base B^*_t (t = 1, ..., L). $\theta_{ran,0,t}v_{t,2}$, ..., $\theta_{ran,0,t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 2, ..., n_t. 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{ran,0,t,1}$, ..., $\eta_{ran,0,t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., n_t+u_t+w_t. 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+u_t+w_t+1, ..., n_t+u_t+w_t+z_t.

Por otra parte, cuando el valor de ρ_t es 1, $s_{ran,0,t}v_{t,1}$, ..., $s_{ran,0,t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 1, ..., n_t de la base B^*_t (t = 1, ..., L) 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{ran,0,t,1}$, ..., $\eta_{ran,0,t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., $n_t+u_t+w_t$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_t+u_t+w_t+1$, ..., $n_t+u_t+w_t+z_t$.

A continuación, la descripción se dirigirá a la base B^*_τ. Para simplificar la notación, un vector de la base $b^*_{\tau,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{\tau,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{\tau,1}$, ..., $b^*_{\tau,3}$.

$s_{ran,0,L+1}$ se ajusta como un coeficiente de un vector de base 1 de la base de B^*_τ. 0 se ajusta como un coeficiente de cada uno de los vectores de base 2, ..., n_τ, ..., $n_\tau+u_\tau$. $\eta_{ran,0,(\tau,\iota),1}$, ..., $\eta_{ran,0,(\tau,\iota)s,w\tau}$ (donde wτ denota w_τ) se ajustan respectivamente como coeficientes de vectores de base $n_\tau+u_\tau+1$, ..., $n_\tau+u_\tau+w_\tau$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_\tau+u_\tau+w_\tau+1$, ..., $n_\tau+u_\tau+w_\tau+z_\tau$.

(S606: etapa de generación del primer elemento de delegación)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de delegación 144 genera un primer elemento de delegación $k^*_{L,del,(\tau,\iota,0)}$ que es un elemento de la clave de desciframiento sk_L, para cada número entero τ de τ = L+1, ..., d y cada número entero ι de ι = 1, ,.., n_τ con respecto a cada número entero τ, tal como se muestra en la fórmula 166.

[Fórmula 166]

$$k^*_{L,\mathrm{del},(\tau,\iota,0)} := ((-s_{\mathrm{del},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{del},0,0}, 0^{z_0})_{\mathbb{B}^*_0}, \left\{ \begin{array}{ll} (s_{\mathrm{del},0,t}\vec{e}_{t,1} + \theta_{\mathrm{del},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{del},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathrm{del},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{del},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\} : t = 1, ..., L), (s_{\mathrm{del},0,L+1}\vec{e}_{\tau,1}, +\psi\vec{e}_{\tau,t}, 0^{u_\tau}, \vec{\eta}_{\mathrm{del},0,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^*_\tau})$$

Tal como se ha descrito anteriormente, para la base B y la base B* mostradas en la fórmula 110, se define la fórmula 111. Por lo tanto, la fórmula 166 denota que los coeficientes de vectores de base de la base B^*_0, la base B^*_t (t = 1, ..., L) y la base B^*_τ se ajustan tal como se describe a continuación para generar el primer elemento de delegación $k^*_{L,del,(\tau,\iota,0)}$.

En primer lugar, la descripción se dirigirá a la base B^*_0. Para simplificar la notación, un vector de la base $b^*_{0,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{0,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{0,1}$, ..., $b^*_{0,3}$.

$-s_{del,0,0}$ se ajusta como un coeficiente de un vector de la base 1, de la base de B^*_0. 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+1, ..., $1+u_0+1$. $\eta_{del,0,0,1}$, ..., $\eta_{del,0,0,w0}$ (donde w0 denota w_0) se ajustan respectivamente como coeficientes de vectores de base $1+u_0+1+1$, ..., $1+u_0+1+w_0$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $1+u_0+1+w_0+1$, ..., $1+u_0+1+w_0+z_0$.

A continuación, la descripción se dirigirá a la base B^*_t (t = 1, ..., L). Para simplificar la notación, un vector de la base $b^*_{t,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{t,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{t,1}$, ..., $b^*_{t,3}$. Los ajustes de la base B^*_t (t = 1, ..., L) varían en función de si el valor de ρ_t es 0 o 1.

Cuando el valor de ρ_t es 0, $s_{del,0,t}+\theta_{del,0,t}v_{t,1}$ se ajusta como un coeficiente de un vector de base 1 de la base B^*_t (t = 1, ..., L). $\theta_{del,0,t}v_{t,2}$, ..., $\theta_{del,0,t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 2, ..., n_t. 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{del,0,t,1}$, ..., $\eta_{del,0,t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., $n_t+u_t+w_t$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_t+u_t+w_t+1$, ..., $n_t+u_t+w_t+z_t$.

Por otra parte, cuando el valor de ρ_t es 1, $s_{del,0,t}v_{t,1}$, ..., $s_{del,0,t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 1, ..., n_t de la base B^*_t (t = 1, ..., L) 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{del,0,t,1}$, ..., $\eta_{del,0,t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., $n_t+u_t+w_t$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_t+u_t+w_t+1$, ..., $n_t+u_t+w_t+z_t$.

A continuación, la descripción se dirigirá a la base B^*_τ. Para simplificar la notación, un vector de la base $b^*_{\tau,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{\tau,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{\tau,i}$, ..., $b^*_{\tau,3}$.

$s_{del,0,L+1}\vec{e}_{\tau,1}+\psi\vec{e}_{\tau,\iota}$ se ajusta como un coeficiente de vector de la base 1, ..., n_τ de la base B^*_τ. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_\tau+1$, ..., $n_\tau+u_\tau$. $\eta_{del,0,(\tau,\iota),1}$, ..., $\eta_{del,0,(\tau,\iota),w\tau}$ (donde wτ denota w_τ) se ajustan respectivamente como coeficientes de vectores de base $n_\tau+u_\tau+1$, ..., $n_\tau+u_\tau+w_\tau$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_\tau+u_\tau+w_\tau+1$, ..., $n_\tau+u_\tau+w_\tau+z_\tau$.

(S607: etapa de generación del segundo elemento de delegación)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de delegación 144 genera un segundo elemento de delegación $k^*_{L,del,(\tau,\iota,1)}$ que es un elemento de la clave de desciframiento sk_L, para cada número entero τ de τ = L+1, ..., d y cada número entero ι de ι = 1, ,.., n_τ con respecto a cada número entero τ, tal como se muestra en la fórmula 167.

[Fórmula 167]

$$k^*_{L,\mathrm{del},(\tau,\iota,1)} := (\ (-s_{\mathrm{del},1,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{del},1,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{\begin{array}{ll}(s_{\mathrm{del},1,t}\vec{e}_{t,1}+\theta_{\mathrm{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{del},1,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0\\ (s_{\mathrm{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{del},1,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1\end{array}\right\}$$
$$: t = 1,\ldots,L),$$
$$(s_{\mathrm{del},1,L+1}\vec{e}_{\tau,\iota}, 0^{u_\tau}, \vec{\eta}_{\mathrm{del},1,(\tau,\iota)}, 0^{z_\tau})_{\mathbb{B}^*_\tau})$$

Tal como se ha descrito anteriormente, para la base B y la base B* mostradas en la fórmula 110, se define la fórmula 111. Por lo tanto, la fórmula 167 denota que los coeficientes de vectores de base de la base B^*_0, la base B^*_t (t = 1, ..., L) y la base B^*_τ se ajustan tal como se describe a continuación para generar el segundo elemento de delegación $k^*_{L,del,(\tau,\iota,1)}$.

En primer lugar, la descripción se dirigirá a la base B^*_0. Para simplificar la notación, un vector de la base $b^*_{0,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{0,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{0,1}$, ..., $b^*_{0,3}$.

$-s_{del,1,0}$ se ajusta como un coeficiente de un vector de la base 1, de la base de B^*_0. 0 se ajusta como un coeficiente de cada uno de los vectores de base 1+1, ..., $1+u_0+1$. $\eta_{del,1,0,1}$, ..., $\eta_{del,1,0,w0}$ (donde w0 denota w_0) se ajustan respectivamente como coeficientes de vectores de base $1+u_0+1+1$, ..., $1+u_0+1+w_0$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $1+u_0+1+w_0+1$, ..., $1+u_0+1+w_0+z_0$.

A continuación, la descripción se dirigirá a la base B^*_t (t = 1, ..., L). Para simplificar la notación, un vector de la base $b^*_{t,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{t,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{t,1}$, ..., $b^*_{t,3}$. Los ajustes de la base B*t (t = 1, ..., L) varían en función de si el valor de ρ_t es 0 o 1.

Cuando el valor de ρ_t es 0, $s_{del,1,t}+\theta_{del,1,t}v_{t,1}$ se ajusta como un coeficiente de un vector de base 1 de la base B^*_t (t = 1, ..., L). $\theta_{del,1,t}v_{t,2}$, ..., $\theta_{del,1,t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 2, ..., n_t. 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{del,1,1,t,1}$, ..., $\eta_{del,1,t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., $n_t+u_t+w_t$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_t+u_t+w_t+1$, ..., $n_t+u_t+w_t+z_t$.

Por otra parte, cuando el valor de ρ_t es 1, $s_{del,1,t}v_{t,1}$, ..., $S_{del,1,t}v_{t,nt}$ (donde nt denota n_t) se ajustan respectivamente como coeficientes de vectores de base 1, ..., n_t de la base B^*_t (t = 1, ..., L). 0 se ajusta como un coeficiente de cada uno de los vectores de base n_t+1, ..., n_t+u_t. $\eta_{del,1,t,1}$, ..., $\eta_{del,1,t,wt}$ (donde wt denota w_t) se ajustan respectivamente como coeficientes de vectores de base n_t+u_t+1, ..., $n_t+u_t+w_t$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_t+u_t+w_t+1$, ..., $n_t+u_t+w_t+z_t$.

A continuación, la descripción se dirigirá a la base B^*_τ. Para simplificar la notación, un vector de la base $b^*_{\tau,i}$ se identifica utilizando solamente la parte i. Por ejemplo, un vector de la base 1 denota un vector de la base $b^*_{\tau,1}$. Los vectores de la base 1, ..., 3 denotan vectores de la base $b^*_{\tau,1}$, ..., $b^*_{\tau,3}$.

$s_{del,L+1}\vec{e}_{\tau,\iota}$ se ajusta como un coeficiente de vectores de base 1, ..., n_τ, de la base B^*_τ. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_\tau+1$, ..., $n_\tau+u_\tau$. $\eta_{del,1,(\tau,\iota),1}$, ..., $\eta_{del,1,(\tau,\iota),w\tau}$ (donde wτ denota w_τ) se ajustan respectivamente como coeficientes de vectores de base $n_\tau+u_\tau+1$, ..., $n_\tau+u_\tau+w_\tau$. 0 se ajusta como un coeficiente de cada uno de los vectores de base $n_\tau+u_\tau+w_\tau+1$, ..., $n_\tau+u_\tau+w_\tau+z_\tau$.

(S608: etapa de distribución de clave)

Utilizando el dispositivo de comunicación y por medio de la red, por ejemplo, la unidad de distribución de claves 150 proporciona secretamente al dispositivo de desciframiento 300 la clave de desciframiento sk_L que tiene elementos del elemento de desciframiento $k^*_{L,dec}$, el primer elemento de aleatorización $k^*_{L,ran,j}$ (j = 1, ..., 2L), el segundo elemento de aleatorización $k^*_{L,ran,(\tau,I,0)}$ (τ = L+1, ..., d; (τ,I) = (τ,1), ..., (τ,n_τ)), el primer elemento de delegación $k^*_{L,del,(\tau,I,0)}$ (τ = L+1, ..., d; (τ,I) = (τ,1), ..., (τ,n_τ)) y el segundo elemento de delegación $k^*_{L,del,(\tau,I,1)}$ (τ = L+1, ..., d; (τ,I) = (τ,1), ..., (τ,η_τ)). Es obvio que la clave de desciframiento sk_L se puede proporcionar al dispositivo de desciframiento 300 mediante otros métodos.

Resumiendo, en (S601) a (S607), el dispositivo de generación de claves 100 ejecuta el algoritmo KeyGen mostrado en las fórmulas 168 y 169, y genera la clave de desciframiento sk_L. A continuación, en (S608), el dispositivo de generación de claves 100 proporciona la clave de desciframiento sk_L generada al dispositivo de desciframiento 300.

[Fórmula 168]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,\rho_1),...,(\vec{v}_L,\rho_L)) := (((v_{1,1},...,v_{1,n_1}) \in \mathbb{F}_q^{n_1}, \rho_1 \in \{0,1\}),...,$$

$$((v_{L,1},...,v_{L,n_L}) \in \mathbb{F}_q^{n_L}, \rho_L \in \{0,1\})):$$

para $j = 1,...,2L;\ \tau = L+1,...,d;\ (\tau,\iota) = (\tau,1),...,(\tau,n_\tau);$

$$\psi, s_{\mathsf{dec},t}, s_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ (t = 1,...,L);$$

$$\theta_{\mathsf{dec},t}, \theta_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\vec{\eta}_{\mathsf{dec},t},\ \vec{\eta}_{\mathsf{ran},j,t},\ \vec{\eta}_{\mathsf{ran},0,t},\ \vec{\eta}_{\mathsf{del},0,t}\ \vec{\eta}_{\mathsf{del},1,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t} \quad (t = 0,...,L);$$

$$s_{\mathsf{ran},0,t}, s_{\mathsf{del},0,t}, s_{\mathsf{del},1,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\theta_{\mathsf{ran},0,t}, \theta_{\mathsf{del},0,t}, \theta_{\mathsf{del},1,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\vec{\eta}_{\mathsf{ran},0,(\tau,\iota)},\ \vec{\eta}_{\mathsf{del},0,(\tau,\iota)},\ \vec{\eta}_{\mathsf{del},1,(\tau,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t}\ , (t = 0,...,L+1);$$

$$s_{\mathsf{dec},0} := \sum_{t=1}^{L} s_{\mathsf{dec},t},\ s_{\mathsf{ran},j,0} := \sum_{t=1}^{L} s_{\mathsf{ran},j,t},\ s_{\mathsf{ran},0,0} := \sum_{t=1}^{L} s_{\mathsf{ran},0,t},$$

$$s_{\mathsf{del},0,0} := \sum_{t=1}^{L+1} s_{\mathsf{del},0,t},\ s_{\mathsf{del},1,0} := \sum_{t=1}^{L+1} s_{\mathsf{del},1,t},$$

$$k^*_{L,\mathsf{dec}} := (\ (-s_{\mathsf{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathsf{dec},0}, 0^{z_0})_{\mathbb{B}_0^*},$$

$$\left\{ \begin{array}{ll} (s_{\mathsf{dec},t}\vec{e}_{t,1} + \theta_{\mathsf{dec},t}, \vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{dec},t}, 0^{z_t})_{\mathbb{B}_t^*}, & \text{si } \rho_t = 0 \\ (s_{\mathsf{dec},t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{dec},t}, 0^{z_t})_{\mathbb{B}_t^*}, & \text{si } \rho_t = 1 \end{array} \right\}$$

$$: t = 1,...,L),$$

$$k^*_{L,\mathsf{ran},j} := (\ (-s_{\mathsf{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},j,0}, 0^{z_0})_{\mathbb{B}_0^*},$$

$$\left\{ \begin{array}{ll} (s_{\mathsf{ran},j,t}\vec{e}_{t,1} + \theta_{\mathsf{ran},j,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{ran},j,t}, 0^{z_t})_{\mathbb{B}_t^*}, & \text{si } \rho_t = 0 \\ (s_{\mathsf{ran},j,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{ran},j,t}, 0^{z_t})_{\mathbb{B}_t^*}, & \text{si } \rho_t = 1 \end{array} \right\}$$

$$: t = 1,...,L),$$

[Fórmula 169]

$$k^*_{L,\mathsf{ran},(\tau,\iota,0)} := ((-s_{\mathsf{ran},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},0,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathsf{ran},0,t}\vec{e}_{t,1} + \theta_{\mathsf{ran},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{ran},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathsf{ran},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{ran},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathsf{ran},0,L+1}\vec{e}_{\tau,1}, 0^{u_\tau}, \vec{\eta}_{\mathsf{ran},0,(\tau,\iota)}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,\iota,0)} := ((-s_{\mathsf{del},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{del},0,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathsf{del},0,t}\vec{e}_{t,1} + \theta_{\mathsf{del},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathsf{del},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathsf{del},0,L+1}\vec{e}_{\tau,1}, +\psi\vec{e}_{\tau,\iota}, 0^{u_\tau}, \vec{\eta}_{\mathsf{del},0,(\tau,\iota)}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,\iota,1)} := ((-s_{\mathsf{del},1,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{del},1,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathsf{del},1,t}\vec{e}_{t,1} + \theta_{\mathsf{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},1,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathsf{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},1,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathsf{del},1,L+1}\vec{e}_{\tau,\iota}, 0^{u_\tau}, \vec{\eta}_{\mathsf{del},1,(\tau,\iota)}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$\mathsf{sk}_L := (((\vec{v}_1, \rho_1), \ldots, (\vec{v}_L, \rho_L));$$
$$k^*_{L,\mathsf{dec}}, \{k^*_{L,\mathsf{ran},j}\}_{j=1,\ldots,2L}, \{k^*_{L,\mathsf{ran},(\tau,\iota,0)}, k^*_{L,\mathsf{del},(\tau,\iota,0)}, k^*_{L,\mathsf{del},(\tau,\iota,1)}\}$$
$$\tau = L+1, \ldots, d; (\tau,\iota) = (\tau,1), \ldots, (\tau,n_\tau)),$$

devuelve sk_L.

Haciendo referencia a la figura 18, se describirá el proceso del algoritmo Dec ejecutado por el dispositivo de desciframiento 300.

(S701: etapa de adquisición de clave de desciframiento)

Utilizando el dispositivo de comunicación y por medio de la red, por ejemplo, la unidad de adquisición de clave de desciframiento 310 obtiene la clave de desciframiento sk_L. La unidad de adquisición de clave de desciframiento 310 obtiene asimismo la clave pública maestra pk generada por el dispositivo de generación de claves 100.

(S702: etapa de recepción de datos)

Utilizando el dispositivo de comunicación y por medio de la red, por ejemplo, la unidad de recepción de datos 320 recibe el texto cifrado ct transmitido por el dispositivo de cifrado 200.

(S703: etapa de operación de emparejamiento)

Utilizando el dispositivo de procesamiento, la unidad de operación de emparejamiento 330 realiza una operación de emparejamiento mostrada en la fórmula 170, y computa una clave de sesión $K = g_T^{\zeta}$.

[Fórmula 170]

$$K := e(c_{1,0}, k^*_{L,\mathsf{dec},0}) \cdot \prod_{1 \le t \le d \wedge \rho_t = 0} e(c_{1,t}, k^*_{L,\mathsf{dec},t}) \cdot \prod_{1 \le t \le d \wedge \rho_t = 1} e(c_{1,t}, k^*_{L,\mathsf{dec},t})^{1/(\vec{v}_t \cdot \vec{x}_t)}$$

En este caso, se define la fórmula 171.

[Fórmula 171]

$$(k^*_{L,\mathsf{dec},0} \in \langle \mathbb{B}^*_0 \rangle, \ldots, k^*_{L,\mathsf{dec},d} \in \langle \mathbb{B}^*_d \rangle) := k^*_{L,\mathsf{dec}},$$

$$(c_{1,0} \in \langle \mathbb{B}^*_0 \rangle, \ldots, c_{1,d} \in \langle \mathbb{B}^*_d \rangle := c_1$$

La clave de sesión K se calcula calculando la fórmula 170 si el producto escalar de $\vec{v}_t$ y $\vec{x}_t$ es 0 para cada número entero t de $\rho_t = 0$ y si el producto escalar de $\vec{v}_t$ y $\vec{x}_t$ no es 0 para cada número entero t de $\rho_t = 1$ con respecto a cada número entero t de t = 1, ..., L.

(S704: etapa de computación de mensaje)

Utilizando el dispositivo de procesamiento, la unidad de computación de mensajes 340 divide el texto cifrado c2 por la clave de sesión K, y calcula de ese modo un mensaje m' (= m).

En resumen, en (S701) a (S704), el dispositivo de desciframiento 300 ejecuta el algoritmo Dec mostrado en la fórmula 172 y calcula el mensaje m' (= m).

[Fórmula 172]

$$\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_L, \mathsf{ct}):$$

$$K := e(c_{1,0}, k^*_{L,\mathsf{dec},0}) \cdot \prod_{1 \le t \le d \wedge \rho_t = 0} e(c_{1,t}, k^*_{L,\mathsf{dec},t}) \cdot \prod_{1 \le t \le d \wedge \rho_t = 1} e(c_{1,t}, k^*_{L,\mathsf{dec},t})^{1/(\vec{v}_t \cdot \vec{x}_t)},$$

donde $(k^*_{L,\mathsf{dec},0} \in \langle \mathbb{B}^*_0 \rangle, \ldots, k^*_{L,\mathsf{dec},d} \in \langle \mathbb{B}^*_d \rangle) := k^*_{L,\mathsf{dec}},$

$(c_{1,0} \in \langle \mathbb{B}^*_0 \rangle, \ldots, c_{1,d} \in \langle \mathbb{B}^*_d \rangle := c_1,$

$m' := c_2 / K,$

devuelve m'.

Haciendo referencia a la figura 19, se describirá el proceso del algoritmo $\mathsf{Delegate}_L$ ejecutado por el dispositivo de delegación de claves 400.

(S801: etapa de adquisición de clave de desciframiento)

Utilizando el dispositivo de comunicación y por medio de la red, por ejemplo, la unidad de adquisición de clave de desciframiento 410 obtiene la clave de desciframiento sk_L. La unidad de adquisición de clave de desciframiento 410 obtiene asimismo la clave pública maestra pk generada por el dispositivo de generación de claves 100.

(S802: etapa de introducción de información)

Utilizando el dispositivo de entrada, la unidad de introducción de información 420 introduce información de predicado ($v^{\rightarrow}_{L+1}$, ρ_{L+1}): = ($v_{L+1,i}$ (i = 1, ..., n_{L+1}), $\rho_{L+1} \in \{0,1\}$). Como información de predicado, se introduce un atributo de una persona a la que se delega la clave.

(S803: etapa de generación de números aleatorios)

Utilizando el dispositivo de procesamiento, la unidad de generación de números aleatorios 431 genera números aleatorios $\alpha_{dec,j}$, σ_{dec}, $\alpha_{ran,j',j}$, $\sigma_{ran,j'}$, $\alpha_{ran,(\tau,\iota,0),j}$, $\sigma_{ran,(\tau,\iota,0)}$, $\phi_{ran,(\tau,\iota,0)}$, $\alpha_{del,(\tau,\iota,0),j}$, $\sigma_{del,(\tau,\iota,0)}$, $\phi_{del,(\tau,\iota,0)}$, $\alpha_{del,(\tau,\iota,0),j}$, $\sigma_{del,(\tau,\iota,1)}$, $\phi_{del,(\tau,\iota,1)}$, $\eta_{dec,(t,i)}$, $\eta_{ran,j',(t,i)}$, $\eta_{ran,(\tau,\iota,0),(t,i)}$, $\eta_{del,(\tau,\iota,0),(t,i)}$, $\eta_{del,(\tau,\iota,0),(t,i)}$, ψ_0, ψ_1 para cada número entero j, j', τ, ι, t, i de j = 1, ..., 2L, j' = 1, ..., 2(L+1), τ = L+2, ..., d, (τ,ι) = (τ,1), ..., (τ,n_τ), t = 0, ..., L+1, τ, (t,i) = (t,1), ..., (t,n_t), tal como se muestra en la fórmula 173.

[Fórmula 173]

$$\text{para } j=1,...,2L;\ j'=1,...,2(L+1);\ \tau=L+2,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau);$$
$$t=0,...,L+1,\tau;\ (t,i)=(t,1),...,(t,w_t);$$
$$\alpha_{\mathrm{dec},j},\ \sigma_{\mathrm{dec}},\ \alpha_{\mathrm{ran},j',j},\ \sigma_{\mathrm{ran},j'},\ \alpha_{\mathrm{ran},(\tau,\iota,0),j},\ \sigma_{\mathrm{ran},(\tau,\iota,0)},$$
$$\phi_{\mathrm{ran},(\tau,\iota,0)},\ \alpha_{\mathrm{del},(\tau,\iota,0),j},\ \sigma_{\mathrm{del},(\tau,\iota,0)},\ \phi_{\mathrm{del},(\tau,\iota,0)},\ \alpha_{\mathrm{del},(\tau,\iota,1),j},$$
$$\sigma_{\mathrm{del},(\tau,\iota,1)},\ \phi_{\mathrm{del},(\tau,\iota,1)},\ \eta_{\mathrm{dec},(t,i)},\ \eta_{\mathrm{ran},j',(t,i)},\ \eta_{\mathrm{ran},(\tau,\iota,0),(t,i)},$$
$$\eta_{\mathrm{del},(\tau,\iota,0),(t,i)},\ \eta_{\mathrm{del},(\tau,\iota,1),(t,i)},\ \psi_0,\psi_1,\xleftarrow{\mathrm{U}}\mathbb{F}_q$$

(S804: etapa de generación de elemento de desciframiento de nivel inferior)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de desciframiento de nivel inferior 432 genera un elemento de desciframiento de nivel inferior $k^*_{L+1,dec}$ que es un elemento de una clave de delegación sk_{L+1}, tal como se muestra en la fórmula 174.

[Fórmula 174]

$$k^*_{L+1,\mathrm{dec}} := k^*_{L,\mathrm{dec}} + \sum_{j=1}^{2L} \alpha_{\mathrm{dec},j} k^*_{L,\mathrm{ran},j}$$
$$+ \left\{ \begin{array}{ll} (\sigma_{\mathrm{dec}}(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{si } \rho_t = 0 \\ (\sigma_{\mathrm{dec}}([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i}[k^*_{L,\mathrm{del},(L+1,i,1)}]_L) & \text{si } \rho_t = 1 \end{array} \right\}$$
$$+ \sum_{i=1}^{w_t} \eta_{\mathrm{dec},(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{dec},(t,i)} b^*_{t,n_t+u_t+i}$$

(S805: etapa de generación del primer elemento de aleatorización de nivel inferior)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de aleatorización de nivel inferior 433 genera un primer elemento de aleatorización de nivel inferior $k^*_{L+1,ran,j'}$ que es un elemento de la clave de delegación sk_{L+1}, para cada número entero j' de j' = 1, ..., 2(L+1), tal como se muestra en la fórmula 175.

[Fórmula 175]

$$k^{*}_{L+1,\mathrm{ran},j'} := \sum_{j=1}^{2L} \alpha_{\mathrm{ran},j',j} k^{*}_{L,\mathrm{ran},j} + \left\{ \begin{array}{ll} \sigma_{\mathrm{ran},j'}\left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i,0)}\right) & \text{si } \rho_t = 0 \\ \sigma_{\mathrm{ran},j'}\left([k^{*}_{L,\mathrm{del},(L+1,i,1)}]^{L} + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^{*}_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}\right) & \text{si } \rho_t = 1 \end{array} \right\} + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(t,i)} b^{*}_{t,n_t+u_t+i}$$

(S806: etapa de generación del segundo elemento de aleatorización de nivel inferior)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de aleatorización de nivel inferior 433 genera un segundo elemento de aleatorización de nivel inferior $k^{*}_{L+1,\mathrm{ran},(\tau,\iota)}$ que es un elemento de la clave de delegación sk_{L+1}, para cada número entero τ de τ = L+2, ..., d y cada número entero ι de ι = 1, ..., n_τ con respecto a cada número entero τ, tal como se muestra en la fórmula 176.

[Fórmula 176]

$$k^{*}_{L+1,\mathrm{ran},(\tau,\iota,0)} := \sum_{j=1}^{2L} \alpha_{\mathrm{ran},(\tau,\iota)j,} k^{*}_{L,\mathrm{ran},j} + \phi_{\mathrm{ran},(\tau,\iota,0)} k^{*}_{L,\mathrm{ran},(\tau,\iota,0)} + \left\{ \begin{array}{ll} \sigma_{\mathrm{ran},(\tau,\iota,0)}\left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i,0)}\right) & \text{si } \rho_t = 0 \\ \sigma_{\mathrm{ran},(\tau,\iota,0)}\left([k^{*}_{L,\mathrm{del},(L+1,i,1)}]^{L} + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^{*}_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}\right) & \text{si } \rho_t = 1 \end{array} \right\} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^{*}_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^{*}_{\tau,n_\tau+u_\tau+i}$$

(S807: etapa de generación del primer elemento de delegación de nivel inferior)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de delegación de nivel inferior 434 genera un primer elemento de delegación de nivel inferior $k^{*}_{L+1,\mathrm{del},(\tau,\iota,0)}$ que es un elemento de la clave de delegación sk_{L+1} para cada número entero τ de τ = L+2, ..., d y cada número entero ι de ι = 1, ..., n_τ, con respecto a cada número entero τ, tal como se muestra en la fórmula 177.

[Fórmula 177]

$$k^{*}_{L+1,\mathrm{del},(\tau,\iota,0)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del},(\tau,\iota,0),j} k^{*}_{L,\mathrm{ran},j} + \phi_{\mathrm{del},(\tau,\iota,0)} k^{*}_{L,\mathrm{ran}(\tau,\iota,0)} + \psi_0 k^{*}_{L,\mathrm{del}(\tau,\iota,0)} + \left\{ \begin{array}{ll} \sigma_{\mathrm{del},(\tau,\iota,0)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i,0)} \right) & \text{si } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,0)} \left([k^{*}_{L,\mathrm{del},(L+1,i,1)}]^{L} + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^{*}_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}} \right) & \text{si } \rho_t = 1 \end{array} \right\} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^{*}_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^{*}_{\tau,n_\tau+u_\tau+i}$$

(S808: etapa de generación del segundo elemento de delegación de nivel inferior)

Utilizando el dispositivo de procesamiento, la unidad de generación de elementos de delegación de nivel inferior 434 genera un segundo elemento de delegación de nivel inferior $k^{*}_{L+1,\mathrm{del},(\tau,\iota,1)}$ que es un elemento de la clave de delegación sk_{L+1} para cada número entero τ de τ = L+2, ..., d y cada número entero ι de ι = 1, ..., n_τ con respecto a cada número entero τ, tal como se muestra en la fórmula 178.

[Fórmula 178]

$$k^{*}_{L+1,\mathrm{del},(\tau,\iota,1)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del}(\tau,\iota,1),j} k^{*}_{L,\mathrm{ran},j} + \psi_1 k^{*}_{L,\mathrm{del}(\tau,\iota,1)} + \left\{ \begin{array}{ll} \sigma_{\mathrm{del},(\tau,\iota,1)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i,0)} \right) & \text{si } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,1)} \left([k^{*}_{L,\mathrm{del},(L+1,i,1)}]^{L} + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^{*}_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}} \right) & \text{si } \rho_t = 1 \end{array} \right\} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,1),(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,1),(t,i)} b^{*}_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,1),(\tau,i)} b^{*}_{\tau,n_\tau+u_\tau+i}$$

(S809: etapa de distribución de clave)

Utilizando el dispositivo de comunicación y por medio de la red, por ejemplo, la unidad de distribución de claves 150 proporciona secretamente al dispositivo de desciframiento de nivel inferior 300 la clave de delegación sk_{L+1} que tiene elementos del elemento de desciframiento de nivel inferior $k^{*}_{L+1,\mathrm{dec}}$, el primer elemento de aleatorización de nivel inferior $k^{*}_{L+1,\mathrm{ran},j'}$ (j' = 1, ..., 2(L+1)), el segundo elemento de aleatorización de nivel inferior $k^{*}_{L+1,\mathrm{ran},(\tau,\iota,0)}$ (τ = L+2, ..., d; (τ,ι) = (τ,1), ..., (τ,η_τ)), el primer elemento de delegación de nivel inferior $k^{*}_{L+2,\mathrm{del},(\tau,\iota,0)}$ (τ = L+2, ..., d; (τ,ι) = (τ,1), ..., (τ,η_τ)) y el segundo elemento de delegación de nivel inferior $k^{*}_{L+2,\mathrm{del},(\tau,\iota,1)}$ (τ = L+2, ..., d; (τ,ι) = (τ,1), ..., (τ,n_τ)). Es obvio que la clave de delegación sk_{L+1} se puede proporcionar al dispositivo de desciframiento de nivel inferior 300 mediante otros métodos.

Resumiendo, en (S501) a (S507), el dispositivo de delegación de claves 400 ejecuta el algoritmo $\mathrm{Delegate}_L$ mostrado en las fórmulas 179 y 180, y genera la clave de delegación de sk_{L+1}. A continuación, en (S508), el dispositivo de delegación de claves 400 proporciona la clave de delegación generada sk_{L+1} al dispositivo de desciframiento de nivel inferior 300.

[Fórmula 179]

$$\mathsf{Delegate}_L(\mathsf{pk},\mathsf{sk}_L,(\vec{v}_{L+1},\rho_{L+1}) := ((v_{L+1,1},\ldots,v_{L+1,n_{L+1}}),\rho_{L+1})):$$

para $j=1,\ldots,2L;\ j'=1,\ldots,2(L+1);\ \tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau);$

$t=0,\ldots,L+1,\tau;\ (t,i)=(t,1),\ldots,(t,w_t);$

$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota,0),j},\ \sigma_{\mathsf{ran},(\tau,\iota,0)},\ \phi_{\mathsf{ran},(\tau,\iota,0)},$

$\alpha_{\mathsf{del},(\tau,\iota,0),j},\ \sigma_{\mathsf{del},(\tau,\iota,0)},\ \phi_{\mathsf{del},(\tau,\iota,0)},\ \alpha_{\mathsf{del},(\tau,\iota,1),j},\ \sigma_{\mathsf{del},(\tau,\iota,1)},\ \phi_{\mathsf{del},(\tau,\iota,1)},$

$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota,0),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota,0),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota,1),(t,i)},$

$\psi_0,\psi_1,\xleftarrow{\mathsf{U}}\mathbb{F}_q,$

$$k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + \sum_{j=1}^{2L}\alpha_{\mathsf{dec},j}k^*_{L,\mathsf{ran},j}$$

$$+\begin{cases}(\sigma_{\mathsf{dec}}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{si } \rho_t=0\\ (\sigma_{\mathsf{dec}}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad +\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{si } \rho_t=1\end{cases}$$

$$+\sum_{i=1}^{w_t}\eta_{\mathsf{dec},(0,i)}b^*_{0,1+u_0+1+i}+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathsf{dec},(t,i)}b^*_{t,n_t+u_t+i},$$

$$k^*_{L+1,\mathsf{ran},j'} := \sum_{j=1}^{2L}\alpha_{\mathsf{ran},j',j}k^*_{L,\mathsf{ran},j}$$

$$+\begin{cases}\sigma_{\mathsf{ran},j'}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{si } \rho_t=0\\ \sigma_{\mathsf{ran},j'}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad +\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{si } \rho_t=1\end{cases}$$

$$+\sum_{i=1}^{w_t}\eta_{\mathsf{ran},j',(0,i)}b^*_{0,1+u_0+1+i}$$

$$+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathsf{ran},j',(t,i)}b^*_{t,n_t+u_t+i},$$

$$k^*_{L+1,\mathsf{ran},(\tau,\iota,0)} := \sum_{j=1}^{2L}\alpha_{\mathsf{ran},(\tau,\iota)j},k^*_{L,\mathsf{ran},j}+\phi_{\mathsf{ran},(\tau,\iota,0)}k^*_{L,\mathsf{ran},(\tau,\iota,0)}$$

$$+\begin{cases}\sigma_{\mathsf{ran},(\tau,\iota,0)}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{si } \rho_t=0\\ \sigma_{\mathsf{ran},(\tau,\iota,0)}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad +\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{si } \rho_t=1\end{cases}$$

$$+\sum_{i=1}^{w_t}\eta_{\mathsf{del},(\tau,\iota,0),(0,i)}b^*_{0,1+u_0+1+i}$$

$$+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathsf{del},(\tau,\iota,0),(t,i)}b^*_{t,n_t+u_t+i}$$

$$+\sum_{i=1}^{w_\tau}\eta_{\mathsf{del},(\tau,\iota,0),(\tau,i)}b^*_{\tau,n_\tau+u_\tau+i},$$

[Fórmula 180]

$$k^*_{L+1,\mathrm{del},(\tau,\iota,0)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del},(\tau,\iota,0),j} k^*_{L,\mathrm{ran},j} + \phi_{\mathrm{del},(\tau,\iota,0)} k^*_{L,\mathrm{ran}(\tau,\iota,0)}$$
$$+ \psi_0 k^*_{L,\mathrm{del}(\tau,\iota,0)}$$
$$+ \begin{cases} \sigma_{\mathrm{del},(\tau,\iota,0)} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{si } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,0)} ([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{si } \rho_t = 1 \end{cases}$$
$$+ \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^*_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$
$$k^*_{L+1,\mathrm{del},(\tau,\iota,1)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del}(\tau,\iota,1),j} k^*_{L,\mathrm{ran},j} + \psi_1 k^*_{L,\mathrm{del}(\tau,\iota,1)}$$
$$+ \begin{cases} \sigma_{\mathrm{del},(\tau,\iota,1)} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{si } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,1)} ([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{si } \rho_t = 1 \end{cases}$$
$$+ \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,1),(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,1),(t,i)} b^*_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,1),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$
$$\mathrm{sk}_{L+1} := (((\vec{v}_1,\rho_1),\ldots,(\vec{v}_{L+1},\rho_{L+1}));$$
$$k^*_{L+1,\mathrm{dec}}, \{k^*_{L+1,\mathrm{ran},j'}\}_{j'=1,\ldots,2(L+1)},$$
$$\{k^*_{L+1,\mathrm{ran},(\tau,\iota,0)}, k^*_{L+1,\mathrm{del},(\tau,\iota,0)}, k^*_{L+1,\mathrm{del},(\tau,\iota,1)}\}_{\tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}),$$

devuelve sk_{L+1}.

Cuando el dispositivo de desciframiento de nivel inferior 300 ejecuta el algoritmo Dec utilizando la clave de delegación de sk_{L+1}, la clave de sesión K se computa mediante la computación de la fórmula 170 si el producto escalar de ($\vec{v}_1$, ..., $\vec{v}_{L+1}$) y ($\vec{x}_1$, ..., $\vec{x}_{L+1}$) es 0 en (S403) de la figura 15.

Tal como se ha descrito anteriormente, el sistema de procesamiento criptográfico 10 acorde con la segunda realización realiza el esquema HPE para productos escalares que permite el desciframiento si el producto escalar de la información de atributo y la información de predicado es 0 para algunas partes, y si el producto escalar de la información de atributo y la información de predicado no es 0 para las partes restantes. Por lo tanto, es posible ajustar una combinación de condiciones positivas y negativas, y similar, por ejemplo.

En la descripción anterior, las dimensiones u_t, w_t y z_t (t = 0, ..., d) se proporcionan para una seguridad reforzada. Por lo tanto, al coste de una seguridad reducida, las dimensiones u_t, w_t y z_t (t = 0, ..., d) se pueden omitir ajustando u_t, w_t y z_t (t = 0, ..., d) respectivamente a 0.

En la descripción anterior, $1+u_0+1+w_0+z_0$ se ajusta en N_0 y $n_t+u_t+w_t+z_t$ se ajusta en N_t. Sin embargo, $1+u_0+1+w_0+z_0$ puede ser sustituido por 1+1+1+1+1, de tal modo que 5 se ajusta en N_0, y $n_t+u_t+w_t+z_t$ puede ser sustituido por $n_t+n_t+n_t+1$, de tal modo que $3n_t+1$ se ajusta en N_t.

En este caso, el algoritmo KeyGen mostrado en las fórmulas 168 y 169 se reescribe tal como se muestran las fórmulas 181 y 182.

[Fórmula 181]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,\rho_1),\ldots,(\vec{v}_L,\rho_L)) := (((v_{1,1},\ldots,v_{1,n_1}) \in \mathbb{F}_q^{n_1}, \rho_1 \in \{0,1\}),\ldots,$$

$$((v_{L,1},\ldots,v_{L,n_L}) \in \mathbb{F}_q^{n_L}, \rho_L \in \{0,1\})):$$

para $j = 1,\ldots,2L;\ \tau = L+1,\ldots,d;\ (\tau,\iota) = (\tau,1),\ldots,(\tau,n_\tau);$

$$\psi, s_{\mathsf{dec},t}, s_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q \quad (t = 1,\ldots,L);$$

$$\theta_{\mathsf{dec},t}, \theta_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\vec{\eta}_{\mathsf{dec},t},\ \vec{\eta}_{\mathsf{ran},j,t},\ \vec{\eta}_{\mathsf{ran},0,t},\ \vec{\eta}_{\mathsf{del},0,t}\ \vec{\eta}_{\mathsf{del},1,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t} \quad (t = 0,\ldots,L);$$

$$s_{\mathsf{ran},0,t}, s_{\mathsf{del},0,t}, s_{\mathsf{del},1,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\theta_{\mathsf{ran},0,t}, \theta_{\mathsf{del},0,t}, \theta_{\mathsf{del},1,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\vec{\eta}_{\mathsf{ran},0,(\tau,\iota)},\ \vec{\eta}_{\mathsf{del},0,(\tau,\iota)},\ \vec{\eta}_{\mathsf{del},1,(\tau,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}\ ,\ (t = 0,\ldots,L+1);$$

$$s_{\mathsf{dec},0} := \sum_{t=1}^{L} s_{\mathsf{dec},t},\ s_{\mathsf{ran},j,0} := \sum_{t=1}^{L} s_{\mathsf{ran},j,t},\ s_{\mathsf{ran},0,0} := \sum_{t=1}^{L} s_{\mathsf{ran},0,t},$$

$$s_{\mathsf{del},0,0} := \sum_{t=1}^{L+1} s_{\mathsf{del},0,t},\ s_{\mathsf{del},1,0} := \sum_{t=1}^{L+1} s_{\mathsf{del},1,t},$$

$$k^*_{L,\mathsf{dec}} := (\ (-s_{\mathsf{dec},0}, 0, 1, \eta_{\mathsf{dec},0}, 0)_{\mathbb{B}^*_0},$$

$$\left\{ \begin{array}{ll} (s_{\mathsf{dec},t}\ \vec{e}_{t,1} + \theta_{\mathsf{dec},t}, \vec{v}_t, 0^{n_t},\ \vec{\eta}_{\mathsf{dec},t}, 0)_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathsf{dec},t}\ \vec{v}_t, 0^{n_t},\ \vec{\eta}_{\mathsf{dec},t}, 0)_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\} : t = 1,\ldots,L),$$

$$k^*_{L,\mathsf{ran},j} := (\ (-s_{\mathsf{ran},j,0}, 0, 0, \eta_{\mathsf{ran},j,0}, 0)_{\mathbb{B}^*_0},$$

$$\left\{ \begin{array}{ll} (s_{\mathsf{ran},j,t}\ \vec{e}_{t,1} + \theta_{\mathsf{ran},j,t}\vec{v}_t, 0^{n_t},\ \vec{\eta}_{\mathsf{ran},j,t}, 0)_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathsf{ran},j,t}\ \vec{v}_t, 0^{n_t},\ \vec{\eta}_{\mathsf{ran},j,t}, 0)_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\}$$

$$: t = 1,\ldots,L),$$

[Fórmula 182]

$$k^*_{L,\mathsf{ran},(\tau,t,0)} := (\ (-s_{\mathsf{ran},0,0},0,0,\eta_{\mathsf{ran},0,0},0)_{\mathbb{B}^*_0},$$
$$\left\{\begin{array}{ll}(s_{\mathsf{ran},0,t}\ \vec{e}_{t,1}+\theta_{\mathsf{ran},0,t}\vec{v}_t,0^{n_t},\ \vec{\eta}_{\mathsf{ran},0,t},0)_{\mathbb{B}^*_t}, & \text{si } \rho_t=0\\ (s_{\mathsf{ran},0,t}\ \vec{v}_t,0^{n_t},\ \vec{\eta}_{\mathsf{ran},0,t},0)_{\mathbb{B}^*_t}, & \text{si } \rho_t=1\end{array}\right\}$$
$$:t=1,\ldots,L),$$
$$(s_{\mathsf{ran},0,L+1}\ \vec{e}_{\tau,1},0^{n_\tau},\ \vec{\eta}_{\mathsf{ran},0,(\tau,t)},0)_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,t,0)} := (\ (-s_{\mathsf{del},0,0},0,0,\eta_{\mathsf{del},0,0},0)_{\mathbb{B}^*_0},$$
$$\left\{\begin{array}{ll}(s_{\mathsf{del},0,t}\ \vec{e}_{t,1}+\theta_{\mathsf{del},0,t}\vec{v}_t,0^{n_t},\ \vec{\eta}_{\mathsf{del},0,t},0)_{\mathbb{B}^*_t}, & \text{si } \rho_t=0\\ (s_{\mathsf{del},0,t}\ \vec{v}_t,0^{n_t},\ \vec{\eta}_{\mathsf{del},0,t},0)_{\mathbb{B}^*_t}, & \text{si } \rho_t=1\end{array}\right\}$$
$$:t=1,\ldots,L),$$
$$(s_{\mathsf{del},0,L+1}\ \vec{e}_{\tau,1},+\psi\vec{e}_{\tau,t},0^{n_\tau},\ \vec{\eta}_{\mathsf{del},0,(\tau,t)},0)_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,t,1)} := (\ (-s_{\mathsf{del},1,0},0,0,\eta_{\mathsf{del},1,0},0)_{\mathbb{B}^*_0},$$
$$\left\{\begin{array}{ll}(s_{\mathsf{del},1,t}\ \vec{e}_{t,1}+\theta_{\mathsf{del},1,t}\vec{v}_t,0^{n_t},\ \vec{\eta}_{\mathsf{del},1,t},0)_{\mathbb{B}^*_t}, & \text{si } \rho_t=0\\ (s_{\mathsf{del},1,t}\ \vec{v}_t,0^{n_t},\ \vec{\eta}_{\mathsf{del},1,t},0)_{\mathbb{B}^*_t}, & \text{si } \rho_t=1\end{array}\right\}$$
$$:t=1,\ldots,L),$$
$$(s_{\mathsf{del},1,L+1}\ \vec{e}_{\tau,t},0^{n_\tau},\ \vec{\eta}_{\mathsf{del},1,(\tau,t)},0)_{\mathbb{B}^*_\tau}),$$

$$\mathsf{sk}_L := (((\vec{v}_1,\rho_1),\ldots,(\vec{v}_L,\rho_L));$$
$$k^*_{L,\mathsf{dec}},\{k^*_{L,\mathsf{ran},j}\}_{j=1,\ldots,2L},\{k^*_{L,\mathsf{ran},(\tau,t,0)},k^*_{L,\mathsf{del},(\tau,t,0)},k^*_{L,\mathsf{del},(\tau,t,1)}\}$$
$$\tau=L+1,\ldots,d;(\tau,t)=(\tau,1),\ldots,(\tau,n_\tau)),$$

devuelve sk_L.

El algoritmo $\mathsf{Delegate}_L$ mostrado en las fórmulas 179 y 180 se reescribe tal como se muestra en las fórmulas 183 y 184.

[Fórmula 183]

$$\mathsf{Delegate}_L(\mathsf{pk},\mathsf{sk}_L,(\vec{v}_{L+1},\rho_{L+1}) := ((v_{L+1,1},\ldots,v_{L+1,n_{L+1}}),\rho_{L+1})):$$

para $j=1,\ldots,2L;\ j'=1,\ldots,2(L+1);\ \tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau);$

$t=0,\ldots,L+1,\tau;\ (t,i)=(t,1),\ldots,(t,n_t);$

$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota,0),j},\ \sigma_{\mathsf{ran},(\tau,\iota,0)},\ \phi_{\mathsf{ran},(\tau,\iota,0)},$

$\alpha_{\mathsf{del},(\tau,\iota,0),j},\ \sigma_{\mathsf{del},(\tau,\iota,0)},\ \phi_{\mathsf{del},(\tau,\iota,0)},\ \alpha_{\mathsf{del},(\tau,\iota,1),j},\ \sigma_{\mathsf{del},(\tau,\iota,1)},\ \phi_{\mathsf{del},(\tau,\iota,1)},$

$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota,0),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota,0),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota,1),(t,i)},$

$\psi_0,\psi_1,\xleftarrow{\mathsf{U}} \mathbb{F}_q,$

$$k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + \sum_{j=1}^{2L} \alpha_{\mathsf{dec},j} k^*_{L,\mathsf{ran},j}$$

$$+ \left\{ \begin{array}{ll} (\sigma_{\mathsf{dec}} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{si } \rho_t = 0 \\ (\sigma_{\mathsf{dec}} ([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{si } \rho_t = 1 \end{array} \right\}$$

$$+ \eta_{\mathsf{dec},(0,1)} b^*_{0,4} + \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathsf{dec},(t,i)} b^*_{t,2n_t+i},$$

$$k^*_{L+1,\mathsf{ran},j'} := \sum_{j=1}^{2L} \alpha_{\mathsf{ran},j',j} k^*_{L,\mathsf{ran},j}$$

$$+ \left\{ \begin{array}{ll} \sigma_{\mathsf{ran},j'} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{si } \rho_t = 0 \\ \sigma_{\mathsf{ran},j'} ([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{si } \rho_t = 1 \end{array} \right\}$$

$$+ \eta_{\mathsf{ran},j',(0,1)} b^*_{0,4} + \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathsf{ran},j',(t,i)} b^*_{t,2n_t+i},$$

$$k^*_{L+1,\mathsf{ran},(\tau,\iota,0)} := \sum_{j=1}^{2L} \alpha_{\mathsf{ran},(\tau,\iota)j,} k^*_{L,\mathsf{ran},j} + \phi_{\mathsf{ran},(\tau,\iota,0)} k^*_{L,\mathsf{ran},(\tau,\iota,0)}$$

$$+ \left\{ \begin{array}{ll} \sigma_{\mathsf{ran},(\tau,\iota,0)} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{si } \rho_t = 0 \\ \sigma_{\mathsf{ran},(\tau,\iota,0)} ([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{si } \rho_t = 1 \end{array} \right\}$$

$$+ \eta_{\mathsf{del},(\tau,\iota,0),(0,1)} b^*_{0,4} + \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathsf{del},(\tau,\iota,0),(t,i)} b^*_{t,2n_t+i}$$

$$+ \sum_{i=1}^{n_\tau} \eta_{\mathsf{del},(\tau,\iota,0),(\tau,i)} b^*_{\tau,2n_\tau+i},$$

[Fórmula 184]

$$k^*_{L+1,\mathrm{del},(\tau,\iota,0)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del},(\tau,\iota,0),j} k^*_{L,\mathrm{ran},j} + \phi_{\mathrm{del},(\tau,\iota,0)} k^*_{L,\mathrm{ran}(\tau,\iota,0)}$$
$$+ \psi_0 k^*_{L,\mathrm{del}(\tau,\iota,0)}$$
$$+ \begin{cases} \sigma_{\mathrm{del},(\tau,\iota,0)} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{si } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,0)} ([k^*_{L,\mathrm{del},(L+1,i,1)}]^L \\ \qquad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_L) & \text{si } \rho_t = 1 \end{cases}$$
$$+ \eta_{\mathrm{del},(\tau,\iota,0),(0,1)} b^*_{0,4} + \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^*_{t,2n_t+i}$$
$$+ \sum_{i=1}^{n_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^*_{\tau,2n_\tau+i},$$
$$k^*_{L+1,\mathrm{del},(\tau,\iota,1)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del}(\tau,\iota,1),j} k^*_{L,\mathrm{ran},j} + \psi_1 k^*_{L,\mathrm{del}(\tau,\iota,1)}$$
$$+ \begin{cases} \sigma_{\mathrm{del},(\tau,\iota,1)} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{si } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,1)} ([k^*_{L,\mathrm{del},(L+1,i,1)}]^L \\ \qquad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_L) & \text{si } \rho_t = 1 \end{cases}$$
$$+ \eta_{\mathrm{del},(\tau,\iota,1),(0,1)} b^*_{0,4} + \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathrm{del},(\tau,\iota,1),(t,i)} b^*_{t,2n_t+i}$$
$$+ \sum_{i=1}^{n_\tau} \eta_{\mathrm{del},(\tau,\iota,1),(\tau,i)} b^*_{\tau,2n_\tau+i},$$
$$\mathrm{sk}_{L+1} := (((\vec{v}_1,\rho_1),\ldots,(\vec{v}_{L+1},\rho_{L+1}));$$
$$k^*_{L+1,\mathrm{dec}}, \{k^*_{L+1,\mathrm{ran},j'}\}_{j'=1,\ldots,2(L+1)},$$
$$\{k^*_{L+1,\mathrm{ran},(\tau,\iota,0)}, k^*_{L+1,\mathrm{del},(\tau,\iota,0)}, k^*_{L+1,\mathrm{del},(\tau,\iota,1)}\}_{\tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}),$$

devuelve sk_{L+1}.

El algoritmo Dec mostrado en la fórmula 172 permanece igual.

El algoritmo Setup tiene que ser ejecutado una vez cuando se configura el sistema de procesamiento criptográfico 10, y no se tiene que ejecutar cada vez que se genera una clave de desciframiento. En la descripción anterior, el algoritmo Setup y el algoritmo KeyGen son ejecutados por el dispositivo de generación de claves 100. Sin embargo, el algoritmo Setup y el algoritmo KeyGen pueden ser ejecutados por dispositivos diferentes.

Tercera realización

En las realizaciones anteriores, se han descrito los métodos para implementar el proceso criptográfico en espacios vectoriales duales. En esta realización, se describirá un método para implementar el proceso criptográfico en módulos duales.

Es decir, en las realizaciones anteriores, los procesos criptográficos se implementan en grupos cíclicos de orden primo q. Sin embargo, cuando un anillo R se expresa utilizando un número compuesto M, tal como se muestra en la fórmula 185, los procesos criptográficos descritos en las realizaciones anteriores se pueden adaptar a un módulo

[Fórmula 185]

que tenga el anillo R como coeficiente. $\mathbb{R} := \mathbb{Z}/M\mathbb{Z}$

donde

$\mathbb{Z}$: número entero,

M: número compuesto.

Cuando el esquema HPE descrito en la primera realización se implementa en el módulo que tiene R como coeficiente, el esquema HPE se representa tal como se muestra en las fórmulas 186 a 193.

[Fórmula 186]

$$\mathsf{Setup}(1^{\lambda},\ \vec{n} := (d; n_1,...,n_d, u_0,...,u_d, w_0,...,w_d, z_0,...,z_d)) :$$

$$(\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,...,d}) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}(1^{\lambda}, \vec{n}),$$

$$\hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,1+u_0+1}, b_{0,1+u_0+1+w_0+1}, ..., b_{0,1+u_0+1+w_0+z_0}),$$

$$\hat{\mathbb{B}}_t := (b_{t,1}, .., b_{t,n_t}, b_{t,n_t+u_t+w_t+1}, ..., b_{t,n_t+u_t+w_t+z_t}) \text{ para } t = 1,..,d,$$

$$\hat{\mathbb{B}}_0^* := (b_{0,1}^*, b_{0,1+u_0+1}^*),$$

$$\hat{\mathbb{B}}_t^* := (b_{t,1}^*, .., b_{t,n_t}^*) \text{ para } t = 1,..,d,$$

$$\mathsf{pk} := (1^{\lambda}, \mathsf{param}_{\vec{n}}, \{\hat{\mathbb{B}}_t\}_{t=0,...,d},$$

$$b_{0,1+u_0+1+1}^*, ..., b_{0,1+u_0+1+w_0}^*, \{b_{t,n_t+u_t+1}^*, ..., b_{t,n_t+u_t+w_t}^*\}_{t=1,...,d}),$$

$$\mathsf{sk} := \{\hat{\mathbb{B}}_t^*\}_{t=0,...,d},$$

devolver pk, sk.

[Fórmula 187]

$$\mathcal{G}_{\mathsf{ob}}(1^{\lambda}, \vec{n} := (d; \vec{n} := (d; n_1,...,n_d, u_0,...,u_d, w_0,..., w_d, z_0,..., z_d)$$

$$N_0 := 1 + u_0 + 1 + w_0 + z_0,\ N_t := n_t + u_t + w_t + z_t \text{ para } t = 1,..,d,$$

$$\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, g, e) \xleftarrow{R} \mathcal{G}_{\mathsf{bpg}}(1^{\lambda}),$$

$$\psi \xleftarrow{U} \mathbb{R}^{\times},$$

Para $t = 0,\ldots,d$,

$$\mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^{\lambda}, N_t, \mathsf{param}_{\mathbb{G}}),$$

$$X_t := (\chi_{t,i,j})_{i,j} \xleftarrow{U} GL(N_t, \mathbb{R}),\quad (\nu_{t,i,j})_{i,j} := \psi \cdot (X_t^{\mathrm{T}})^{-1},$$

$$b_{t,i} := (\chi_{t,i,1}, \cdots, \chi_{t,i,N_t})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \chi_{t,i,j} a_{t,j},\ \mathbb{B}_t := (b_{t,1}, \ldots, b_{t,N_t}),$$

$$b_{t,i}^* := (\nu_{t,i,1}, \cdots, \nu_{t,i,N_t})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \nu_{t,i,j} a_{t,j},\ \mathbb{B}_t^* := (b_{t,1}^*, \ldots, b_{t,N_t}^*),$$

$$g_T := e(g,g)^{\psi},\quad \mathsf{param}_n^{-} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,...,d}, g_T)$$

devolver $(\mathsf{param}_n^{-}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,...,d})$.

[Fórmula 188]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,...,\vec{v}_L) := (v_{1,1},...,v_{1,n_1}),...,\ (v_{L,1},...,v_{L,n_L})):$$

para $j=1,...,2L;\ \tau=L+1,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau);$

$$\psi, s_{\mathsf{dec},t}, s_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{R}\ (t=1,...,L);$$

$$\theta_{\mathsf{dec},t}, \theta_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{R},\ \vec{\eta}_{\mathsf{dec},t},\ \vec{\eta}_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{R}^{w_t}\ (t=0,...,L);$$

$$s_{\mathsf{ran},(\tau,\iota),t}, s_{\mathsf{del},(\tau,\iota),t} \xleftarrow{\mathsf{U}} \mathbb{R}\ (t=1,...,L+1);$$

$$\theta_{\mathsf{ran},(\tau,\iota),t}, \theta_{\mathsf{del},(\tau,\iota),t} \xleftarrow{\mathsf{U}} \mathbb{R},\ \vec{\eta}_{\mathsf{ran},(\tau,\iota),t},\ \vec{\eta}_{\mathsf{del},(\tau,\iota),t} \xleftarrow{\mathsf{U}} \mathbb{R}^{w_t},$$
$$(t=0,...,L+1);$$

$$s_{\mathsf{dec},0} := \sum_{t=1}^{L} s_{\mathsf{dec},t},\ s_{\mathsf{ran},j,0} := \sum_{t=1}^{L} s_{\mathsf{ran},j,t},$$

$$s_{\mathsf{ran},(\tau,\iota),0} := \sum_{t=1}^{L+1} s_{\mathsf{ran},(\tau,\iota),t},\ s_{\mathsf{del},(\tau,\iota),0} := \sum_{t=1}^{L+1} s_{\mathsf{del},(\tau,\iota),t},$$

[Fórmula 189]

$$k^*_{L,\mathsf{dec}} := (\ (-s_{\mathsf{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathsf{dec},0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{dec},t}\ \vec{e}_{t,1} + \theta_{\mathsf{dec},t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{dec},t}, 0^{z_t})_{\mathbb{B}^*_t} : t = 1,\ldots,L),$$

$$k^*_{L,\mathsf{ran},j} := (\ (-s_{\mathsf{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},j,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{ran},j,t}\ \vec{e}_{t,1} + \theta_{\mathsf{ran},j,t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L),$$

$$k^*_{L,\mathsf{ran},(\tau,\iota)} := (\ (-s_{\mathsf{ran},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{ran},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathsf{ran},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{ran},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L$$
$$(s_{\mathsf{ran},(\tau,\iota),L+1}\ \vec{e}_{\tau,1},\ 0^{u_\tau}, \vec{\eta}_{\mathsf{ran},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,\iota)} := (\ (-s_{\mathsf{del},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{del},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{del},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathsf{del},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{del},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L$$
$$(s_{\mathsf{del},(\tau,\iota),L+1}\ \vec{e}_{\tau,1} + \psi\vec{e}_{\tau,\iota}, 0^{u_\tau}, \vec{\eta}_{\mathsf{del},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$\mathsf{sk}_L := (k^*_{L,\mathsf{dec}}, \{k^*_{L,\mathsf{ran},j}\}_{j=1,\ldots,2L},$$
$$\{k^*_{L,\mathsf{ran},(\tau,\iota)}\}_{\tau=L+1,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)},$$
$$\{k^*_{L,\mathsf{del},(\tau,\iota)}\}_{\tau=L+1,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}),$$

devolver sk_L.

[Fórmula 190]

$$\mathsf{Enc}(\mathsf{pk}, m \in \mathbb{G}_T, (\vec{x}_1,\ldots,\vec{x}_L) := ((x_{1,1},\ldots,x_{1,n_1}),\ldots,(x_{L,1},\ldots,x_{L,n_L})):$$
$$(\vec{x}_{L+1},\ldots,\vec{x}_d) \xleftarrow{\mathsf{U}} \mathbb{R}^{n_{L+1}} \times \cdots \times \mathbb{R}^{n_d};$$
$$\omega, \zeta \xleftarrow{\mathsf{U}} \mathbb{R},\ \vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{R}^{z_t}\ (t = 0,\ldots,d),$$
$$c_1 := (\ (\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t} : t = 1,\ldots,d),$$
$$c_2 := g_T^{\zeta} m,$$
$$\mathsf{ct} := (c_1, c_2),$$

devolver ct.

[Fórmula 191]

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

devolver m'.

[Fórmula 192]

$$\mathsf{Delegate}_L(\mathsf{pk}, \mathsf{sk}_L, \vec{v}_{L+1} := (v_{L+1,1},\ldots,v_{L+1,n_{L+1}})):$$

para $j = 1,\ldots,2L;\ j' = 1,\ldots,2(L+1);\ \tau = L+2,\ldots,d;\ (\tau,\iota) = (\tau,1),\ldots,(\tau,n_\tau);$

$t = 0,\ldots,L+1,\tau;\ (t,i) = (t,1),\ldots,(t,w_t);$

$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota),j},\ \sigma_{\mathsf{ran},(\tau,\iota)},$

$\phi_{\mathsf{ran},(\tau,\iota)},\ \alpha_{\mathsf{del},(\tau,\iota),j},\ \sigma_{\mathsf{del},(\tau,\iota)},\ \phi_{\mathsf{del},(\tau,\iota)},\ \psi',$

$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota),(t,i)} \xleftarrow{\mathsf{U}} \mathbb{R},$

[Fórmula 193]

$$k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + \sum_{j=1}^{2L} \alpha_{\mathsf{dec},j}\, k^*_{L,\mathsf{ran},j}$$
$$+ \sigma_{\mathsf{dec}} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)}\Big) + \sum_{i=1}^{w_t} \eta_{\mathsf{dec},(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{dec},(t,i)} b^*_{t,n_t+u_t+i},$$
$$k^*_{L+1,\mathsf{ran},j'} := \sum_{j=1}^{2L} \alpha_{\mathsf{ran},j',j}\, k^*_{L,\mathsf{ran},j}$$
$$+ \sigma_{\mathsf{ran},j'} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)}\Big) + \sum_{i=1}^{w_t} \eta_{\mathsf{ran},j',(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{ran},j',(t,i)} b^*_{t,n_t+u_t+i},$$
$$k^*_{L+1,\mathsf{ran},(\tau,\iota)} := \sum_{j=1}^{2L} \alpha_{\mathsf{ran},(\tau,\iota),j}\, k^*_{L,\mathsf{ran},j}$$
$$+ \sigma_{\mathsf{ran},(\tau,\iota)} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)}\Big)$$
$$+ \phi_{\mathsf{ran},(\tau,\iota)} k^*_{L,\mathsf{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathsf{ran},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{ran},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathsf{ran},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$
$$k^*_{L+1,\mathsf{del},(\tau,\iota)} := \sum_{j=1}^{2L} \alpha_{\mathsf{del},(\tau,\iota),j}\, k^*_{L,\mathsf{ran},j}$$
$$+ \sigma_{\mathsf{del},(\tau,\iota)} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)}\Big) + \psi' k^*_{L,\mathsf{del},(\tau,\iota)}$$
$$+ \phi_{\mathsf{del},(\tau,\iota)} k^*_{L,\mathsf{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathsf{del},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{del},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathsf{del},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$
$$\mathsf{sk}_{L+1} := \big(k^*_{L+1,\mathsf{dec}}, \{k^*_{L+1,\mathsf{ran},j'}\}_{j'=1,\ldots,2(L+1)},$$
$$\{k^*_{L+1,\mathsf{ran},(\tau,\iota)}, k^*_{L+1,\mathsf{del},(\tau,\iota)}\}_{\tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}\big),$$

devolver sk_{L+1}

Cuando el esquema HPE descrito en la segunda realización se implementa en el módulo que tiene el anillo R como coeficiente, el esquema HPE se expresa tal como se muestra en las fórmulas 194 a 199. El algoritmo Setup y el algoritmo G_{ob} son tal como se muestra en las fórmulas 186 y 187, respectivamente.

[Fórmula 194]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,\rho_1),...,(\vec{v}_L,\rho_L)) := (((v_{1,1},...,v_{1,n_1}) \in \mathbb{R}^{n_1}, \rho_1 \in \{0,1\}),...,$$

$$((v_{L,1},...,v_{L,n_L}) \in \mathbb{R}^{n_L}, \rho_L \in \{0,1\})):$$

para $j = 1,...,2L;\ \tau = L+1,...,d;\ (\tau,\iota) = (\tau,1),...,(\tau,n_\tau);$

$$\psi, s_{\mathsf{dec},t}, s_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{R}\ (t = 1,...,L);$$

$$\theta_{\mathsf{dec},t}, \theta_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{R},$$

$$\vec{\eta}_{\mathsf{dec},t},\ \vec{\eta}_{\mathsf{ran},j,t},\ \vec{\eta}_{\mathsf{ran},0,t},\ \vec{\eta}_{\mathsf{del},0,t}\ \vec{\eta}_{\mathsf{del},1,t} \xleftarrow{\mathsf{U}} \mathbb{R}^{w_t}\ \ (t = 0,...,L);$$

$$s_{\mathsf{ran},0,t}, s_{\mathsf{del},0,t}, s_{\mathsf{del},1,t} \xleftarrow{\mathsf{U}} \mathbb{R},$$

$$\theta_{\mathsf{ran},0,t}, \theta_{\mathsf{del},0,t}, \theta_{\mathsf{del},1,t} \xleftarrow{\mathsf{U}} \mathbb{R},$$

$$\vec{\eta}_{\mathsf{ran},0,(\tau,\iota)},\ \vec{\eta}_{\mathsf{del},0,(\tau,\iota)},\ \vec{\eta}_{\mathsf{del},1,(\tau,\iota)} \xleftarrow{\mathsf{U}} \mathbb{R}^{w_t}\ ,\ (t = 0,...,L+1);$$

$$s_{\mathsf{dec},0} := \sum_{t=1}^{L} s_{\mathsf{dec},t},\ s_{\mathsf{ran},j,0} := \sum_{t=1}^{L} s_{\mathsf{ran},j,t},\ s_{\mathsf{ran},0,0} := \sum_{t=1}^{L} s_{\mathsf{ran},0,t},$$

$$s_{\mathsf{del},0,0} := \sum_{t=1}^{L+1} s_{\mathsf{del},0,t},\ s_{\mathsf{del},1,0} := \sum_{t=1}^{L+1} s_{\mathsf{del},1,t},$$

$$k^*_{L,\mathsf{dec}} := (\ (-s_{\mathsf{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathsf{dec},0}, 0^{z_0})_{\mathbb{B}^*_0},$$

$$\left\{ \begin{array}{ll} (s_{\mathsf{dec},t}\vec{e}_{t,1} + \theta_{\mathsf{dec},t}, \vec{v}_t, 0^{u_t},\ \vec{\eta}_{\mathsf{dec},t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathsf{dec},t}\vec{v}_t, 0^{u_t},\ \vec{\eta}_{\mathsf{dec},t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\}$$

$$: t = 1,...,L),$$

$$k^*_{L,\mathsf{ran},j} := (\ (-s_{\mathsf{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},j,0}, 0^{z_0})_{\mathbb{B}^*_0},$$

$$\left\{ \begin{array}{ll} (s_{\mathsf{ran},j,t}\vec{e}_{t,1} + \theta_{\mathsf{ran},j,t}\vec{v}_t, 0^{u_t},\ \vec{\eta}_{\mathsf{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathsf{ran},j,t}\vec{v}_t, 0^{u_t},\ \vec{\eta}_{\mathsf{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\}$$

$$: t = 1,...,L),$$

[Fórmula 195]

$$k^*_{L,\mathsf{ran},(\tau,t,0)} := ((-s_{\mathsf{ran},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},0,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathsf{ran},0,t}\vec{e}_{t,1} + \theta_{\mathsf{ran},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{ran},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathsf{ran},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{ran},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\}$$
$$: t = 1,\ldots,L),$$
$$(s_{\mathsf{ran},0,L+1}\vec{e}_{\tau,1}, 0^{u_\tau}, \vec{\eta}_{\mathsf{ran},0,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,t,0)} := ((-s_{\mathsf{del},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{del},0,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathsf{del},0,t}\vec{e}_{t,1} + \theta_{\mathsf{del},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathsf{del},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\}$$
$$: t = 1,\ldots,L),$$
$$(s_{\mathsf{del},0,L+1}\vec{e}_{\tau,1}, +\psi\vec{e}_{\tau,t}, 0^{u_\tau}, \vec{\eta}_{\mathsf{del},0,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,t,1)} := ((-s_{\mathsf{del},1,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{del},1,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathsf{del},1,t}\vec{e}_{t,1} + \theta_{\mathsf{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},1,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 0 \\ (s_{\mathsf{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},1,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{si } \rho_t = 1 \end{array} \right\}$$
$$: t = 1,\ldots,L),$$
$$(s_{\mathsf{del},1,L+1}\vec{e}_{\tau,t}, 0^{u_\tau}, \vec{\eta}_{\mathsf{del},1,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$\mathsf{sk}_L := (((\vec{v}_1,\rho_1),\ldots,(\vec{v}_L,\rho_L));$$
$$k^*_{L,\mathsf{dec}}, \{k^*_{L,\mathsf{ran},j}\}_{j=1,\ldots,2L}, \{k^*_{L,\mathsf{ran},(\tau,t,0)}, k^*_{L,\mathsf{del},(\tau,t,0)}, k^*_{L,\mathsf{del},(\tau,t,1)}\}$$
$$\tau=L+1,\ldots,d;(\tau,t)=(\tau,1),\ldots,(\tau,n_\tau)),$$

devolver sk_L.

[Fórmula 196]

$$\mathsf{Enc}(\mathsf{pk}, m \in \mathbb{G}_T, (\vec{x}_1,\ldots,\vec{x}_L) := ((x_{1,1},\ldots,x_{1,n_1}),\ldots,(x_{L,1},\ldots,x_{L,n_L})):$$

$$(\vec{x}_{L+1},\ldots,\vec{x}_d) \xleftarrow{\mathsf{U}} \mathbb{R}^{n_{L+1}} \times \cdots \times \mathbb{R}^{n_d};$$

$$\omega,\zeta \xleftarrow{\mathsf{U}} \mathbb{R},\ \vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{R}^{z_t}\ (t = 0,\ldots,d),$$

$$c_1 := ((\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t} : t = 1,\ldots,d),$$

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

$$\mathsf{ct} := ((\vec{x}_1,\ldots,\vec{x}_L); c_1, c_2),$$

devolver ct.

[Fórmula 197]

$$\mathsf{Dec}(\mathsf{pk},\mathsf{sk}_L,\mathsf{ct}):$$

$$K := e(c_{1,0},k^*_{L,\mathsf{dec},0})\cdot \prod_{1\le t\le d\wedge\rho_t=0} e(c_{1,t},k^*_{L,\mathsf{dec},t})\cdot \prod_{1\le t\le d\wedge\rho_t=1} e(c_{1,t},k^*_{L,\mathsf{dec},t})^{1/(\vec{v}_t\cdot\vec{x}_t)},$$

donde $(k^*_{L,\mathsf{dec},0}\in\langle\mathbb{B}^*_0\rangle,\ldots,k^*_{L,\mathsf{dec},d}\in\langle\mathbb{B}^*_d\rangle) := k^*_{L,\mathsf{dec}}$,

$(c_{1,0}\in\langle\mathbb{B}^*_0\rangle,\ldots,c_{1,d}\in\langle\mathbb{B}^*_d\rangle := c_1$,

$m' := c_2 / K$,

devolver m'.

[Fórmula 198]

$$\mathsf{Delegate}_L(\mathsf{pk},\mathsf{sk}_L,(\vec{v}_{L+1},\rho_{L+1}) := ((v_{L+1,1},\ldots,v_{L+1,n_{L+1}}),\rho_{L+1})):$$

para $j=1,\ldots,2L;\ j'=1,\ldots,2(L+1);\ \tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau);$

$t=0,\ldots,L+1,\tau;\ (t,i)=(t,1),\ldots,(t,w_t);$

$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota,0),j},\ \sigma_{\mathsf{ran},(\tau,\iota,0)},\ \phi_{\mathsf{ran},(\tau,\iota,0)},$

$\alpha_{\mathsf{del},(\tau,\iota,0),j},\ \sigma_{\mathsf{del},(\tau,\iota,0)},\ \phi_{\mathsf{del},(\tau,\iota,0)},\ \alpha_{\mathsf{del},(\tau,\iota,1),j},\ \sigma_{\mathsf{del},(\tau,\iota,1)},\ \phi_{\mathsf{del},(\tau,\iota,1)},$

$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota,0),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota,0),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota,1),(t,i)},$

$\psi_0,\psi_1,\xleftarrow{\mathsf{U}}\mathbb{R},$

$$k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + \sum_{j=1}^{2L}\alpha_{\mathsf{dec},j}k^*_{L,\mathsf{ran},j}$$

$$+\left\{\begin{array}{ll}(\sigma_{\mathsf{dec}}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{si } \rho_t=0\\ (\sigma_{\mathsf{dec}}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad +\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{si } \rho_t=1\end{array}\right\}$$

$$+\sum_{i=1}^{w_t}\eta_{\mathsf{dec},(0,i)}b^*_{0,1+u_0+1+i}+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathsf{dec},(t,i)}b^*_{t,n_t+u_t+i},$$

$$k^*_{L+1,\mathsf{ran},j'} := \sum_{j=1}^{2L}\alpha_{\mathsf{ran},j',j}k^*_{L,\mathsf{ran},j}$$

$$+\left\{\begin{array}{ll}\sigma_{\mathsf{ran},j'}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{si } \rho_t=0\\ \sigma_{\mathsf{ran},j'}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad +\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{si } \rho_t=1\end{array}\right\}$$

$$+\sum_{i=1}^{w_t}\eta_{\mathsf{ran},j',(0,i)}b^*_{0,1+u_0+1+i}$$

$$+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathsf{ran},j',(t,i)}b^*_{t,n_t+u_t+i},$$

$$k^*_{L+1,\mathsf{ran},(\tau,\iota,0)} := \sum_{j=1}^{2L}\alpha_{\mathsf{ran},(\tau,\iota)j,}k^*_{L,\mathsf{ran},j}+\phi_{\mathsf{ran},(\tau,\iota,0)}k^*_{L,\mathsf{ran},(\tau,\iota,0)}$$

$$+\left\{\begin{array}{ll}\sigma_{\mathsf{ran},(\tau,\iota,0)}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{si } \rho_t=0\\ \sigma_{\mathsf{ran},(\tau,\iota,0)}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad +\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{si } \rho_t=1\end{array}\right\}$$

$$+\sum_{i=1}^{w_t}\eta_{\mathsf{del},(\tau,\iota,0),(0,i)}b^*_{0,1+u_0+1+i}$$

$$+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathsf{del},(\tau,\iota,0),(t,i)}b^*_{t,n_t+u_t+i}$$

$$+\sum_{i=1}^{w_\tau}\eta_{\mathsf{del},(\tau,\iota,0),(\tau,i)}b^*_{\tau,n_\tau+u_\tau+i},$$

[Fórmula 99]

$$k^*_{L+1,\mathsf{del},(\tau,\iota,0)} := \sum_{j=1}^{2L} \alpha_{\mathsf{del},(\tau,\iota,0),j} k^*_{L,\mathsf{ran},j} + \phi_{\mathsf{del},(\tau,\iota,0)} k^*_{L,\mathsf{ran}(\tau,\iota,0)}$$
$$+ \psi_0 k^*_{L,\mathsf{del}(\tau,\iota,0)}$$
$$+ \begin{cases} \sigma_{\mathsf{del},(\tau,\iota,0)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i,0)}\right) & \text{si } \rho_t = 0 \\ \sigma_{\mathsf{del},(\tau,\iota,0)} \left([k^*_{L,\mathsf{del},(L+1,i,1)}]^L \right. & \\ \qquad \left. + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}\right) & \text{si } \rho_t = 1 \end{cases}$$
$$+ \sum_{i=1}^{w_t} \eta_{\mathsf{del},(\tau,\iota,0),(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{del},(\tau,\iota,0),(t,i)} b^*_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathsf{del},(\tau,\iota,0),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$
$$k^*_{L+1,\mathsf{del},(\tau,\iota,1)} := \sum_{j=1}^{2L} \alpha_{\mathsf{del}(\tau,\iota,1),j} k^*_{L,\mathsf{ran},j} + \psi_1 k^*_{L,\mathsf{del}(\tau,\iota,1)}$$
$$+ \begin{cases} \sigma_{\mathsf{del},(\tau,\iota,1)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i,0)}\right) & \text{si } \rho_t = 0 \\ \sigma_{\mathsf{del},(\tau,\iota,1)} \left([k^*_{L,\mathsf{del},(L+1,i,1)}]^L \right. & \\ \qquad \left. + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}\right) & \text{si } \rho_t = 1 \end{cases}$$
$$+ \sum_{i=1}^{w_t} \eta_{\mathsf{del},(\tau,\iota,1),(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{del},(\tau,\iota,1),(t,i)} b^*_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathsf{del},(\tau,\iota,1),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$
$$\mathsf{sk}_{L+1} := (((\vec{v}_1,\rho_1),\ldots,(\vec{v}_{L+1},\rho_{L+1}));$$
$$k^*_{L+1,\mathsf{dec}}, \{k^*_{L+1,\mathsf{ran},j'}\}_{j'=1,\ldots,2(L+1)},$$
$$\{k^*_{L+1,\mathsf{ran},(\tau,\iota,0)}, k^*_{L+1,\mathsf{del},(\tau,\iota,0)}, k^*_{L+1,\mathsf{del},(\tau,\iota,1)}\}_{\tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}),$$
$$\text{devolver } \mathsf{sk}_{L+1}.$$

A continuación se describirá una configuración de hardware del sistema de procesamiento criptográfico 10 (el dispositivo de generación de claves 100, el dispositivo de cifrado 200, el dispositivo de desciframiento 300, el dispositivo de delegación de claves 400) de las realizaciones.

La figura 20 es un diagrama que muestra un ejemplo de una configuración de hardware del dispositivo de generación de claves 100, el dispositivo de cifrado 200, el dispositivo de desciframiento 300 y el dispositivo de delegación de claves 400.

Tal como se muestra en la figura 20, el dispositivo de generación de claves 100, el dispositivo de cifrado 200, el dispositivo de desciframiento 300 y el dispositivo de delegación de claves 400 incluyen cada uno la CPU 911 (unidad central de proceso, denominada asimismo unidad de proceso, unidad aritmética, microprocesador, microordenador o procesador). La CPU 911 está conectada a través de un bus 912, con la ROM 913, la RAM 914, la LCD 901 (pantalla de cristal líquido), el teclado 902 (K/B), la placa de comunicación 915 y el dispositivo de disco magnético 920, y controla estos dispositivos de hardware. El dispositivo de disco magnético 920 (dispositivo de disco fijo) puede ser sustituido por 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 está conectado a través de una interfaz de disco fijo predeterminada.

La ROM 913 y el dispositivo de disco magnético 920 son ejemplos de memoria no volátil. La RAM 914 es un ejemplo de memoria volátil. La ROM 913, la RAM 914 y el dispositivo de disco magnético 920 son ejemplos de 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. La LCD 901 es un ejemplo de un dispositivo de visualización.

El dispositivo de disco magnético 920, la ROM 913, o similar, almacenan un sistema operativo 921 (OS), un sistema de ventanas 922, programas 923 y archivos 924. Los programas 923 son ejecutados 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 anterior, tal como la "unidad de generación de claves maestras 110", la "unidad de almacenamiento de claves maestras 120", la "unidad de introducción de información 130", la "unidad de generación de claves de desciframiento 140", la "unidad de distribución de claves 150", la "unidad de adquisición de clave pública maestra 210", la "unidad de introducción de información 220", la "unidad de generación de texto cifrado 230", la "unidad de transmisión de datos 240", la "unidad de adquisición de clave de desciframiento 310", la "unidad de recepción de datos 320", la "unidad de operación de emparejamiento 330", la "unidad de computación de mensajes 340", la "unidad de adquisición de clave de desciframiento 410", la "unidad de introducción de información 420", la "unidad de generación de claves de delegación 430", la "unidad de distribución de claves 440", y similares, así como otros programas. Los programas son leídos y ejecutados por la CPU 911.

Los archivos 924 almacenan información, datos, valores de señal, valores de variables y parámetros, tal como la "clave pública maestra pk", la "clave secreta maestra sk", la "clave de desciframiento sk_L", la "clave de delegación sk_{L+1}", el "texto cifrado ct", la "información de atributo", la "información de predicado", y el "mensaje m" descritos anteriormente, cada uno de los cuales se almacena como un elemento de un "archivo" o una "base de datos". El "archivo" o la "base de datos" se almacenan en un dispositivo de almacenamiento, tal como un disco o una memoria. La información, datos, valores de señal, valores de variable y parámetros almacenados en el dispositivo de almacenamiento, tal como el disco o una memoria, son leídos por la CPU 911 a través de un circuito de lectura/escritura a una memoria principal o una memoria caché, y se utilizan para operaciones de la CPU 911, tal como extracción, búsqueda, referencia, comparación, cálculo, computación, procesamiento, entrega, 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 tampón durante las operaciones de la CPU 911, tales como la extracción, búsqueda, referencia, comparación, cálculo, computación, procesamiento, entrega, impresión y visualización.

En los diagramas de flujo descritos en lo anterior, una flecha representa principalmente una entrada/salida de datos o de una señal, y cada valor de datos o de señal se almacena en la RAM 914, u otros tipos de medio de almacenamiento, tal como un disco óptico, o un chip IC. Los datos o la señal son transferidos en línea a través del bus 912, una línea de señal, un cable, otros tipos de medio de transferencia, o una onda radioeléctrica.

Lo que se ha descrito en la anterior como "… unidad" puede ser "… circuito", "… dispositivo", "… equipo", "… medio" o "… función", y puede ser asimismo "… etapa", "… procedimiento" o "… proceso". Lo que se ha descrito como "… dispositivo" puede ser "… circuito", "… equipo", "… medio" o "… función", y puede ser asimismo "… etapa", "… procedimiento", o "… proceso". Lo que se ha descrito como "… proceso" puede ser "… etapa". Es decir, lo que se ha descrito como "… unidad" se puede implementar mediante software inalterable almacenado en la ROM 913. Alternativamente, "… unidad" se puede implementar exclusivamente mediante software, o exclusivamente mediante hardware tal como elementos, dispositivos, placas y cableado, o mediante una combinación de software y hardware, o mediante una combinación que incluye software inalterable. El software inalterable o el software está almacenado como un programa en un medio de almacenamiento, tal como la ROM 913. Los programas son leídos por la CPU 911 y ejecutados por la CPU 911. Es decir, cada programa hace que un ordenador, o similar, funcione como una "… unidad" descrita anteriormente. Alternativamente, cada programa hace que el ordenador, o similar, ejecute un procedimiento o un método de una "… unidad" descrita anteriormente.

Lista de signos de referencia

10: sistema de procesamiento criptográfico, 100: dispositivo de generación de claves, 110: unidad de generación de claves maestras, 120: unidad de almacenamiento de claves maestras, 130: unidad de introducción de información, 140: unidad de generación de claves de desciframiento, 141: unidad de generación de números aleatorios, 142: unidad de generación de elementos de desciframiento, 143: unidad de generación de elementos de aleatorización, 144: unidad de generación de elementos de delegación, 150: unidad de distribución de claves, 200: dispositivo de cifrado, 210: unidad de adquisición de clave pública maestra, 220: unidad de introducción de información, 221: unidad de introducción de información de atributo, 222: unidad introducción de mensaje, 230: unidad de generación de texto cifrado, 231: unidad de generación de números aleatorios, 232: unidad de generación de texto cifrado c1, 233: unidad de generación de texto cifrado c2, 240: unidad de transmisión de datos, 300: dispositivo de desciframiento, 310: unidad de adquisición de clave de desciframiento, 320: unidad de recepción de datos, 330: unidad de operación de emparejamiento, 340: unidad de computación de mensajes, 400: dispositivo de delegación de claves, 410: unidad de adquisición de clave de desciframiento, 420: unidad de introducción de información, 430: unidad de generación de claves de delegación, 431: unidad de generación de números aleatorios, 432: unidad de generación de elementos de desciframiento de nivel inferior, 433: unidad de generación de elementos de aleatorización de nivel inferior, 434: unidad de generación de elementos de delegación de nivel inferior, 440: unidad de distribución de claves.

REIVINDICACIONES

1. Un sistema de procesamiento criptográfico 10 que realiza un proceso criptográfico utilizando una base B_t y una base B^*_t para cada número entero t de t = 1, ..., L+1 (siendo L un número entero igual o mayor que 1), comprendiendo el sistema de procesamiento criptográfico:

un dispositivo de cifrado (200) que genera, como un texto cifrado ct, un vector en el que la información de atributo $\vec{x}_t$ está incorporada en un vector de base de la base B_t para por lo menos algún número entero t de t =1, ..., L;

un dispositivo de desciframiento (300) que utiliza, como una clave de desciframiento sk_L, un vector en el que la información de predicado $\vec{v}_t$ está incorporada en un vector de base de la base B^*_t para cada número entero t de t = 1, ..., L, realiza una operación de emparejamiento sobre el texto cifrado ct generado por el dispositivo de cifrado y la clave de desciframiento sk_L, y descifra el texto cifrado ct; y

un dispositivo de delegación de claves (400) que genera una clave de desciframiento de nivel inferior sk_{L+1} de la clave de desciframiento sk_L, en base a un vector en el que la información de predicado $\vec{v}_{L+1}$ está incorporada en un vector de base de una base B^*_{L+1} y a la clave de desciframiento sk_L utilizada por el dispositivo de desciframiento.

2. El sistema de procesamiento criptográfico según la reivindicación 1, que comprende además:

un dispositivo de generación de claves (100) que genera la clave de desciframiento sk_L,

en el que el dispositivo de generación de claves incluye

una primera unidad de introducción de información (130) que introduce información de predicado $\vec{v}_t := (v_{t,i})$ (i = 1, ..., n_t) para cada número entero t de t=1, ..., L;

una unidad de generación de elementos de desciframiento (142) que, utilizando la información de predicado $\vec{v}_t$ introducida por la primera unidad de introducción de información, un valor predeterminado Δ, un valor predeterminado $\theta_{dec,t}$ para cada número entero t de t = 1, ..., L, y un valor predeterminado $s_{dec,t}$ para cada número entero t de t = 0, ..., L de tal modo que $s_{dec,0}=\sum_{t=1}^{L} s_{dec,t}$, genera un elemento de desciframiento $k^*_{L,dec}$ en el que $-s_{dec,0}$ se ajusta como un coeficiente de un vector de la base $b^*_{0,p}$ (siendo p un valor predeterminado) de una base B^*_0, el Δ se ajusta como coeficiente de un vector de la base $b^*_{0,q}$ (q siendo un valor predeterminado) de la base B^*_0, y $s_{dec,t}\vec{e}_{t,1}+\theta_{dec,t}v_{t,i}$ (i = 1, ..., n_t) se ajusta como un coeficiente de un vector de la base $b^*_{t,i}$ (i = 1, ..., n_t) de la base B^*_t para cada número entero t de t = 1, ..., L; y

una unidad de transmisión de claves de desciframiento (150) que transmite al dispositivo de desciframiento la clave de desciframiento sk_L incluyendo el elemento de desciframiento de $k^*_{L,dec}$ generado por la unidad de generación de elementos de desciframiento,

en el que el dispositivo de cifrado incluye

una segunda unidad de introducción de información (220) que introduce información de atributo $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t) para por lo menos algún número entero t de t = 1, ..., L;

una unidad de generación de texto cifrado c1 (232) que, utilizando la información de atributo $\vec{x}_t$ introducida por la segunda unidad de introducción de información y los valores predeterminados ω y ζ, genera un texto cifrado c_1 en el que ω se ajusta como un coeficiente de un vector de la base $b_{0,p}$ de una base B_0, ζ se ajusta como un coeficiente de un vector de la base $b_{0,q}$ de la base B_0, y $\omega x_{t,i}$ (i = 1, ..., n_t) se ajusta como un coeficiente de un vector de la base $b_{t,i}$ (i = 1, ..., n_t) de la base B_t para por lo menos algún número entero t; y

una unidad de transmisión de datos (240) que transmite al dispositivo de desciframiento el texto cifrado ct que incluye el texto cifrado c_1 generado por la unidad de generación del texto cifrado c1, y

en el que el dispositivo de desciframiento incluye

una unidad de operación de emparejamiento (330) que realiza una operación de emparejamiento e (c_1, $k^*_{L,dec}$) sobre el texto cifrado c_1 incluido en el texto cifrado ct transmitido por la unidad de transmisión de datos y el elemento de desciframiento $k^*_{L,dec}$ incluido en la clave de desciframiento sk_L transmitida por la unidad de transmisión de claves de desciframiento.

3. El sistema de procesamiento criptográfico según la reivindicación 2,

en el que el dispositivo de cifrado incluye además

una unidad de generación de texto cifrado c2 (233) que genera un texto cifrado c_2 multiplicando un mensaje m por $g_T^{\Delta\zeta}$ obtenido por un valor $g_T = e(b_{0,1}, b^*_{0,1})$, el Δ y el ζ,

en el que la unidad de transmisión de datos transmite al dispositivo de desciframiento el texto cifrado ct que incluye el texto cifrado c_2 generado por la unidad de generación del texto cifrado c2 y el texto cifrado c_1,

en el que la unidad de operación de emparejamiento realiza la operación de emparejamiento e (c_1, $k^*_{L,dec}$) y calcula una clave de sesión K: = $g_T^{\Delta\zeta}$, y

en el que el dispositivo de descifrado incluye además

una unidad de cálculo de mensajes (340) que calcula el mensaje m dividiendo el texto cifrado c_2 por la clave de sesión K calculada por la unidad de operación de emparejamiento.

4. El sistema de procesamiento criptográfico según la reivindicación 2,

en el que el dispositivo de generación de claves incluye además

una unidad de generación de elementos de delegación (144) que genera un elemento de delegación $k^*_{L,del,(\tau,\iota)}$ para un número entero τ de τ = L+1 y cada número entero ι de ι = 1, ..., n_τ, generando la unidad de generación de elementos de delegación el elemento de delegación $k^*_{L,del,(\tau,\iota)}$ mediante la utilización de un valor predeterminado $\theta_{del,(\tau,\iota),t}$ para cada número entero t de t = 1, ... ,L, un valor predeterminado ψ y un valor predeterminado $s_{del,(\tau,\iota),t}$ para cada número entero t de t = 0, ..., L+1, de tal modo que $s_{del,(\tau,\iota),0} = \sum_{t=1}^{L+1} s_{del,(\tau,\iota),t}$, y ajustando $-s_{del,(\tau,\iota),0}$ como el coeficiente del vector de la base $b^*_{0,p}$ de la base B^*_0, ajustando $s_{del,(\tau,\iota),t}\vec{e}_{t,1}+\theta_{del,(\tau,\iota),t}\vec{v}_{t,i}$ (i = 1, ..., n_t) como el coeficiente del vector de la base $b^*_{t,i}$ (i = 1, ..., n_t) de la base B^*_t para cada número entero t de t = 1, ..., L y ajustando $s_{del,(\tau,\iota),L+1}\vec{e}_{\tau,1}+\psi\vec{e}_{\tau,\iota}$ (i = 1, ..., n_τ) como el coeficiente de un vector de la base $b^*_{\tau,i}$ (i = 1, ..., n_τ) de una base B^*_τ,

en el que la unidad de transmisión de claves de descifrado transmite al dispositivo de delegación la clave de descifrado sk_L que incluye el elemento de delegación $k^*_{L,del,(\tau,\iota)}$ generado por la unidad de generación de elementos de delegación y el elemento de descifrado $k^*_{L,dec}$, y

en el que el dispositivo de delegación de claves incluye

una tercera unidad de introducción de información (420) que introduce información de predicado $\vec{v}_{L+1} := (v_{L+1,i})$ (i = 1, ..., n_{L+1});

una unidad de generación de elementos de descifrado de nivel inferior (432) que, utilizando la información de predicado $\vec{v}_{L+1}$ introducida por la tercera unidad de introducción de información y la clave de descifrado sk_L transmitida por la unidad de transmisión de claves de descifrado, genera un elemento de descifrado de nivel inferior $k^*_{L+1,dec}$ que incluye un vector mostrado en la fórmula 1; y

una unidad de transmisión de claves de delegación (440) que transmite a un dispositivo de descifrado de nivel inferior una clave de descifrado de nivel inferior sk_{L+1} que incluye el elemento de descifrado de nivel inferior $k^*_{L+1,dec}$ generado por la unidad de generación de elementos de descifrado de nivel inferior.

[Fórmula 1]

$$k^*_{L,\mathrm{dec}} + \sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)}$$

5. El sistema de procesamiento criptográfico según la reivindicación 4,

en el que el sistema de procesamiento criptográfico realiza el proceso criptográfico utilizando la base B_0 que tiene por lo menos un vector de la base $b_{0,i}$ (i = 1, ..., $1+n_0$, $1+n_0+1$, ..., $1+n_0+1+u_0$, ..., $1+n_0+1+u_0+w_0$, ..., $1+n_0+1+u_0+w_0+z_0$) (siendo n_0, u_0, w_0, y z_0 respectivamente un número entero igual o mayor que 1),

teniendo la base B^*_0 por lo menos un vector de la base $b^*_{0,i}$ (i = 1, ..., $1+n_0$, $1+n_0+1$, ..., $1+n_0+1+u_0$, ..., $1+n_0+1+u_0+w_0$, ..., $1+n_0+1+u_0+w_0+z_0$) (n_0, u_0, w_0 y z_0 siendo respectivamente un número entero igual o mayor que 1),

teniendo la base B_t (t = 1, ..., L+1) por lo menos un vector de la base $b_{t,i}$ (i = 1, ..., n_t, ..., n_t+u_t, ..., $n_t+u_t+w_t$, ..., $n_t+u_t+w_t+z_t$) (u_t, w_t y z_t siendo respectivamente un número entero igual o mayor que 1), y

teniendo la base B^*_t (t = 1, ..., L+1) por lo menos un vector de la base $b^*_{t,i}$ (i = 1, ..., n_t, ..., n_t+u_t, ..., $n_t+u_t+w_t$, ..., $n_t+u_t+w_t+z_t$),

en el que la unidad de generación de elementos de descifrado genera el elemento de descifrado $k^*_{L,dec}$ como se muestra en la fórmula 2, en base a un número aleatorio $\vec{\eta}_{dec,t} := (\eta_{dec,t,i})$ (i = 1, ..., w_t) para cada número entero t de t = 0, ..., L, y

en el que la unidad de generación del texto cifrado c1 genera el texto cifrado c_1 como se muestra en la fórmula 3, en base a un número aleatorio $\vec{\phi}_t := (\phi_{t,i})$ (i = 1, ..., z_t) para cada número entero t de t = 0, ..., L.

[Fórmula 2]

$$k^*_{L,\mathrm{dec}} := (\ (-s_{\mathrm{dec},0}, 0^{u_0}, \Delta, \vec{\eta}_{\mathrm{dec},0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathrm{dec},t}\ \vec{e}_{t,1} + \theta_{\mathrm{dec},t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{dec},t}, 0^{z_t})_{\mathbb{B}^*_t} : t = 1,...,L)$$

[Fórmula 3]

$$c_1 := (\ (\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t} : t = 1,...,L)$$

6. El sistema de procesamiento criptográfico según la reivindicación 5,

en el que el dispositivo de generación de claves incluye además

una unidad de generación de elementos de aleatorización (143) que genera un primer elemento de aleatorización $k^*_{L,\mathrm{ran},j}$ para cada número entero j de j = 1, ..., 2L, y genera un segundo elemento de aleatorización $k^*_{L,\mathrm{ran},(\tau,\iota)}$ para cada número entero τ de τ = L+1, ..., d (siendo d un número entero de L + 1 o mayor) y cada número entero ι de ι = 1, ..., n_τ con respecto a cada número entero τ,

generando la unidad de generación de elementos de aleatorización el primer elemento de aleatorización $k^*_{L,\mathrm{ran},j}$ como se muestra en la fórmula 4, en base a un valor predeterminado $\theta_{\mathrm{ran},j,t}$ para cada número entero t de t = 1, ..., L, un valor predeterminado $s_{\mathrm{ran},j,t}$ para t = 0, ..., L de tal modo que $s_{\mathrm{ran},j,0} = \sum_{t=1}^{L} s_{\mathrm{ran},j,t}$, y un número aleatorio $\vec{\eta}_{\mathrm{ran},j,t} := (\eta_{\mathrm{ran},j,t,i})$ (i = 1, ..., w_t) para cada número entero t de t = 0, ..., L, y

generar el segundo elemento de aleatorización $k^*_{L,\mathrm{ran},(\tau,\iota)}$ como se muestra en la fórmula 5, en base a un valor predeterminado $\theta_{\mathrm{ran},(\tau,\iota),t}$ para cada número entero t de t = 1, ..., L, un valor predeterminado $s_{\mathrm{ran},(\tau,\iota),t}$ para t = 0, ..., L+1 de tal modo que t $s_{\mathrm{ran},(\tau,\iota),0} = \sum_{t=1}^{L+1} s_{\mathrm{ran},(\tau,\iota),t}$, y un número aleatorio $\vec{\eta}_{\mathrm{ran},(\tau,\iota),t} := (\eta_{\mathrm{ran},(\tau,\iota),t,i})$ (i = 1, ..., w_t) para cada número entero t de t = 0, ..., L+1,

en el que la unidad de generación de elementos de delegación genera el elemento de delegación $k^*_{L(\mathrm{del},(\tau,\iota)}$ como se muestra en la fórmula 6 para cada número entero τ de τ = L+1, ..., d, y cada número entero ι de ι = 1, ..., n_τ con respecto a cada número entero τ, en base a un número aleatorio $\vec{\eta}_{\mathrm{del},(\tau,\iota),t} := (\eta_{\mathrm{del},(\tau,\iota),t,i})$ (i = 1, ..., w_t) para cada número entero t de t = 0, ..., L+1,

en el que la unidad de transmisión de claves de desciframiento transmite al dispositivo de delegación la clave de desciframiento sk_L que incluye el primer elemento de aleatorización $k^*_{L,\mathrm{ran},j}$ y el segundo elemento de aleatorización $k^*_{L,\mathrm{ran},(\tau,\iota)}$ generados por la unidad de generación de elementos de aleatorización, el elemento de delegación $k^*_{L,\mathrm{del},(\tau,\iota)}$ generado por la unidad de generación de elementos de delegación y el elemento de desciframiento $k^*_{L,\mathrm{dec}}$, y

en el que la unidad de generación de elementos de desciframiento de nivel inferior genera el elemento de desciframiento de nivel inferior $k^*_{L+1,\mathrm{dec}}$ como se muestra en la fórmula 7, utilizando la información de predicado $\vec{v}_{L+1}$, la clave de desciframiento sk_L transmitida por la unidad de transmisión de claves de desciframiento, un número aleatorio $\alpha_{\mathrm{dec},j}$ para cada número entero j de j = 1, ..., 2L, un número aleatorio σ_{dec} y un número aleatorio $\eta_{\mathrm{dec},(t,i)}$ para cada número entero t de t = 0, ..., L+1 y cada número entero i de i = 1, ..., w_t.

[Fórmula 4]

$$k^*_{L,\mathrm{ran},j} := (\ (-s_{\mathrm{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},j,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathrm{ran},j,t}\ \vec{e}_{t,1} + \theta_{\mathrm{ran},j,t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,...,L)$$

[Fórmula 5]

$$k^*_{L,\mathsf{ran},(\tau,\iota)} := (\ (-s_{\mathsf{ran},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{ran},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathsf{ran},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{ran},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L$$
$$(s_{\mathsf{ran},(\tau,\iota),L+1}\ \vec{e}_{\tau,1},\ 0^{u_\tau}, \vec{\eta}_{\mathsf{ran},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau})$$

[Fórmula 6]

$$k^*_{L,\mathsf{del},(\tau,\iota)} := (\ (-s_{\mathsf{del},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{del},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{del},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathsf{del},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{del},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L$$
$$(s_{\mathsf{del},(\tau,\iota),L+1}\ \vec{e}_{\tau,1} + \psi\vec{e}_{\tau,\iota}, 0^{u_\tau}, \vec{\eta}_{\mathsf{del},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau})$$

[Fórmula 7]

$$k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + \sum_{j=1}^{2L+1} \alpha_{\mathsf{dec},j} k^*_{L,\mathsf{ran},j}$$
$$+ \sigma_{\mathsf{dec}} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)}) + \sum_{i=1}^{w_t} \eta_{\mathsf{dec},(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{dec},(t,i)} b^*_{t,n_t+u_t+i}$$

7. El sistema de procesamiento criptográfico según la reivindicación 6,

en el que el dispositivo de delegación incluye además

una unidad de generación de elementos de aleatorización de nivel inferior (433) que genera un primer elemento de aleatorización de nivel inferior $k^*_{L+1,\mathsf{ran},j}$ para cada número entero j' de j' = 1, ..., 2(L+1), y genera un segundo elemento de aleatorización de nivel inferior $k^*_{L+1,\mathsf{ran},(\tau,\iota)}$ para cada número entero τ de τ = L+2, ..., d (siendo d un número entero de L + 2 o mayor) y cada número entero ι de ι = 1, ..., n_τ con respecto a cada número entero τ,

generando la unidad de generación de elementos de aleatorización de nivel inferior el primer elemento de aleatorización de nivel inferior $k^*_{L+1,\mathsf{ran},j}$ como se muestra en la fórmula 8, en base a la información de predicado $\vec{v}_{L+1}$, la clave de desciframiento sk_L, un número aleatorio $\alpha_{\mathsf{ran},j',j}$ para cada número entero j de j = 1, ..., 2L y cada número entero j' de j' = 1, ..., 2(L+1), un número aleatorio $\sigma_{\mathsf{ran},j'}$ para cada número entero j' de j' = 1, ..., 2(L+1) y un número aleatorio $\eta_{\mathsf{ran},j',(t,i)}$ para cada número entero t de t = 0, ..., L+1 y cada número entero i de i = 1, ..., w_t, y

generar el segundo elemento de aleatorización de nivel inferior $k^*_{L+1,\mathsf{ran},(\tau,\iota)}$ como se muestra en la fórmula 9, en base a la información de predicado $\vec{v}_{L+1}$, la clave de desciframiento sk_L, un número aleatorio $\alpha_{\mathsf{ran},(\tau,\iota),j}$ para cada número entero j de j = 1, ..., 2L, un número aleatorio $\sigma_{\mathsf{ran},(\tau,\iota)}$, un número aleatorio $\phi_{\mathsf{ran},(\tau,\iota)}$ y un número aleatorio $\eta_{\mathsf{ran},(\tau,\iota),(t,i)}$ para cada número entero t de t = 0, ..., L+1, τ y cada número entero i de i = 1, ..., w_t; y

una unidad de generación de elementos de delegación de nivel inferior (434) que genera un elemento de delegación de nivel inferior $k^*_{L+1,\mathsf{del},(\tau,\iota)}$ para cada número entero τ de τ = L+2, ..., d (siendo d un número entero de L + 2 o mayor) y cada número entero ι de ι = 1, ..., n_τ con respecto a cada número entero τ, generando la unidad de generación de elementos de delegación de nivel inferior el elemento de delegación de nivel inferior $k^*_{L+1,\mathsf{del},(\tau,\iota)}$ como se muestra en la fórmula 10, en base a la información de predicado $\vec{v}_{L+1}$, la clave de desciframiento sk_L, un número aleatorio $\alpha_{\mathsf{del},(\tau,\iota),j}$ para cada número entero j de j = 1, ..., 2L, un número aleatorio $\sigma_{\mathsf{del},(\tau,\iota)}$, un número aleatorio ψ', un número aleatorio $\phi_{\mathsf{del},(\tau,\iota)}$ y un número aleatorio $\eta_{\mathsf{del},(\tau,\iota),(t,i)}$ para cada número entero t de t = 0, ... ,L+1, τ y cada número entero i de i = 1, ..., w_t, y

en el que la unidad de transmisión de claves de delegación transmite a un dispositivo de delegación de nivel inferior una clave de desciframiento de nivel inferior sk_{L+1} que incluye el elemento de desciframiento de nivel inferior $k^*_{L+1,\mathsf{dec}}$

generado por la unidad de generación de elementos de desciframiento de nivel inferior, el primer elemento de aleatorización de nivel inferior $k^*_{L+1,ran,j'}$ y el segundo elemento de aleatorización de nivel inferior $k^*_{L+1,ran,(\tau,\iota)}$ generados por la unidad de generación de elementos de aleatorización de nivel inferior, y el elemento de delegación de nivel inferior $k^*_{L+1,del,(\tau,\iota)}$ generado por la unidad de generación de elementos de delegación de nivel inferior.

[Fórmula 8]

$$k^*_{L+1,\mathrm{ran},j'} := \sum_{j=1}^{2L+1} \alpha_{\mathrm{ran},j',j} k^*_{L,\mathrm{ran},j} + \sigma_{\mathrm{ran},j'} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)} \right) + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(t,i)} b^*_{t,n_t+u_t+i}$$

[Fórmula 9]

$$k^*_{L+1,\mathrm{ran},(\tau,\iota)} := \sum_{j=1}^{2L+1} \alpha_{\mathrm{ran},(\tau,\iota),j} k^*_{L,\mathrm{ran},j} + \sigma_{\mathrm{ran},(\tau,\iota)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)} \right) + \phi_{\mathrm{ran},(\tau,\iota)} k^*_{L,\mathrm{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{ran},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}$$

[Fórmula 10]

$$k^*_{L+1,\mathrm{del},(\tau,\iota)} := \sum_{j=1}^{2L+1} \alpha_{\mathrm{del},(\tau,\iota),j} k^*_{L,\mathrm{ran},j} + \sigma_{\mathrm{del},(\tau,\iota)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)} \right) + \psi' k^*_{L,\mathrm{del},(\tau,\iota)} + \phi_{\mathrm{del},(\tau,\iota)} k^*_{L,\mathrm{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$

8. El sistema de procesamiento criptográfico según la reivindicación 2,

en el que la primera unidad de introducción de información introduce información de predicado ($\vec{v}_t := (v_{t,i})$ (i = 1, ..., n_t), $\rho_t \in \{0, 1\}$) para cada número entero t de t = 1, ..., L, y

en el que la unidad de generación de elementos de desciframiento genera el elemento de desciframiento $k^*_{L,dec}$ en el que $-s_{dec,0}$ se ajusta como el coeficiente del vector de la base $b^*_{0,p}$, Δ se ajusta como el coeficiente del vector de la base $b^*_{0,q}$, y $s_{dec,t}\vec{e}_{t,1}+\theta_{dec,t}v_{t,i}$ (i = 1, ..., n_t) cuando ρ_t es 0 o $s_{dec,t}v_{t,i}$ (i = 1, ..., n_t) cuando ρ_t es 1 se ajusta como el coeficiente del vector de la base $b^*_{t,i}$ para cada número entero t de t = 1, ..., L.

9. El sistema de procesamiento criptográfico según la reivindicación 8,

en el que el dispositivo de generación de claves incluye además

una unidad de generación de elementos de delegación (144) que genera un primer elemento de delegación $k^*_{L,del,(\tau,\iota,0)}$ y un segundo elemento de delegación $k^*_{L,del,(\tau,\iota,1)}$ para un número entero τ de $\tau = L+1$ y cada número entero ι de $\iota = 1, ..., n_\tau$,

generando la unidad de generación de elementos de delegación el primer elemento de delegación $k^*_{L,del,(\tau,\iota,0)}$ utilizando un valor predeterminado $\theta_{del,0,t}$ para cada número entero t de t = 1, ..., L, un valor predeterminado ψ y un valor predeterminado $s_{del,0,t}$ para t = 0, ..., L+1 de tal modo que $s_{del,0,0}=\sum_{t=1}^{L+1} s_{del,0,t}$, y ajustando $-s_{del,0,0}$ como el coeficiente del vector de la base $b^*_{0,p}$ de la base B^*_0, ajustando $s_{del,0,t}\vec{e}_{t,1}+\theta_{del,0,t}v_{t,i}$ (i = 1, ..., n_t) cuando ρ_t es 0 o $s_{del,0,t}v_{t,i}$ (i = 1, ..., n_t) cuando ρ_t es 1 como el coeficiente del vector de la base $b^*_{t,i}$ (i = 1, ..., n_t) para cada número entero t de t = 1, ..., L, y ajustando $s_{del,0,L+1}\vec{e}_{\tau,1}+\psi\vec{e}_{\tau,\iota}$ (i = 1, ..., n_τ) como un coeficiente de un vector de la base $b^*_{\tau,i}$ (i = 1, ..., n_τ) de una base B^*_τ, y

generar el segundo elemento de delegación $k^*_{L,del,(\tau,\iota,1)}$ utilizando un valor predeterminado $\theta_{del,1,t}$ para cada número entero t de t = 1, ..., L y un valor predeterminado $s_{del,1,t}$ para t = 0, ..., L+1 de tal modo que $s_{del,1,0}=\sum_{t=1}^{L+1} s_{del,1,t}$, y ajustando $-s_{del,1,0}$ como el coeficiente del vector de la base $b^*_{0,p}$ de la base B^*_0, ajustando $s_{del,1,t}\vec{e}+\theta_{del,1,t}v_{t,i}$ (i = 1, ..., n_t) cuando ρ_t es 0 o $s_{del,1,t}v_{t,i}$ (i = 1, ..., n_t) cuando ρ_t es 1 como el coeficiente del vector de la base $b^*_{t,i}$ (i = 1, ..., n_t) de la base B^*_t para cada número entero t de t = 1, ..., L, y ajustando $s_{del,1,L+1}\vec{e}_{\tau,1}$ (i = 1, ..., n_τ) como el coeficiente del vector de la base $b^*_{\tau,i}$ (i = 1, ..., n_τ) de la base B^*_τ,

en el que la unidad de transmisión de claves de desciframiento transmite al dispositivo de delegación la clave de desciframiento sk_L que incluye el primer elemento de delegación $k^*_{L,del,(\tau,\iota,0)}$ y el segundo elemento de delegación $k^*_{L,del,(\tau,\iota,1)}$ generados por la unidad de generación de elementos de delegación y el elemento de desciframiento $k^*_{L,dec}$, y

en el que el dispositivo de delegación de claves incluye

una tercera unidad de introducción de información (420) que introduce información de predicado $\vec{v}_{L+1} := (v_{L+1,i})$ (i= 1, ..., n_{L+1}), $\rho_{L+1} \in \{0, 1\}$); y

una unidad de generación de elementos de desciframiento de nivel inferior (432) que genera un elemento de desciframiento de nivel inferior $k^*_{L+1,dec}$ que incluye un vector mostrado en la fórmula 11, utilizando la información de predicado $\vec{v}_{L+1}$ introducida por la tercera unidad de introducción de información y la clave de desciframiento sk_L transmitida por la unidad de transmisión de claves de desciframiento.

[Fórmula 11]

$$k^*_{L,\mathrm{dec}} + \begin{cases} (\sigma_{\mathrm{dec}}(\sum_{t=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{si } \rho_t = 0 \\ (\sigma_{\mathrm{dec}}([k^*_{L,\mathrm{del},(L+1,i,1)}]^L \\ \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i}[k^*_{L,\mathrm{del},(L+1,i,1)}]_L) & \text{si } \rho_t = 1 \end{cases}$$

10. El sistema de procesamiento criptográfico según la reivindicación 9,

en el que el sistema de procesamiento criptográfico realiza el proceso criptográfico utilizando la base B_0 que tiene por lo menos un vector de la base $b_{0,i}$ (i = 1, ..., $1+n_0$, $1+n_0+1$, ..., $1+n_0+1+u_0$, ..., $1+n_0+1+u_0+w_0$, ..., $1+n_0+1+u_0+w_0+z_0$) (siendo n_0, u_0, w_0, y z_0 respectivamente un número entero igual o mayor que 1),

teniendo la base B^*_0 por lo menos un vector de la base $b^*_{0,i}$ (i = 1, ..., $1+n_0$, $1+n_0+1$, ..., $1+n_0+1+u_0$, ..., $1+n_0+1+u_0+w_0$, ..., $1+n_0+1+u_0+w_0+z_0$) (n_0, u_0, w_0 y z_0 siendo respectivamente un número entero igual o mayor que 1),

teniendo la base B_t (t = 1, ..., L+1) por lo menos un vector de la base $b_{t,i}$ (i = 1, ..., n_t, ..., n_t+u_t, ..., $n_t+u_t+w_t$, ..., $n_t+u_t+w_t+z_t$) (u_t, w_t y z_t siendo respectivamente un número entero igual o mayor que 1), y

teniendo la base B^*_t (t = 1, ..., L+1) por lo menos un vector de la base $b^*_{t,i}$ (i = 1, ..., n_t, ..., n_t+u_t, ..., $n_t+u_t+w_t$, ..., $n_t+u_t+w_t+z_t$),

en el que la unidad de generación de elementos de desciframiento genera el elemento de desciframiento $k^*_{L,ded}$ como se muestra en la fórmula 12, en base a un número aleatorio $\vec{\eta}_{dec,t} := (\eta_{dec,t,i})$ (i = 1, ..., w_t) para cada número entero t de t = 0, ..., L, y

en el que la unidad de generación del texto cifrado c1 genera el texto cifrado c_1 como se muestra en la fórmula 13, en base a un número aleatorio $\vec{\phi}_t := (\phi_{t,i})$ (i = 1, ..., z_t) para cada número entero t de t = 0, ..., L.

[Fórmula 12]

$$k^{*}_{L,\mathrm{dec}} := \Big((-s_{\mathrm{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathrm{dec},0}, 0^{z_0})_{\mathbb{B}^{*}_{0}},$$
$$\left\{ \begin{array}{ll} (s_{\mathrm{dec},t}\vec{e}_{t,1} + \theta_{\mathrm{dec},t}, \vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{dec},t}, 0^{z_t})_{\mathbb{B}^{*}_{t}}, & \text{si } \rho_t = 0 \\ (s_{\mathrm{dec},t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{dec},t}, 0^{z_t})_{\mathbb{B}^{*}_{t}}, & \text{si } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, \ldots, L \Big)$$

[Fórmula 13]

$$c_1 := \Big((\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t} : t = 1, \ldots, L \Big)$$

11. El sistema de procesamiento criptográfico según la reivindicación 10,

en el que el dispositivo de generación de claves incluye además

una unidad de generación de elementos de aleatorización (143) que genera un primer elemento de aleatorización $k^{*}_{L,\mathrm{ran},j}$ para cada número entero j de j = 1, ..., 2L, y genera un segundo elemento de aleatorización $k^{*}_{L,\mathrm{ran},(\tau,\iota,0)}$ para cada número entero τ de τ = L+1, ..., d (siendo d un número entero de L + 1 o mayor) y cada número entero ι de ι = 1, ..., n_τ con respecto a cada número entero τ,

generando la unidad de generación de elementos de aleatorización el primer elemento de aleatorización $k^{*}_{L,\mathrm{ran},j}$ como se muestra en la fórmula 14, en base a un valor predeterminado $\theta_{\mathrm{ran},j,t}$ para cada número entero t de t = 1, ..., L, un valor predeterminado $s_{\mathrm{ran},j,t}$ para t = 0 de tal modo que $s_{\mathrm{ran},j,0} = \sum_{t=1}^{L} s_{\mathrm{ran},j,t}$, y un número aleatorio $\vec{\eta}_{\mathrm{ran},j,t} := (\eta_{\mathrm{ran},j,t,i})$ (i = 1, ..., w_t) para cada número entero t de t = 0, ..., L, y

generar el segundo elemento de aleatorización $k^{*}_{L,\mathrm{ran},(\tau,\iota,0)}$ como se muestra en la fórmula 15, en base a un valor predeterminado $\theta_{\mathrm{ran},0,t}$ para cada número entero t de t = 1, ..., L, un valor predeterminado $s_{\mathrm{ran},0,t}$ para t = 0, ..., L+1 de manera que $s_{\mathrm{ran},0,0} = \sum_{t=1}^{L+1} s_{\mathrm{ran},0,t}$, un número aleatorio $\vec{\eta}_{\mathrm{ran},0,t} := (\eta_{\mathrm{ran},0,t,i})$ (i = 1, ..., w_t) para cada número entero t de t = 0, ..., L, y un número aleatorio $\vec{\eta}_{\mathrm{ran},0,(\tau,\iota)} := (\eta_{\mathrm{ran},0,(\tau,\iota),i})$ (i = 1, ..., W_t),

en el que la unidad de generación de elementos de delegación genera el primer elemento de delegación $k^{*}_{L,\mathrm{del},(\tau,\iota,0)}$ como se muestra en la fórmula 16 para cada número entero τ de τ = L+1, ..., d y cada número entero ι de ι = 1, ..., n_τ con respecto a cada número entero τ, en base a un número aleatorio $\vec{\eta}_{\mathrm{del},0,t} := (\eta_{\mathrm{del},0,t,i})$ (i = 1, ..., w_t) para cada número entero t de t = 0, ..., L y un número aleatorio $\vec{\eta}_{\mathrm{del},0,(\tau,\iota)} := (\eta_{\mathrm{del},0,(\tau,\iota),i})$ (i = 1, ..., w_t), y genera el segundo elemento de delegación $k^{*}_{L,\mathrm{del},(\tau,\iota,1)}$ como se muestra en la fórmula 17 para cada número entero τ de τ = L+1, ..., d y cada número entero ι de ι = 1, ..., n_τ con respecto a cada número entero τ, en base a un número aleatorio $\vec{\eta}_{\mathrm{del},1,t} := (\eta_{\mathrm{del},1,t,i})$ (i = 1, ..., w_t) para cada número entero t de t = 0, ..., L y un número aleatorio $\vec{\eta}_{\mathrm{del},1,(\tau,\iota)} := (\eta_{\mathrm{del},1,(\tau,\iota),i})$ (i = 1, ..., W_t),

en el que la unidad de transmisión de claves de desciframiento transmite al dispositivo de delegación la clave de desciframiento sk_L que incluye el primer elemento de aleatorización $k^{*}_{L,\mathrm{ran},j}$ y el segundo elemento de aleatorización $k^{*}_{L,\mathrm{ran},(\tau,\iota,0)}$ generados por la unidad de generación de elementos de aleatorización, el primer elemento de delegación $k^{*}_{L,\mathrm{del},(\tau,\iota,0)}$ y el segundo elemento de delegación $k^{*}_{L,\mathrm{del},(\tau,\iota,1)}$ generados por la unidad de generación de elementos de delegación, y el elemento de desciframiento $k^{*}_{L,\mathrm{dec}}$, y

en el que la unidad de generación de elementos de desciframiento de nivel inferior genera el elemento de desciframiento de nivel inferior $k^{*}_{L+1,\mathrm{dec}}$ como se muestra en la fórmula 18, utilizando la información de predicado $\vec{v}_{L+1}$, la clave de desciframiento sk_L transmitida por la unidad de transmisión de claves de desciframiento, un número aleatorio $\alpha_{\mathrm{dec},j}$ para cada número entero j de j = 1, ..., 2L, un número aleatorio σ_{dec} y un número aleatorio $\eta_{\mathrm{dec},(t,i)}$ para cada número entero t de t = 0, ..., L+1 y cada número entero i de i = 1, ..., w_t.

[Fórmula 14]

$$k^{*}_{L,\mathrm{ran},j} := (\ (-s_{\mathrm{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},j,0}, 0^{z_0})_{\mathbb{B}^{*}_{0}},$$
$$\left\{\begin{array}{ll} (s_{\mathrm{ran},j,t}\vec{e}_{t,1} + \theta_{\mathrm{ran},j,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{ran},j,t}, 0^{z_t})_{\mathbb{B}^{*}_{t}}, & \text{si } \rho_t = 0 \\ (s_{\mathrm{ran},j,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{ran},j,t}, 0^{z_t})_{\mathbb{B}^{*}_{t}}, & \text{si } \rho_t = 1 \end{array}\right\}$$
$$: t = 1, \ldots, L)$$

[Fórmula 15]

$$k^{*}_{L,\mathrm{ran},(\tau,t,0)} := (\ (-s_{\mathrm{ran},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},0,0}, 0^{z_0})_{\mathbb{B}^{*}_{0}},$$
$$\left\{\begin{array}{ll} (s_{\mathrm{ran},0,t}\vec{e}_{t,1} + \theta_{\mathrm{ran},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{ran},0,t}, 0^{z_t})_{\mathbb{B}^{*}_{t}}, & \text{si } \rho_t = 0 \\ (s_{\mathrm{ran},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{ran},0,t}, 0^{z_t})_{\mathbb{B}^{*}_{t}}, & \text{si } \rho_t = 1 \end{array}\right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathrm{ran},0,L+1}\vec{e}_{\tau,1}, 0^{u_\tau}, \vec{\eta}_{\mathrm{ran},0,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^{*}_{\tau}})$$

[Fórmula 16]

$$k^{*}_{L,\mathrm{del},(\tau,t,0)} := (\ (-s_{\mathrm{del},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{del},0,0}, 0^{z_0})_{\mathbb{B}^{*}_{0}},$$
$$\left\{\begin{array}{ll} (s_{\mathrm{del},0,t}\vec{e}_{t,1} + \theta_{\mathrm{del},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{del},0,t}, 0^{z_t})_{\mathbb{B}^{*}_{t}}, & \text{si } \rho_t = 0 \\ (s_{\mathrm{del},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{del},0,t}, 0^{z_t})_{\mathbb{B}^{*}_{t}}, & \text{si } \rho_t = 1 \end{array}\right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathrm{del},0,L+1}\vec{e}_{\tau,1}, +\psi\vec{e}_{\tau,t}, 0^{u_\tau}, \vec{\eta}_{\mathrm{del},0,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^{*}_{\tau}})$$

[Fórmula 17]

$$k^{*}_{L,\mathrm{del},(\tau,t,1)} := (\ (-s_{\mathrm{del},1,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{del},1,0}, 0^{z_0})_{\mathbb{B}^{*}_{0}},$$
$$\left\{\begin{array}{ll} (s_{\mathrm{del},1,t}\vec{e}_{t,1} + \theta_{\mathrm{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{del},1,t}, 0^{z_t})_{\mathbb{B}^{*}_{t}} & \text{si } \rho_t = 0 \\ (s_{\mathrm{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{del},1,t}, 0^{z_t})_{\mathbb{B}^{*}_{t}}, & \text{si } \rho_t = 1 \end{array}\right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathrm{del},1,L+1}\vec{e}_{\tau,t}, 0^{u_\tau}, \vec{\eta}_{\mathrm{del},1,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^{*}_{\tau}})$$

[Fórmula 18]

$$k^{*}_{L+1,\mathsf{dec}} := k^{*}_{L,\mathsf{dec}} + \sum_{j=1}^{2L+1} \alpha_{\mathsf{dec},j} k^{*}_{L,\mathsf{ran},j}$$
$$+ \left\{ \begin{array}{ll} (\sigma_{\mathsf{dec}}(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathsf{del},(L+1,i,0)}) & \text{si } \rho_t = 0 \\ (\sigma_{\mathsf{dec}}([k^{*}_{L,\mathsf{del},(L+1,i,1)}]^{L} & \\ \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i}[k^{*}_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{si } \rho_t = 1 \end{array} \right\}$$
$$+ \sum_{i=1}^{w_t} \eta_{\mathsf{dec},(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{dec},(t,i)} b^{*}_{t,n_t+u_t+i}$$

12. El sistema de procesamiento criptográfico según la reivindicación 11,

en el que el dispositivo de delegación incluye además

una unidad de generación de elementos de aleatorización de nivel inferior (433) que genera un primer elemento de aleatorización de nivel inferior $k^{*}_{L+1,ran,j'}$ para cada número entero j' de j' = 1, ..., 2(L+1), y genera un segundo elemento de aleatorización de nivel inferior $k^{*}_{L+1,ran,(\tau,\iota,0)}$ para cada número entero τ de τ = L+2, ..., d (siendo d un número entero de L + 2 o mayor) y cada número entero ι de ι = 1, ..., n_τ con respecto a cada número entero τ,

generando la unidad de generación de elementos de aleatorización de nivel inferior el primer elemento de aleatorización de nivel inferior $k^{*}_{L+1,ran,j}$ como se muestra en la fórmula 19, en base a la información de predicado $\vec{v}_{L+1}$, la clave de desciframiento sk_L, un número aleatorio $\alpha_{ran,j',j}$ para cada número entero j de j = 1, ..., 2L y cada número entero j' de j' = 1, ..., 2(L+1), un número aleatorio $\sigma_{ran,j'}$ para cada número entero j' de j' = 1, ..., 2(L+1) y un número aleatorio $\eta_{ran,j',(t,i)}$ para cada número entero t de t = 0, ..., L+1 y cada número entero i de i = 1, ..., w_t, y

generar el segundo elemento de aleatorización de nivel inferior $k^{*}_{L+1,ran,(\tau,\iota,0)}$ como se muestra en la fórmula 20, en base a la información de predicado $\vec{v}_{L+1}$, la clave de desciframiento sk_L, un número aleatorio $\alpha_{ran,(\tau,\iota),j}$ para cada número entero j de j = 1, ..., 2L, un número aleatorio $\sigma_{ran,(\tau,\iota,0)}$, un número aleatorio $\phi_{ran,(\tau,\iota,0)}$ y un $\eta_{ran,(\tau,\iota,0),(t,i)}$ para cada número entero t de t = 0, ..., L+1 y cada número entero i de i = 1, ..., w_t; y

una unidad de generación de elementos de delegación de nivel inferior (434) que genera un primer elemento de delegación de nivel inferior $k^{*}_{L+1,del,(\tau,\iota,0)}$ y un segundo elemento de delegación de nivel inferior $k^{*}_{L+1,del,(\tau,\iota,1)}$ para cada número entero τ de τ = L+2, ..., d (siendo d un número entero de L + 2 o mayor) y cada número entero ι de ι = 1, ..., n con respecto a cada número entero τ,

generando la unidad de generación de elementos de delegación de nivel inferior el primer elemento de delegación de nivel inferior $k^{*}_{L+1,del,(\tau,\iota,0)}$ como se muestra en la fórmula 21, en base a la información de predicado $\vec{v}_{L+1}$, la clave de desciframiento sk_L, un número aleatorio $\alpha_{del,(\tau,\iota,0),j}$ para cada número entero j de j = 1, ..., 2L, un número aleatorio $\sigma_{del,(\tau,\iota,0)}$, un número aleatorio ψ_0, un número aleatorio $\phi_{del,(\tau,\iota,0)}$ y $\eta_{del,(\tau,\iota,0),(t,i)}$ para cada número entero t de t = 0, ..., L+1 y cada número entero i de i = 1, ..., w_t, y

generando el segundo elemento de delegación de nivel inferior $k^{*}_{L+1,del,(\tau,\iota,1)}$ como se muestra en la fórmula 22, en base a la información de predicado $\vec{v}_{L+1}$, la clave de desciframiento sk_L, un número aleatorio $\alpha_{del,(\tau,\iota,1),j}$ para cada número entero j de j = 1, ..., 2L y un número aleatorio $\sigma_{del,(\tau,\iota,1)}$, un número aleatorio ψ_1, un número aleatorio $\phi_{del,(\tau,\iota,1)}$ y $\eta_{del,(\tau,\iota,1),(t,i)}$ para cada número entero t de t = 0, ..., L+1 y cada número entero i de i = 1, ..., w_t.

[Fórmula 19]

$$k^{*}_{L+1,\mathrm{ran},j'} := \sum_{j=1}^{2L+1} \alpha_{\mathrm{ran},j',j} k^{*}_{L,\mathrm{ran},j} + \left\{ \begin{array}{ll} \sigma_{\mathrm{ran},j'} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i,0)} \right) & \text{si } \rho_t = 0 \\ \sigma_{\mathrm{ran},j'} \left([k^{*}_{L,\mathrm{del},(L+1,i,1)}]^{L} \right. & \\ \left. \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^{*}_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}} \right) & \text{si } \rho_t = 1 \end{array} \right\} + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(t,i)} b^{*}_{t,n_t+u_t+i}$$

[Fórmula 20]

$$k^{*}_{L+1,\mathrm{ran}(\tau,\iota,0)} := \sum_{j=1}^{2L+1} \alpha_{\mathrm{ran},(\tau,\iota)j,} k^{*}_{L,\mathrm{ran},j} + \phi_{\mathrm{ran},(\tau,\iota,0)} k^{*}_{L,\mathrm{ran},(\tau,\iota,0)} + \left\{ \begin{array}{ll} \sigma_{\mathrm{ran},(\tau,\iota,0)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i,0)} \right) & \text{si } \rho_t = 0 \\ \sigma_{\mathrm{ran},(\tau,\iota,0)} \left([k^{*}_{L,\mathrm{del},(L+1,i,1)}]^{L} \right. & \\ \left. \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^{*}_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}} \right) & \text{si } \rho_t = 1 \end{array} \right\} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^{*}_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^{*}_{\tau,n_\tau+u_\tau+i}$$

[Fórmula 21]

$$k^{*}_{L+1,\mathrm{del}(\tau,\iota,0)} := \sum_{j=1}^{2L+1} \alpha_{\mathrm{del},(\tau,\iota,0),j} k^{*}_{L,\mathrm{ran},j} + \phi_{\mathrm{del},(\tau,\iota,0)} k^{*}_{L,\mathrm{ran}(\tau,\iota,0)} + \psi_0 k^{*}_{L,\mathrm{del}(\tau,\iota,0)} + \left\{ \begin{array}{ll} \sigma_{\mathrm{del},(\tau,\iota,0)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i,0)} \right) & \text{si } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,0)} \left([k^{*}_{L,\mathrm{del},(L+1,i,1)}]^{L} \right. & \\ \left. \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^{*}_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}} \right) & \text{si } \rho_t = 1 \end{array} \right\} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^{*}_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^{*}_{\tau,n_\tau+u_\tau+i}$$

[Fórmula 22]

$$k^*_{L+1,\mathsf{del}(\tau,\iota,1)} := \sum_{j=1}^{2L+1} \alpha_{\mathsf{del}(\tau,\iota,1),j} k^*_{L,\mathsf{ran},j} + \psi_1 k^*_{L,\mathsf{del}(\tau,\iota,1)}$$
$$+ \begin{cases} \sigma_{\mathsf{del},(\tau,\iota,1)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i,0)}\right) & \text{si } \rho_t = 0 \\ \sigma_{\mathsf{del},(\tau,\iota,1)} \left([k^*_{L,\mathsf{del},(L+1,i,1)}]^L \right. & \\ \qquad \left. + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathsf{del},(L+1,i,1)}]_L\right) & \text{si } \rho_t = 1 \end{cases}$$
$$+ \sum_{i=1}^{w_t} \eta_{\mathsf{del},(\tau,\iota,1),(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathsf{del},(\tau,\iota,1),(t,i)} b^*_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathsf{del},(\tau,\iota,1),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}$$

13. Un dispositivo de generación de claves (100) que genera una clave de desciframiento sk_L en un sistema de procesamiento criptográfico 10 que realiza un proceso criptográfico utilizando una base B_t y una base B^*_t para cada número entero t de t = 1, ..., L (siendo L un número entero igual o mayor que 1), comprendiendo el dispositivo de generación de claves:

una primera unidad de introducción de información (130) que introduce información de predicado $\vec{v}_t := (v_{t,i})$ (i = 1, ..., n_t) para cada número entero t de t = 1, ..., L;

una unidad de generación de elementos de desciframiento (142) que, utilizando la información de predicado $\vec{v}_t$ introducida por la primera unidad de introducción de información, un valor predeterminado Δ, un valor predeterminado $\theta_{dec,t}$ para cada número entero t de t = 1, ..., L, y un valor predeterminado $s_{dec,t}$ para cada número entero t de t = 0, ..., L de tal modo que $s_{dec,0}=\sum_{t=1}^{L} s_{dec,t}$, genera un elemento de desciframiento $k^*_{L,dec}$ en el que $-s_{dec,0}$ se ajusta como un coeficiente de un vector de la base $b^*_{0,p}$ (siendo p un valor predeterminado) de una base B^*_0, Δ se ajusta como coeficiente de un vector de la base $b^*_{0,q}$ (q siendo un valor predeterminado) de la base B^*_0, y $s_{dec,t}\vec{e}_{t,1}+\theta_{dec,t}v_{t,i}$ (i = 1, ..., n_t) se ajusta como un coeficiente de un vector de la base $b^*_{t,i}$ (i = 1, ..., n_t) de la base B^*_t para cada número entero t de t = 1, ..., L; y

una unidad de transmisión de claves de desciframiento (150) que transmite a un dispositivo de desciframiento la clave de desciframiento sk_L incluyendo el elemento de desciframiento de $k^*_{L,dec}$ generado por la unidad de generación de elementos de desciframiento,

14. Un dispositivo de cifrado (200) que genera un texto cifrado ct en un sistema de procesamiento criptográfico que realiza un proceso criptográfico utilizando una base B_t y una base B^*_t para cada número entero t de t = 1, ..., L (siendo L un número entero igual o mayor que 1), comprendiendo el dispositivo de cifrado:

una segunda unidad de introducción de información (220) que introduce información de atributo $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t) para por lo menos algún número entero t de t = 1, ..., L;

una unidad de generación de texto cifrado c1 (232) que, utilizando la información de atributo $\vec{x}_t$ introducida por la segunda unidad de introducción de información y los valores predeterminados ω y ζ, genera un texto cifrado c_1 en el que ω se ajusta como un coeficiente de un vector de la base $b_{0,p}$ (siendo p un valor predeterminado) de una base B_0, ζ se ajusta como un coeficiente de un vector de la base $b_{0,q}$ (siendo q un valor predeterminado) de la base B_0, y $\omega x_{t,i}$ (i = 1, ..., n_t) se ajusta como un coeficiente de un vector de la base $b_{t,i}$ (i = 1, ..., n_t) de la base B_t para por lo menos algún número entero t; y

una unidad de transmisión de datos (240) que transmite a un dispositivo de desciframiento el texto cifrado ct que incluye el texto cifrado c_1 generado por la unidad de generación del texto cifrado c1.

15. Un dispositivo de desciframiento (300) que descifra un texto cifrado c_1 mediante una clave de desciframiento sk_L en un sistema de procesamiento criptográfico que realiza un proceso criptográfico utilizando una base B_t y una base B^*_t para cada número entero t de t =1, ..., L (siendo L un número entero igual o mayor que 1), comprendiendo el dispositivo de desciframiento:

una unidad de recepción de datos (320) que recibe de un dispositivo de cifrado el texto cifrado c_1 en que, utilizando información de atributo de $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t) y valores predeterminados ω y ζ, ω se ajusta como un coeficiente de un vector de la base $b_{0,p}$ (siendo p un valor predeterminado) de una base B_0, ζ se ajusta como un coeficiente de

un vector de la base $b_{0,q}$ (siendo q un valor predeterminado) de la base B_0, y $\omega x_{t,i}$ (i = 1, ..., n_t) se ajusta como un coeficiente de un vector de la base $b_{t,i}$ (i = 1, ..., n_t) de la base B_t para por lo menos algún número entero t;

una unidad de adquisición de clave de desciframiento (310) que obtiene de un dispositivo de generación de claves la clave de desciframiento sk_L incluyendo un elemento de desciframiento $k^*_{L,dec}$ en que, utilizando información de predicado $\vec{v}_t$: = ($v_{t,i}$) (i = 1, ..., n_t), un valor predeterminado Δ, un valor predeterminado $\theta_{dec,t}$ para cada número entero t de t = 1, ..., L, y un valor predeterminado $s_{dec,t}$ para cada número entero t de t = 0, ..., L de tal modo que $s_{dec,0}=\sum_{t=1}^{L} s_{dec,t}$, $-s_{dec,0}$ se ajusta como un coeficiente de un vector de la base $b^*_{0,p}$ (siendo p un valor predeterminado) de una base B^*_0, Δ se ajusta como un coeficiente de un vector de la base $b^*_{0,q}$ (siendo q un valor predeterminado) de la base B^*_0, y $s_{dec,t}\vec{e}_{t,1}+\theta_{dec,t}v_{t,i}$ (i = 1, ..., n_t) se ajusta como un coeficiente de un vector de la base $b^*_{t,i}$ (i = 1, ..., n_t) de la base B^*_t para cada número entero t de t = 1, ..., L; y

una unidad de operación de emparejamiento (330) que realiza una operación de emparejamiento e (c_1, $k^*_{L,dec}$) sobre el texto cifrado c_1 recibido por la unidad de recepción de datos y el elemento de desciframiento $k^*_{L,dec}$ incluido en la clave de desciframiento k_L obtenida por la unidad de adquisición de clave de desciframiento, y descifra el texto cifrado c_1.

16. Un dispositivo de delegación de claves (400) que genera una clave de desciframiento de nivel inferior sk_{L+1} de una clave de desciframiento sk_L en un sistema de procesamiento criptográfico que realiza un proceso criptográfico utilizando una base B_t y una base B^*_t para cada número entero t de t = 1, ..., L+1 (siendo L un número entero mayor o igual que 1), comprendiendo el dispositivo de delegación de claves:

una unidad de adquisición de clave de desciframiento (410) que obtiene, como la clave de desciframiento sk_L, un vector en el que está incorporada información de predicado $\vec{v}_t$ en un vector de base de la base B^*_t para cada número entero t de t = 1, ..., L; y

una unidad de generación de claves de delegación (430) que genera la clave de desciframiento de nivel inferior sk_{L+1} de la clave de desciframiento sk_L, en base a la clave de desciframiento sk_L obtenida mediante la unidad de adquisición de clave de desciframiento y a un vector en el que está incorporada información de predicado $\vec{v}_{L+1}$ en un vector de la base de una base B^*_{L+1}.

17. Un método de procesamiento criptográfico que utiliza una base B_t y una base B^*_t para cada número entero t de t = 1, ..., L+1 (siendo L un número entero mayor o igual que 1), comprendiendo el método de procesamiento criptográfico:

un proceso de cifrado mediante un dispositivo de cifrado (200) para generar, como un texto cifrado ct, un vector en el que la información de atributo $\vec{x}_t$ está incorporada en un vector de base de la base B_t para por lo menos algún número entero t de t =1, ..., L;

un proceso de desciframiento mediante un dispositivo de desciframiento (300) que utiliza, como una clave de desciframiento sk_L, un vector en el que está incorporada información de predicado $\vec{v}_t$ en un vector de base de la base B^*_t para cada número entero t de t = 1,..., L, realiza una operación de emparejamiento sobre el texto cifrado ct generado en el proceso de cifrado y la clave de desciframiento sk_L, y descifra el texto cifrado ct; y

un proceso de delegación de clave mediante un dispositivo de delegación de claves (400) que genera una clave de desciframiento de nivel inferior sk_{L+1} de la clave de desciframiento sk_L, en base a un vector $\vec{v}_{L+1}$ en el que está incorporada información de predicado en un vector de la base de una base B^*_{L+1} y a la clave de desciframiento sk_L utilizada en el proceso de desciframiento.

18. Un programa de procesamiento criptográfico que ejecuta un proceso criptográfico utilizando una base B_t y una base B^*_t para cada número entero t de t = 1, ..., L+1 (siendo L un número entero igual o mayor que 1), comprendiendo el programa de procesamiento criptográfico:

un proceso de cifrado que genera, como un texto cifrado ct, un vector en el que la información de atributo $\vec{x}_t$ está incorporada en un vector de base de la base B_t para por lo menos algún número entero t de t =1, ..., L;

un proceso de desciframiento que utiliza, como una clave de desciframiento sk_L, un vector en el que está incorporada información de predicado $\vec{v}_t$ en un vector de base de la base B^*_t para cada número entero t de t = 1, ..., L, realiza una operación de emparejamiento sobre el texto cifrado ct generado por el proceso de cifrado y la clave de desciframiento sk_L, y descifra el texto cifrado ct; y

un proceso de delegación de clave que genera una clave de desciframiento de nivel inferior sk_{L+1} de la clave de desciframiento sk_L, en base a un vector $\vec{v}_{L+1}$ en el que está incorporada información de predicado en un vector de la base de una base B^*_{L+1} y a la clave de desciframiento sk_L utilizada en el proceso de desciframiento.

Fig. 1

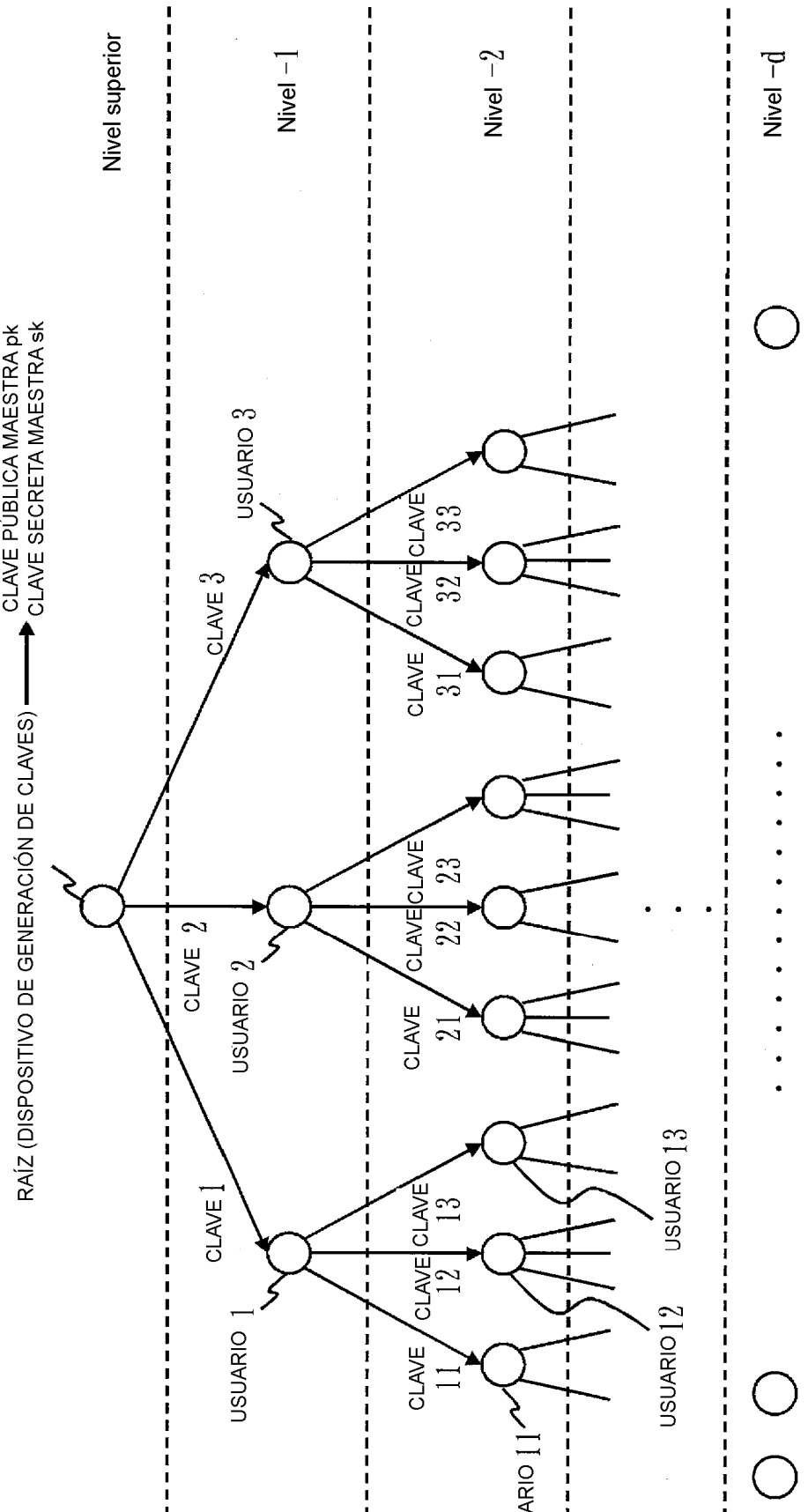

RAÍZ (DISPOSITIVO DE GENERACIÓN DE CLAVES)
CLAVE PÚBLICA MAESTRA pk
CLAVE SECRETA MAESTRA sk
Nivel superior
Nivel −1
Nivel −2
Nivel −d
CLAVE 1
CLAVE 2
CLAVE 3
USUARIO 1
USUARIO 2
USUARIO 3
CLAVE 11
CLAVE 12
CLAVE 13
CLAVE 21
CLAVE 22
CLAVE 23
CLAVE 31
CLAVE 32
CLAVE 33
USUARIO 11
USUARIO 12
USUARIO 13

Fig. 2

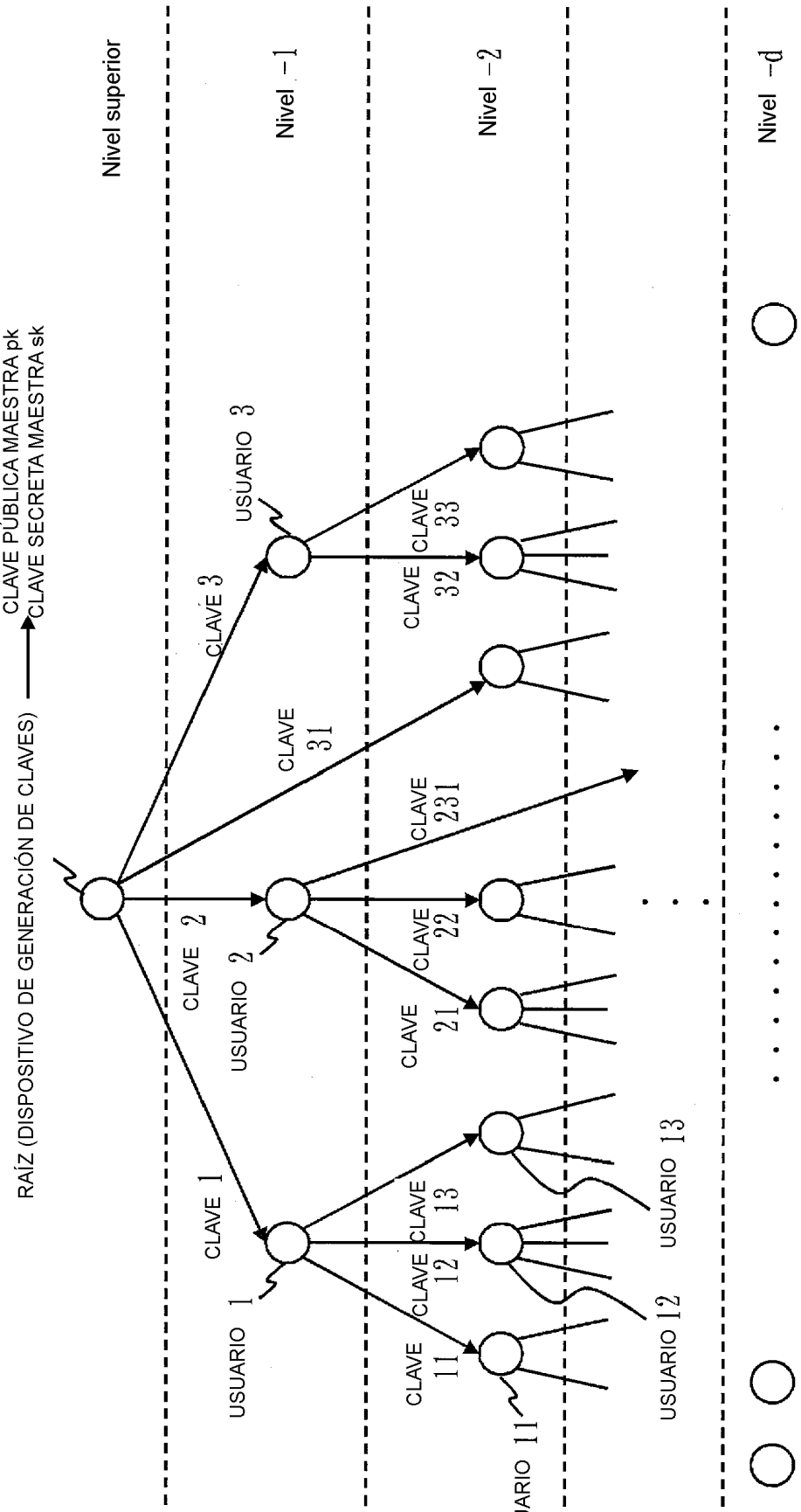

RAÍZ (DISPOSITIVO DE GENERACIÓN DE CLAVES)
CLAVE PÚBLICA MAESTRA pk
CLAVE SECRETA MAESTRA sk
Nivel superior
Nivel −1
Nivel −2
Nivel −d
CLAVE 1
CLAVE 2
CLAVE 3
USUARIO 1
USUARIO 2
USUARIO 3
CLAVE 11
CLAVE 12
CLAVE 13
CLAVE 21
CLAVE 22
CLAVE 31
CLAVE 231
CLAVE 32
CLAVE 33
USUARIO 11
USUARIO 12
USUARIO 13

Fig. 3

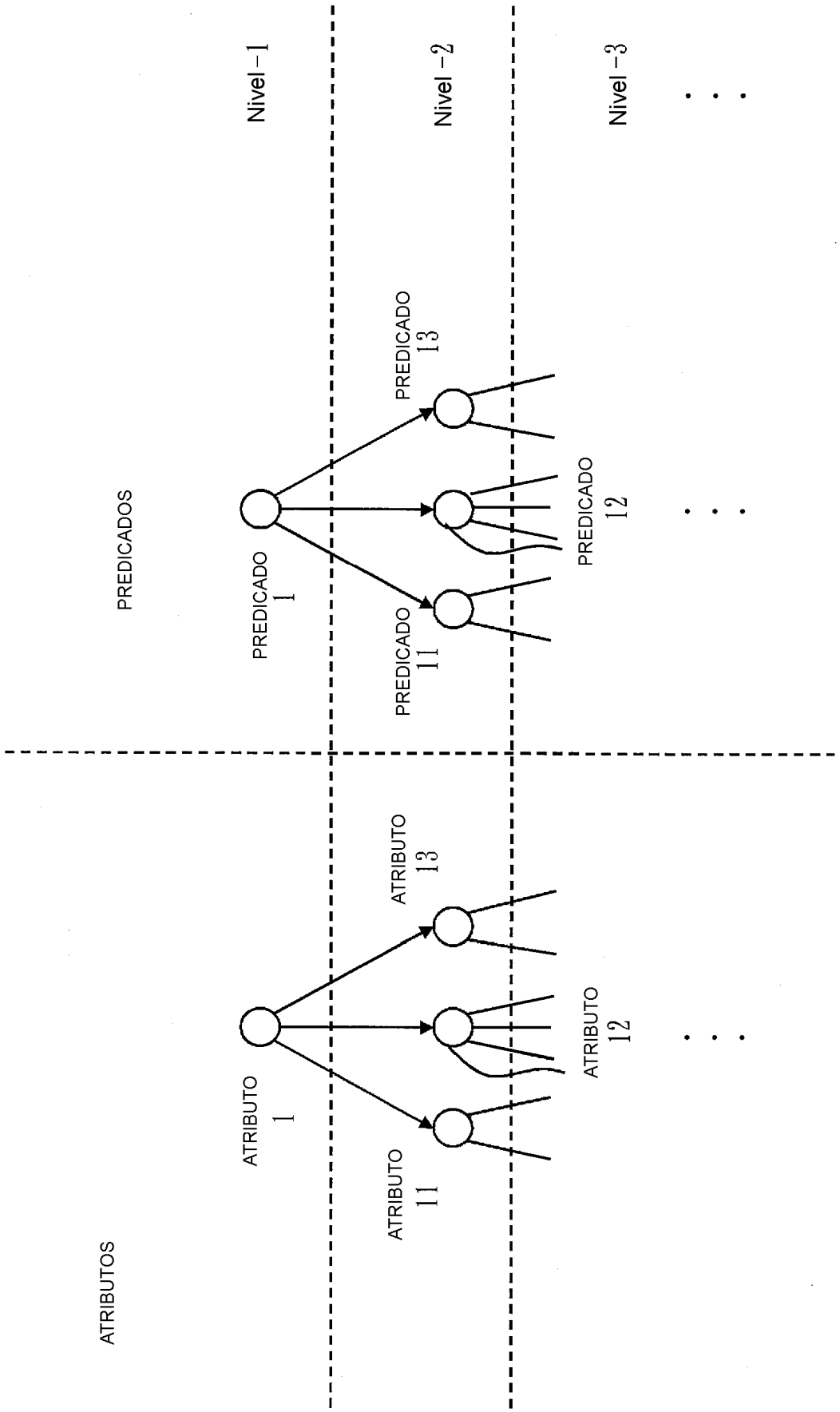

Nivel −1
Nivel −2
Nivel −3
PREDICADOS
ATRIBUTOS
PREDICADO 1
PREDICADO 11
PREDICADO 13
PREDICADO 12
ATRIBUTO 1
ATRIBUTO 11
ATRIBUTO 13
ATRIBUTO 12

Fig. 4

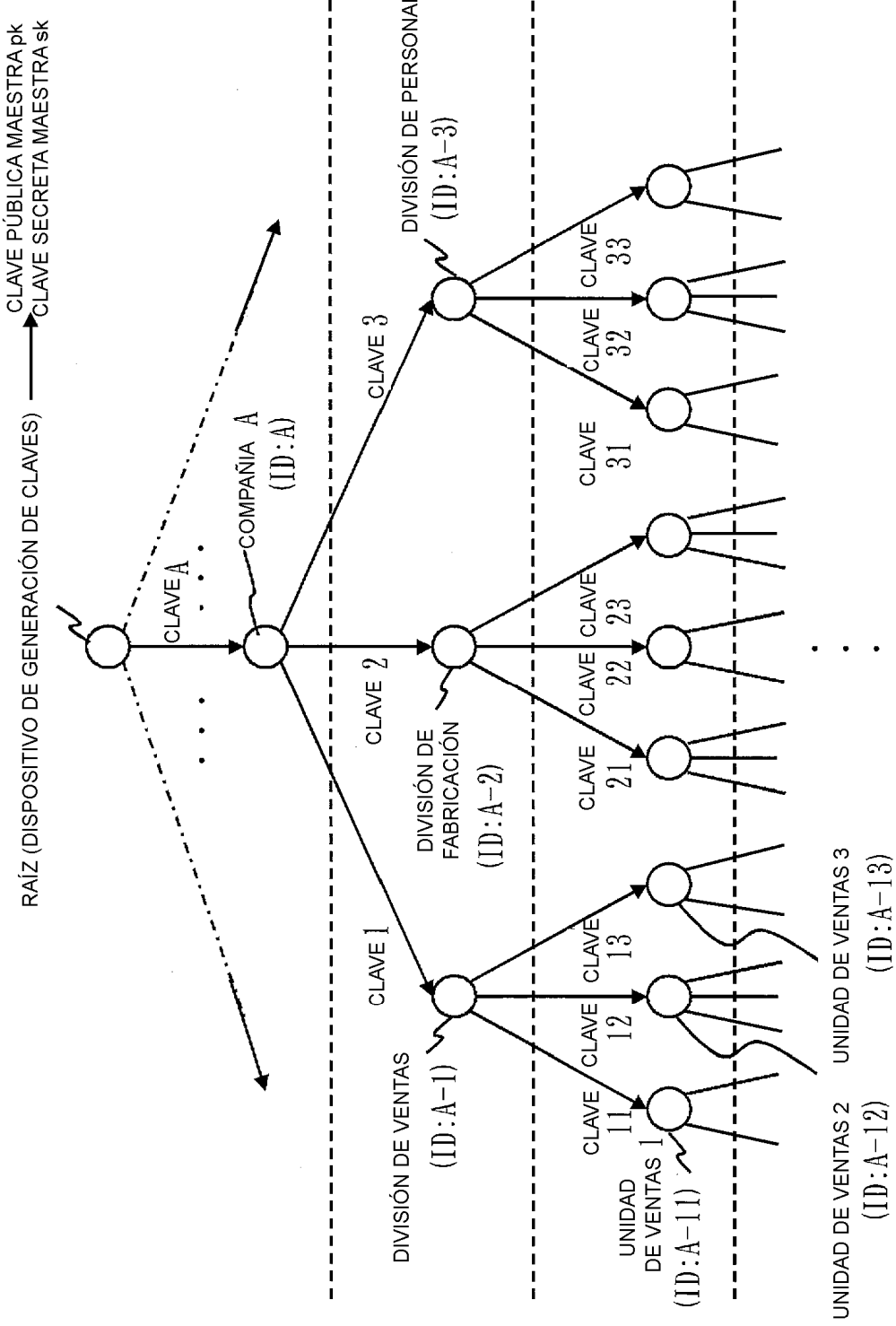

RAÍZ (DISPOSITIVO DE GENERACIÓN DE CLAVES)
CLAVE PÚBLICA MAESTRA pk
CLAVE SECRETA MAESTRA sk
Nivel superior
Nivel −1
Nivel −2
CLAVE A
COMPAÑIA A
(ID:A)
CLAVE 1
CLAVE 2
CLAVE 3
DIVISIÓN DE VENTAS
(ID:A−1)
DIVISIÓN DE FABRICACIÓN
(ID:A−2)
DIVISIÓN DE PERSONAL
(ID:A−3)
CLAVE 11
CLAVE 12
CLAVE 13
CLAVE 21
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

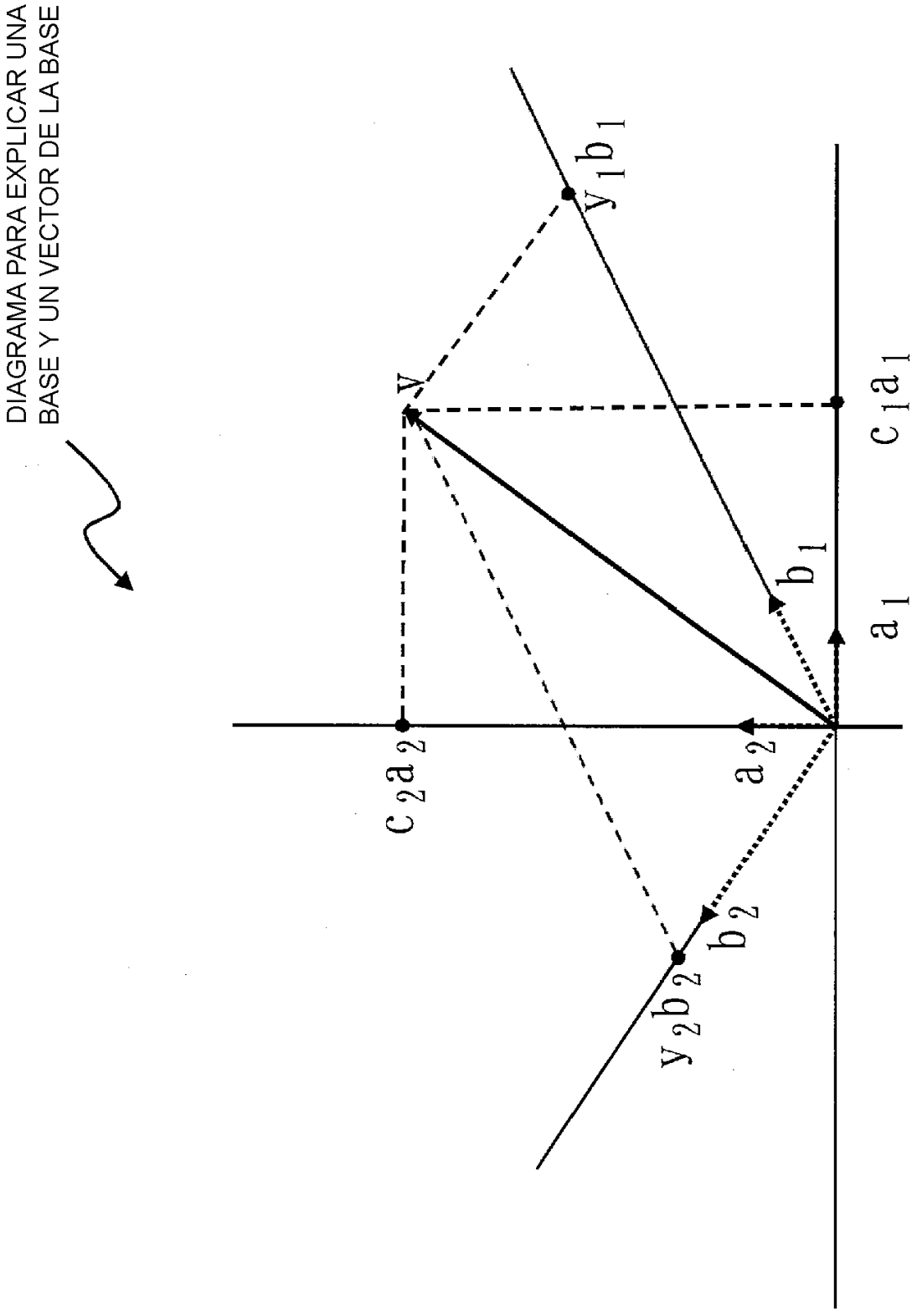


DIAGRAMA PARA EXPLICAR UNA BASE Y UN VECTOR DE LA BASE
v
y1b1
b1
c1a1
a1
c2a2
a2
b2
y2b2

Fig. 6

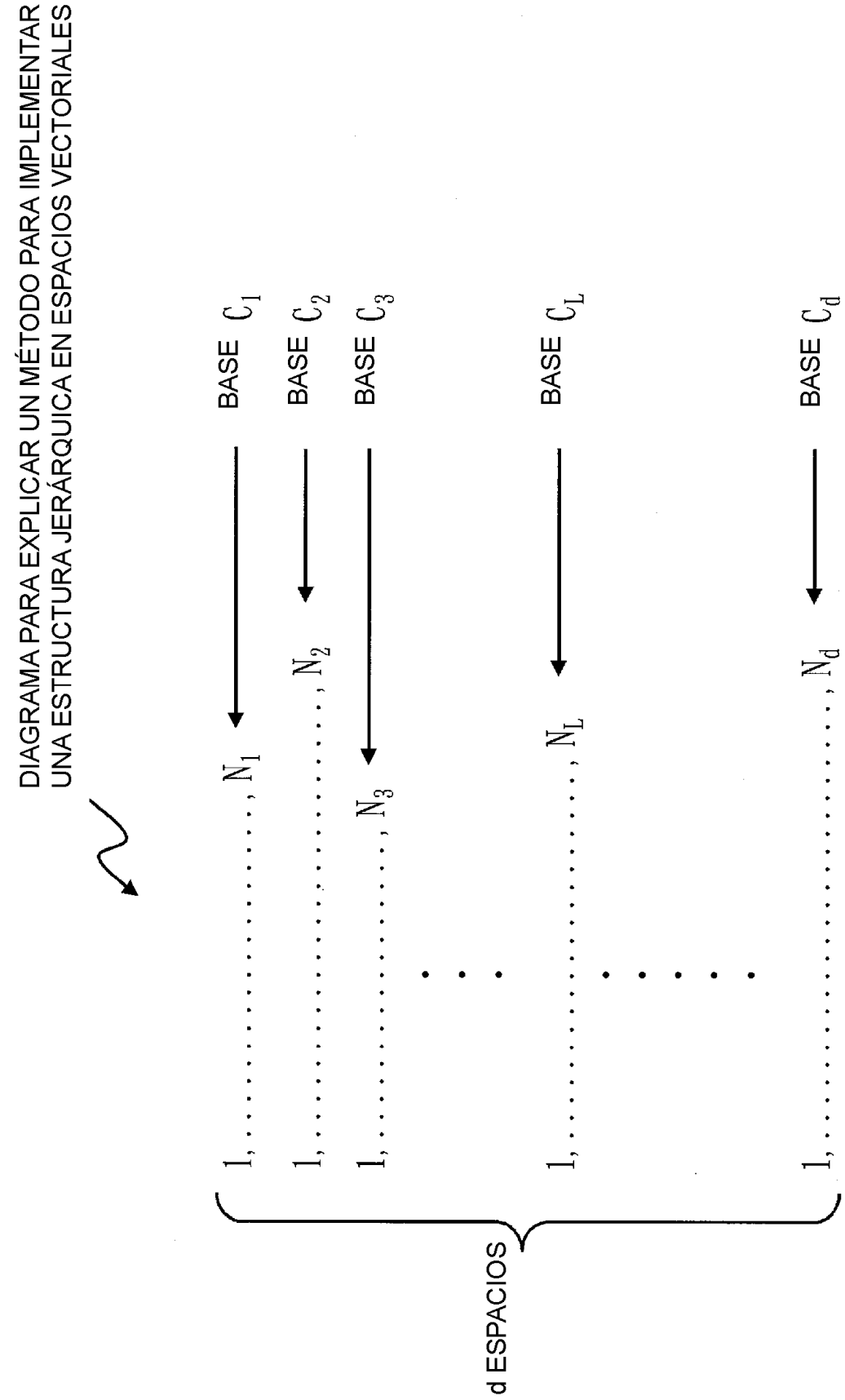


DIAGRAMA PARA EXPLICAR UN MÉTODO PARA IMPLEMENTAR UNA ESTRUCTURA JERÁRQUICA EN ESPACIOS VECTORIALES
BASE C_1
BASE C_2
BASE C_3
BASE C_L
BASE C_d
1, ..., N_1
1, ..., N_2
1, ..., N_3
1, ..., N_L
1, ..., N_d
d ESPACIOS

Fig. 7

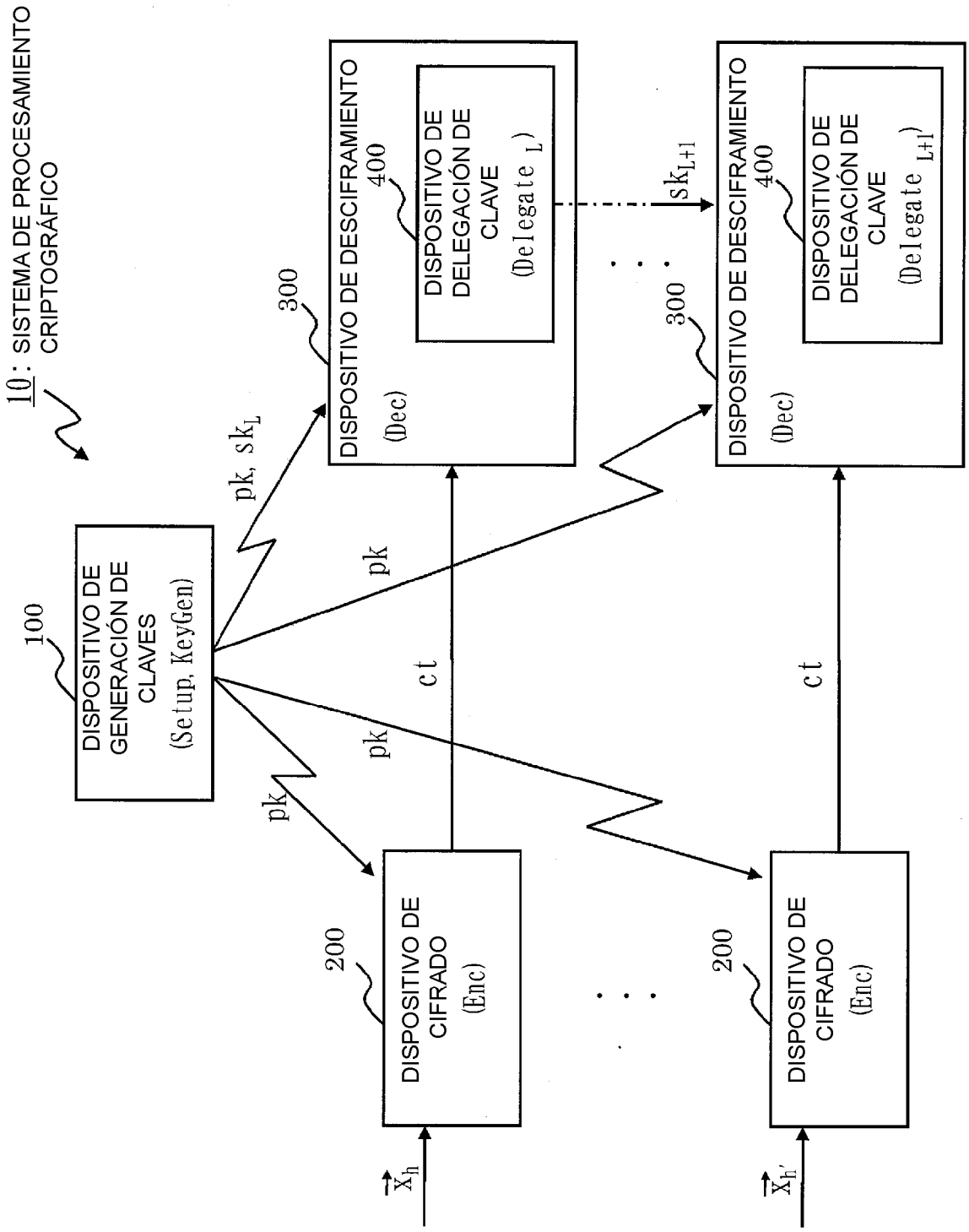

10: SISTEMA DE PROCESAMIENTO CRIPTOGRÁFICO
100
DISPOSITIVO DE GENERACIÓN DE CLAVES (Setup, KeyGen)
pk, sk_L
300
DISPOSITIVO DE DESCIFRAMIENTO (Dec)
400
DISPOSITIVO DE DELEGACIÓN DE CLAVE (Delegate_L)
sk_{L+1}
300
DISPOSITIVO DE DESCIFRAMIENTO (Dec)
400
DISPOSITIVO DE DELEGACIÓN DE CLAVE (Delegate_{L+1})
pk
pk
pk
ct
ct
200
DISPOSITIVO DE CIFRADO (Enc)
200
DISPOSITIVO DE CIFRADO (Enc)
x_h
x_{h'}

Fig. 8

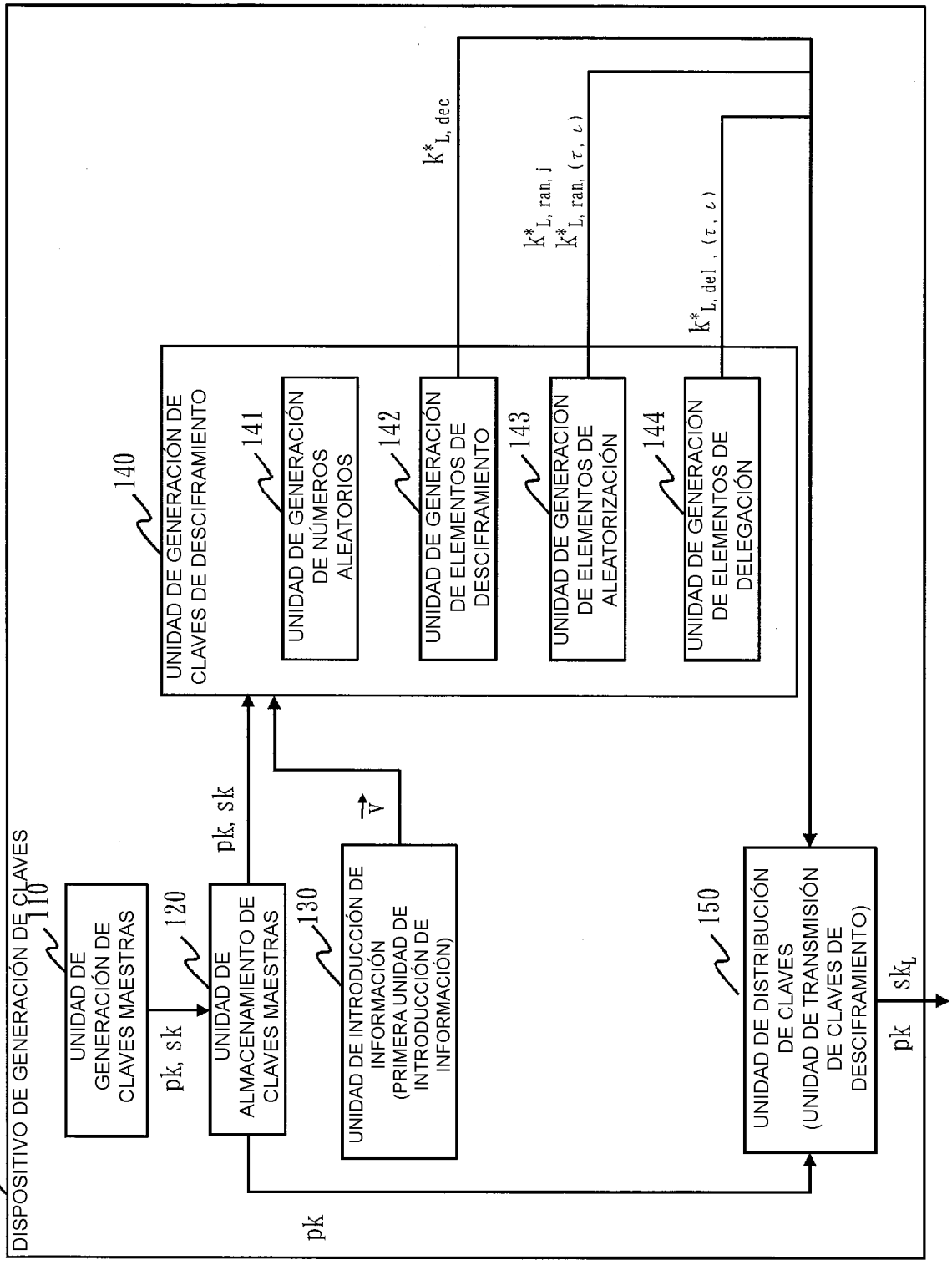

100
DISPOSITIVO DE GENERACIÓN DE CLAVES
110
UNIDAD DE GENERACIÓN DE CLAVES MAESTRAS
pk, sk
120
UNIDAD DE ALMACENAMIENTO DE CLAVES MAESTRAS
pk, sk
130
UNIDAD DE INTRODUCCIÓN DE INFORMACIÓN (PRIMERA UNIDAD DE INTRODUCCIÓN DE INFORMACIÓN)
v
140
UNIDAD DE GENERACIÓN DE CLAVES DE DESCIFRAMIENTO
141
UNIDAD DE GENERACIÓN DE NÚMEROS ALEATORIOS
142
UNIDAD DE GENERACIÓN DE ELEMENTOS DE DESCIFRAMIENTO
143
UNIDAD DE GENERACIÓN DE ELEMENTOS DE ALEATORIZACIÓN
144
UNIDAD DE GENERACIÓN DE ELEMENTOS DE DELEGACIÓN
$k^*_{L, dec}$
$k^*_{L, ran, j}$
$k^*_{L, ran, (\tau, \iota)}$
$k^*_{L, del, (\tau, \iota)}$
150
UNIDAD DE DISTRIBUCIÓN DE CLAVES (UNIDAD DE TRANSMISIÓN DE CLAVES DE DESCIFRAMIENTO)
pk
sk_L
pk

Fig. 9

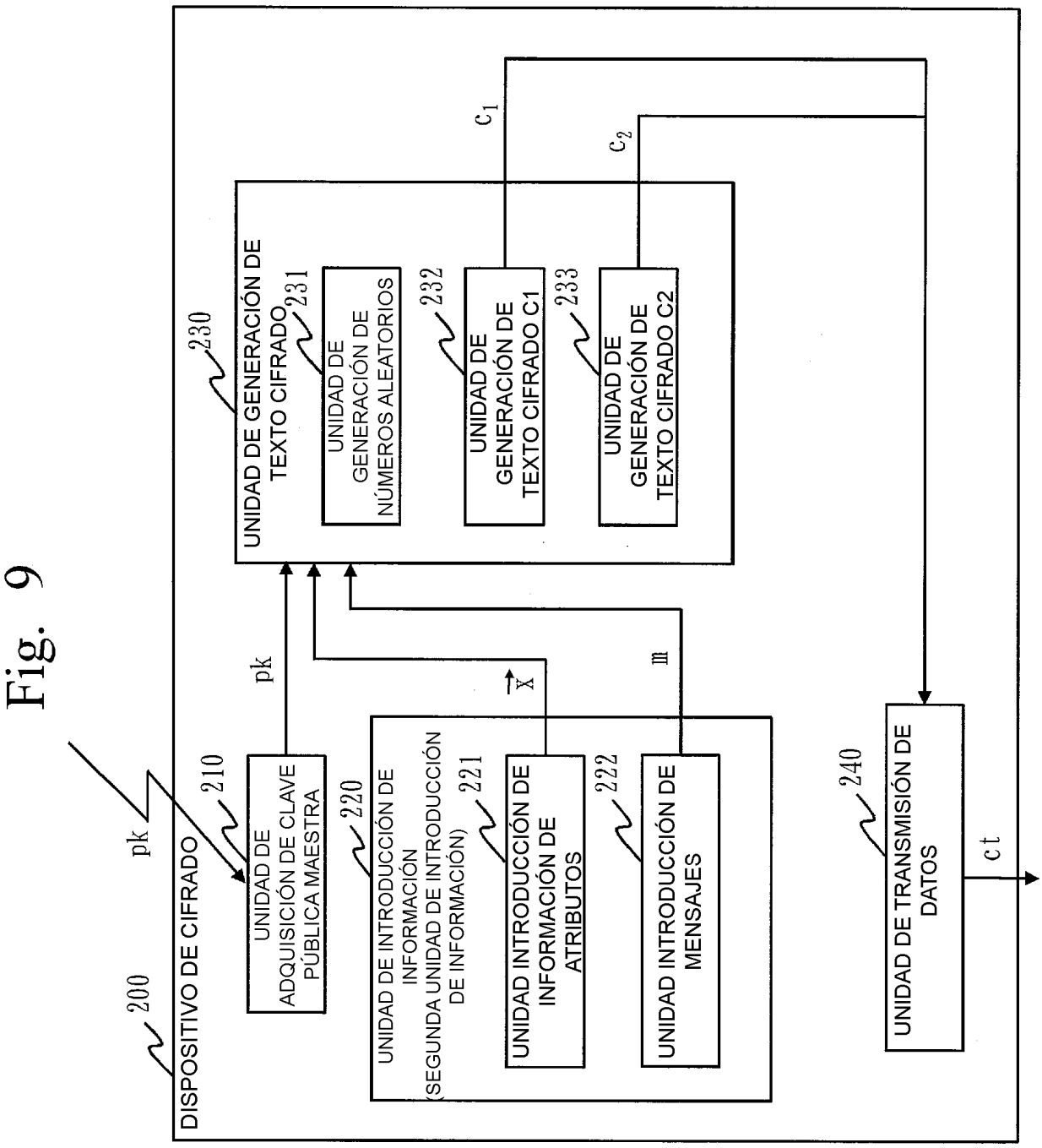

DISPOSITIVO DE CIFRADO
200
pk
UNIDAD DE ADQUISICIÓN DE CLAVE PÚBLICA MAESTRA
210
pk
UNIDAD DE INTRODUCCIÓN DE INFORMACIÓN (SEGUNDA UNIDAD DE INTRODUCCIÓN DE INFORMACIÓN)
220
UNIDAD INTRODUCCIÓN DE INFORMACIÓN DE ATRIBUTOS
221
X
UNIDAD INTRODUCCIÓN DE MENSAJES
222
m
UNIDAD DE GENERACIÓN DE TEXTO CIFRADO
230
UNIDAD DE GENERACIÓN DE NÚMEROS ALEATORIOS
231
UNIDAD DE GENERACIÓN DE TEXTO CIFRADO C1
232
UNIDAD DE GENERACIÓN DE TEXTO CIFRADO C2
233
c1
c2
UNIDAD DE TRANSMISIÓN DE DATOS
240
ct

Fig. 10

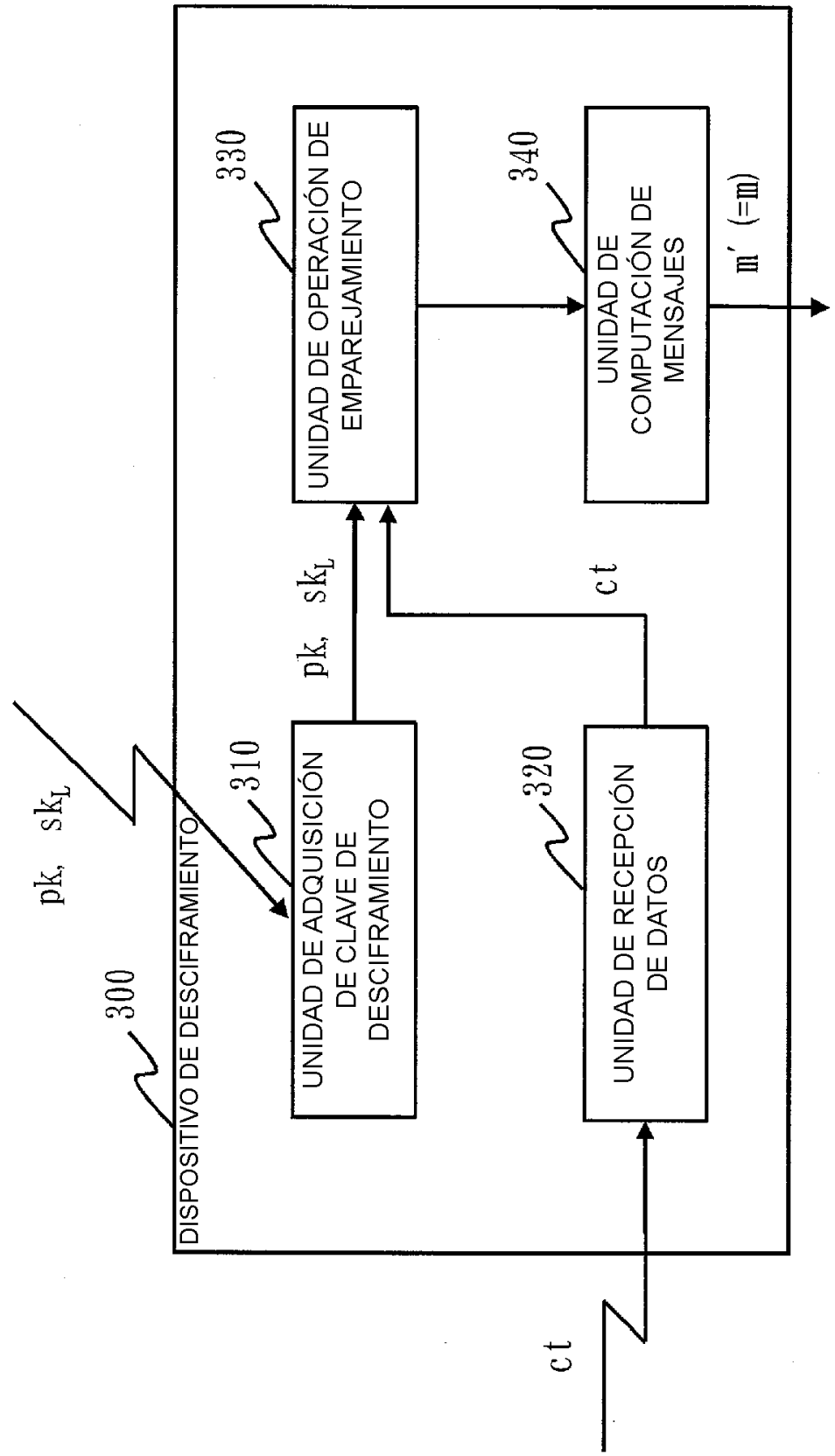

DISPOSITIVO DE DESCIFRAMIENTO
300
pk, sk_L
UNIDAD DE ADQUISICIÓN DE CLAVE DE DESCIFRAMIENTO
310
UNIDAD DE RECEPCIÓN DE DATOS
320
UNIDAD DE OPERACIÓN DE EMPAREJAMIENTO
330
UNIDAD DE COMPUTACIÓN DE MENSAJES
340
pk, sk_L
ct
ct
m' (=m)

Fig. 11

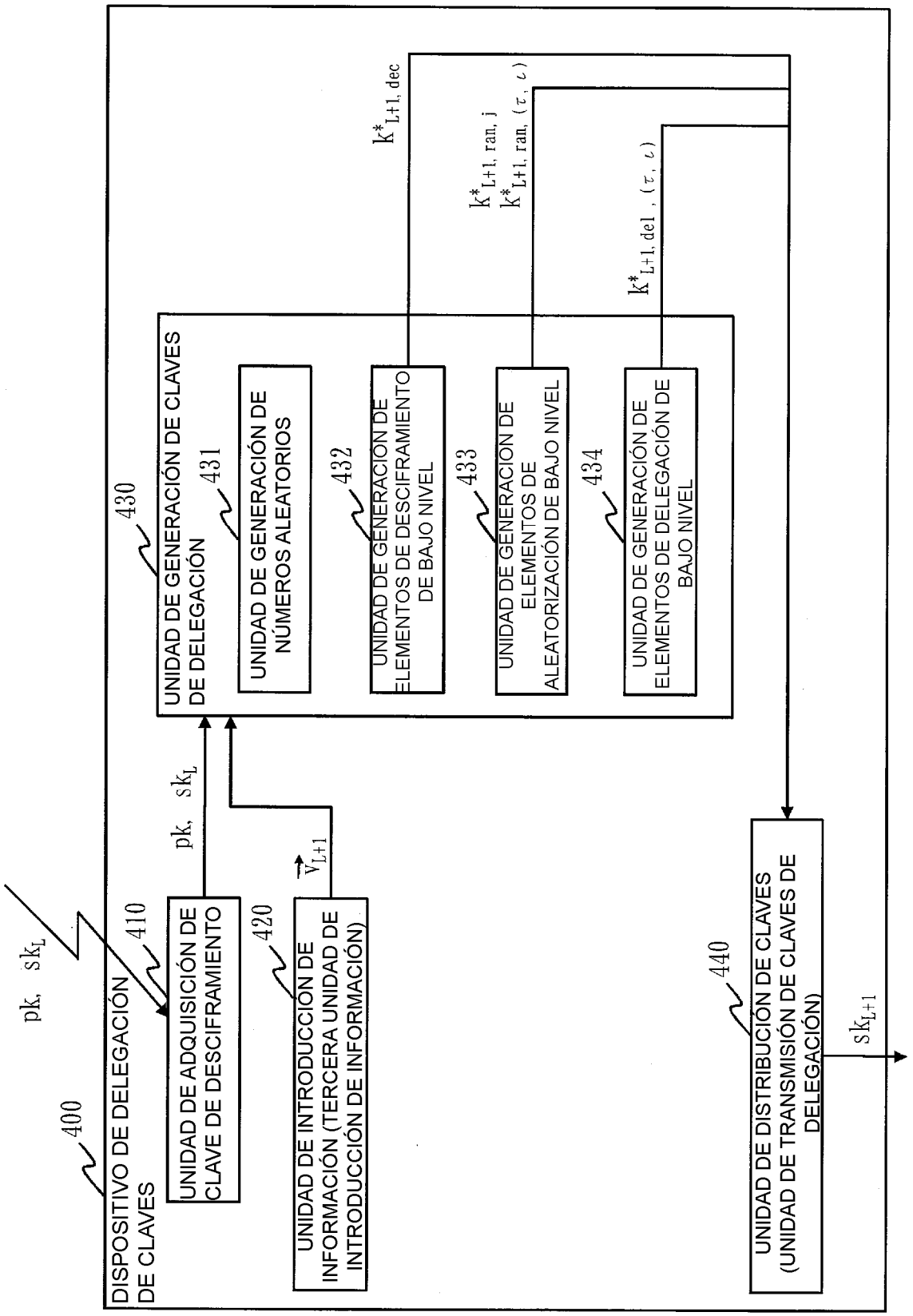

DISPOSITIVO DE DELEGACIÓN DE CLAVES
400
pk, sk_L
UNIDAD DE ADQUISICIÓN DE CLAVE DE DESCIFRAMIENTO
410
pk, sk_L
UNIDAD DE INTRODUCCIÓN DE INFORMACIÓN (TERCERA UNIDAD DE INTRODUCCIÓN DE INFORMACIÓN)
420
v_{L+1}
UNIDAD DE GENERACIÓN DE CLAVES DE DELEGACIÓN
430
UNIDAD DE GENERACIÓN DE NÚMEROS ALEATORIOS
431
UNIDAD DE GENERACIÓN DE ELEMENTOS DE DESCIFRAMIENTO DE BAJO NIVEL
432
UNIDAD DE GENERACIÓN DE ELEMENTOS DE ALEATORIZACIÓN DE BAJO NIVEL
433
UNIDAD DE GENERACIÓN DE ELEMENTOS DE DELEGACIÓN DE BAJO NIVEL
434
$k^*_{L+1, dec}$
$k^*_{L+1, ran, j}$
$k^*_{L+1, ran, (\tau, \iota)}$
$k^*_{L+1, del, (\tau, \iota)}$
UNIDAD DE DISTRIBUCIÓN DE CLAVES (UNIDAD DE TRANSMISIÓN DE CLAVES DE DELEGACIÓN)
440
sk_{L+1}

Fig. 12

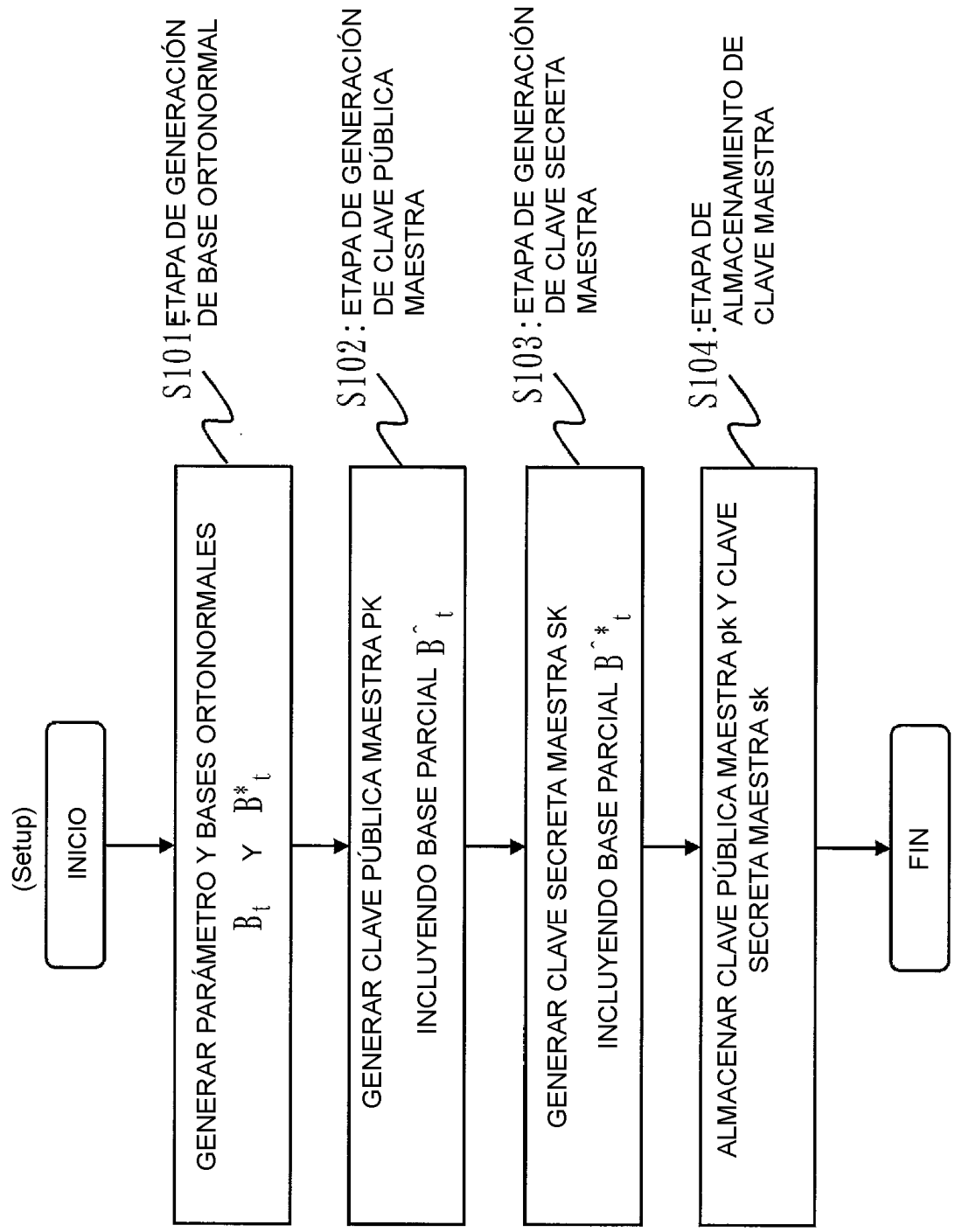

(Setup)
INICIO
S101 ETAPA DE GENERACIÓN DE BASE ORTONORMAL
GENERAR PARÁMETRO Y BASES ORTONORMALES
B_t Y B^*_t
S102 : ETAPA DE GENERACIÓN DE CLAVE PÚBLICA MAESTRA
GENERAR CLAVE PÚBLICA MAESTRA PK
INCLUYENDO BASE PARCIAL $\hat{B}_t$
S103 : ETAPA DE GENERACIÓN DE CLAVE SECRETA MAESTRA
GENERAR CLAVE SECRETA MAESTRA SK
INCLUYENDO BASE PARCIAL $\hat{B}^*_t$
S104 : ETAPA DE ALMACENAMIENTO DE CLAVE MAESTRA
ALMACENAR CLAVE PÚBLICA MAESTRA pk Y CLAVE SECRETA MAESTRA sk
FIN

Fig. 13

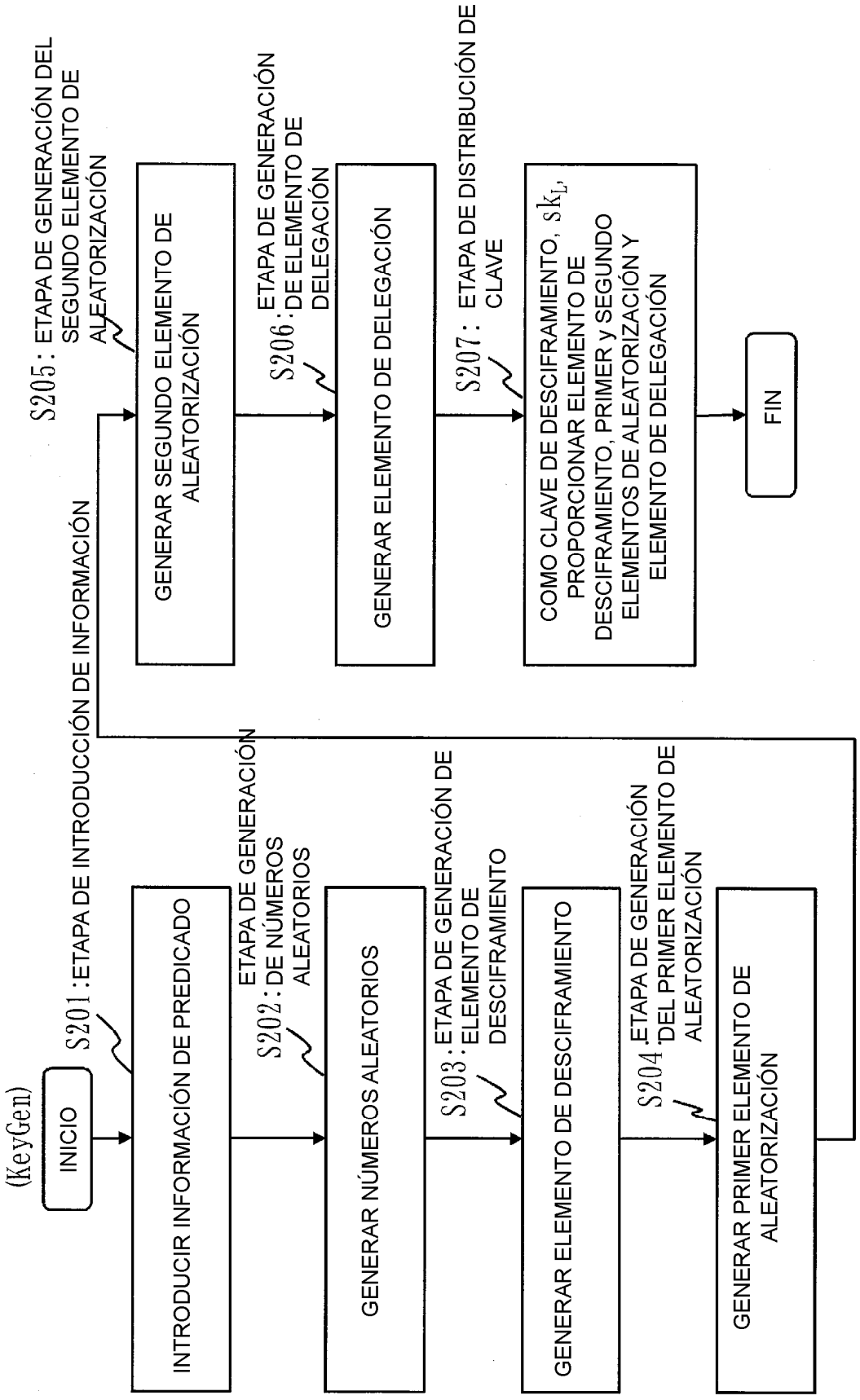

(KeyGen)
INICIO
S201 :ETAPA DE INTRODUCCIÓN DE INFORMACIÓN
INTRODUCIR INFORMACIÓN DE PREDICADO
S202 : ETAPA DE GENERACIÓN DE NÚMEROS ALEATORIOS
GENERAR NÚMEROS ALEATORIOS
S203 . ETAPA DE GENERACIÓN DE ELEMENTO DE DESCIFRAMIENTO
GENERAR ELEMENTO DE DESCIFRAMIENTO
S204 .ETAPA DE GENERACIÓN DEL PRIMER ELEMENTO DE ALEATORIZACIÓN
GENERAR PRIMER ELEMENTO DE ALEATORIZACIÓN
S205 : ETAPA DE GENERACIÓN DEL SEGUNDO ELEMENTO DE ALEATORIZACIÓN
GENERAR SEGUNDO ELEMENTO DE ALEATORIZACIÓN
S206 : ETAPA DE GENERACIÓN DE ELEMENTO DE DELEGACIÓN
GENERAR ELEMENTO DE DELEGACIÓN
S207 : ETAPA DE DISTRIBUCIÓN DE CLAVE
COMO CLAVE DE DESCIFRAMIENTO, sk_L, PROPORCIONAR ELEMENTO DE DESCIFRAMIENTO, PRIMER y SEGUNDO ELEMENTOS DE ALEATORIZACIÓN Y ELEMENTO DE DELEGACIÓN
FIN

Fig. 14

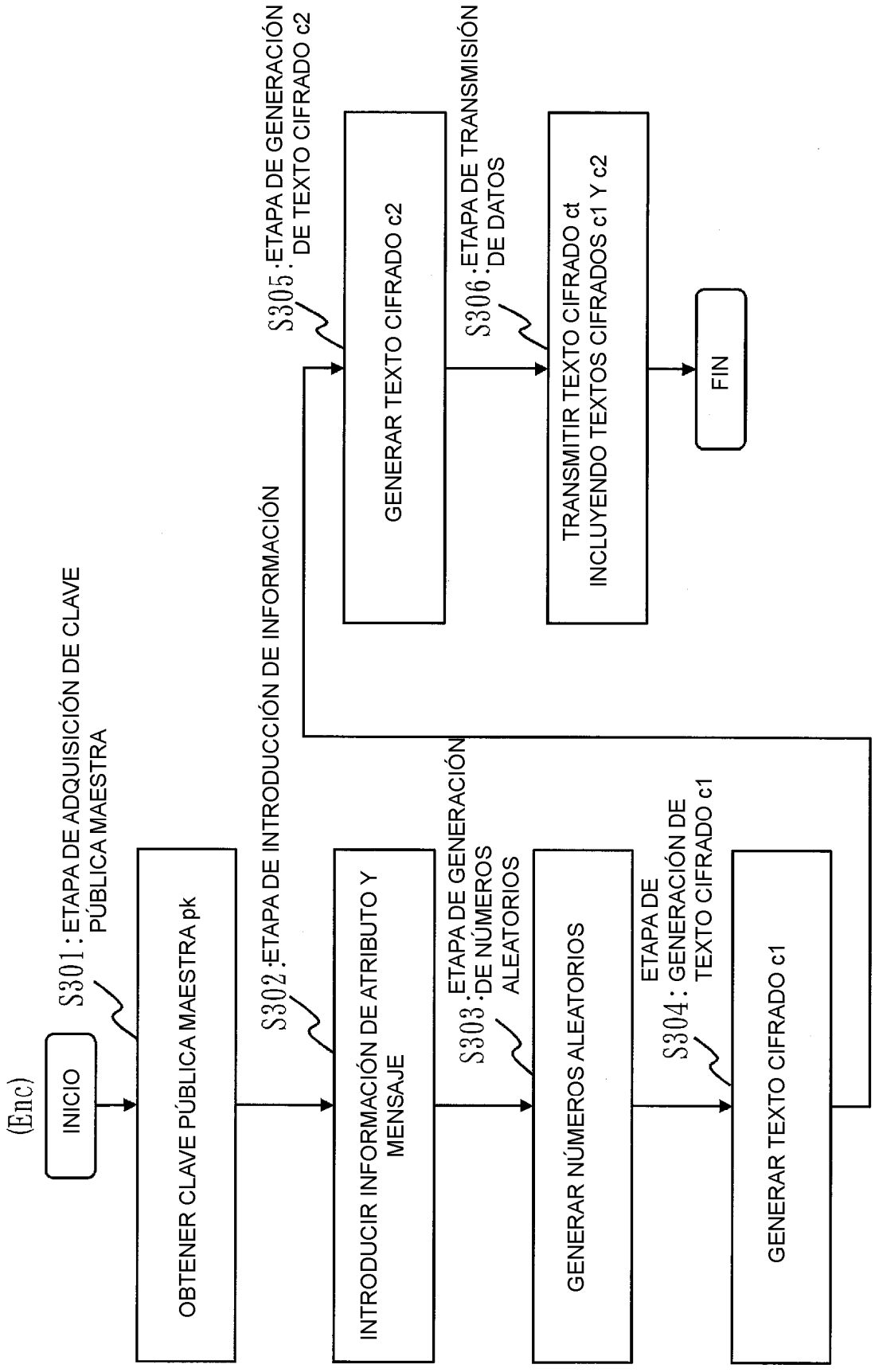

(Enc)
INICIO
S301 : ETAPA DE ADQUISICIÓN DE CLAVE PÚBLICA MAESTRA
OBTENER CLAVE PÚBLICA MAESTRA pk
S302 : ETAPA DE INTRODUCCIÓN DE INFORMACIÓN
INTRODUCIR INFORMACIÓN DE ATRIBUTO Y MENSAJE
S303 : ETAPA DE GENERACIÓN DE NÚMEROS ALEATORIOS
GENERAR NÚMEROS ALEATORIOS
S304 : ETAPA DE GENERACIÓN DE TEXTO CIFRADO c1
GENERAR TEXTO CIFRADO c1
S305 : ETAPA DE GENERACIÓN DE TEXTO CIFRADO c2
GENERAR TEXTO CIFRADO c2
S306 : ETAPA DE TRANSMISIÓN DE DATOS
TRANSMITIR TEXTO CIFRADO ct INCLUYENDO TEXTOS CIFRADOS c1 Y c2
FIN

Fig. 15

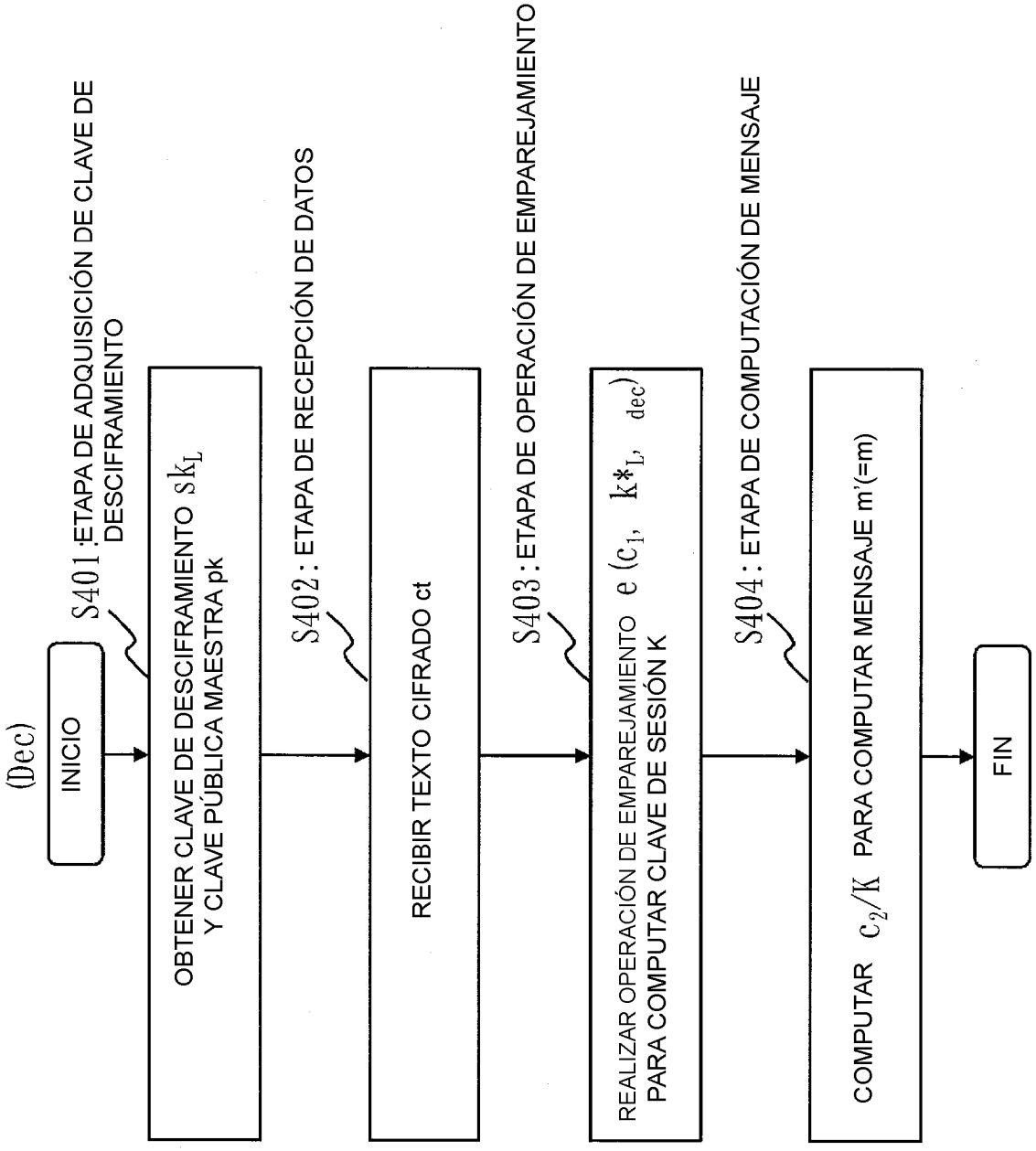

(Dec)
INICIO
S401 :ETAPA DE ADQUISICIÓN DE CLAVE DE DESCIFRAMIENTO
OBTENER CLAVE DE DESCIFRAMIENTO sk_L Y CLAVE PÚBLICA MAESTRA pk
S402 : ETAPA DE RECEPCIÓN DE DATOS
RECIBIR TEXTO CIFRADO ct
S403 : ETAPA DE OPERACIÓN DE EMPAREJAMIENTO
REALIZAR OPERACIÓN DE EMPAREJAMIENTO $e(c_1, k^*_{L, dec})$ PARA COMPUTAR CLAVE DE SESIÓN K
S404 : ETAPA DE COMPUTACIÓN DE MENSAJE
COMPUTAR c_2/K PARA COMPUTAR MENSAJE m'(=m)
FIN

Fig. 16

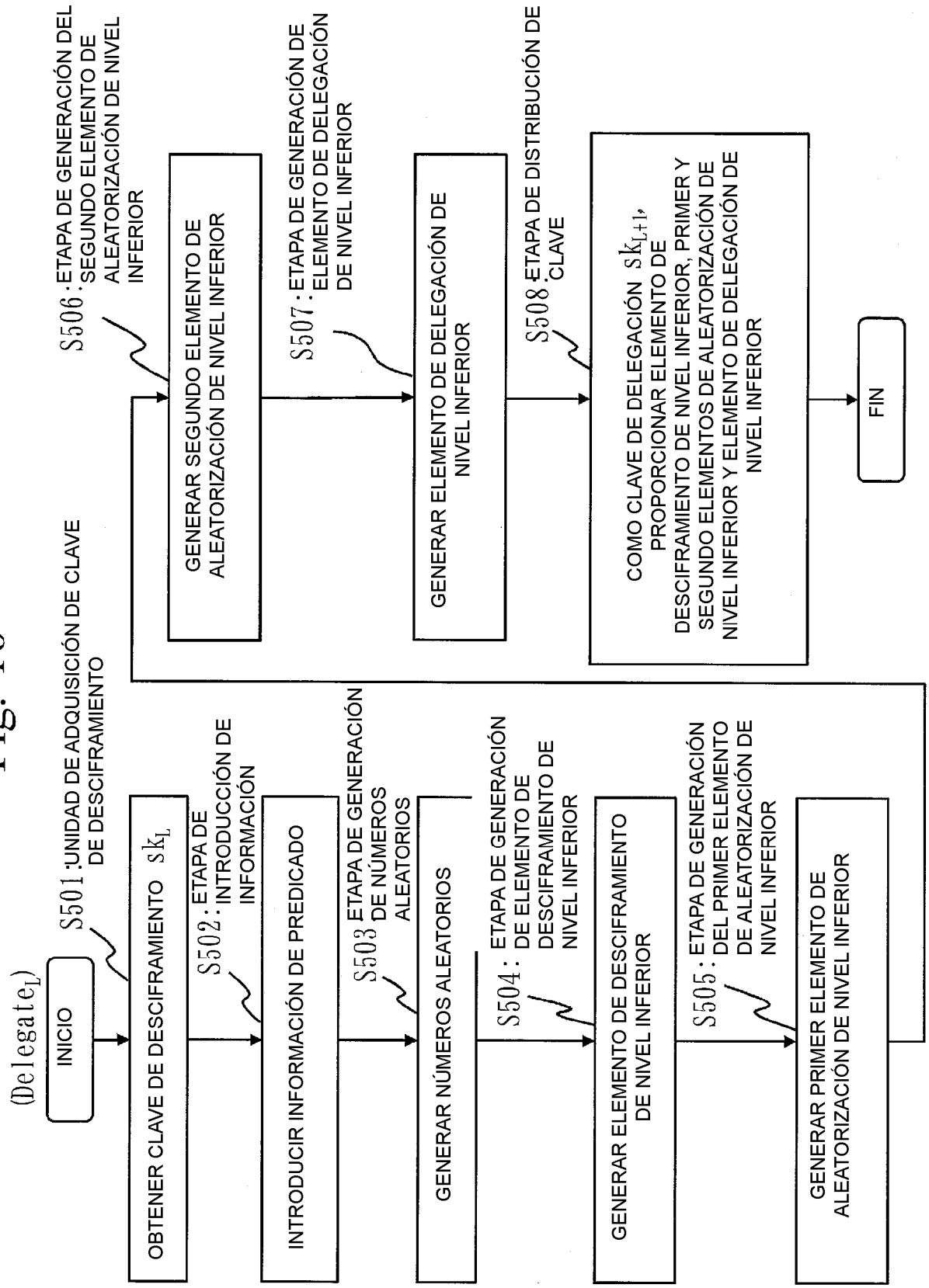

(Delegate$_L$)
INICIO
S501 : UNIDAD DE ADQUISICIÓN DE CLAVE DE DESCIFRAMIENTO
OBTENER CLAVE DE DESCIFRAMIENTO sk_L
S502 : ETAPA DE INTRODUCCIÓN DE INFORMACIÓN
INTRODUCIR INFORMACIÓN DE PREDICADO
S503 ETAPA DE GENERACIÓN DE NÚMEROS ALEATORIOS
GENERAR NÚMEROS ALEATORIOS
S504 : ETAPA DE GENERACIÓN DE ELEMENTO DE DESCIFRAMIENTO DE NIVEL INFERIOR
GENERAR ELEMENTO DE DESCIFRAMIENTO DE NIVEL INFERIOR
S505 : ETAPA DE GENERACIÓN DEL PRIMER ELEMENTO DE ALEATORIZACIÓN DE NIVEL INFERIOR
GENERAR PRIMER ELEMENTO DE ALEATORIZACIÓN DE NIVEL INFERIOR
S506 : ETAPA DE GENERACIÓN DEL SEGUNDO ELEMENTO DE ALEATORIZACIÓN DE NIVEL INFERIOR
GENERAR SEGUNDO ELEMENTO DE ALEATORIZACIÓN DE NIVEL INFERIOR
S507 : ETAPA DE GENERACIÓN DE ELEMENTO DE DELEGACIÓN DE NIVEL INFERIOR
GENERAR ELEMENTO DE DELEGACIÓN DE NIVEL INFERIOR
S508 ETAPA DE DISTRIBUCIÓN DE CLAVE
COMO CLAVE DE DELEGACIÓN sk_{L+1}, PROPORCIONAR ELEMENTO DE DESCIFRAMIENTO DE NIVEL INFERIOR, PRIMER Y SEGUNDO ELEMENTOS DE ALEATORIZACIÓN DE NIVEL INFERIOR Y ELEMENTO DE DELEGACIÓN DE NIVEL INFERIOR
FIN

Fig. 17

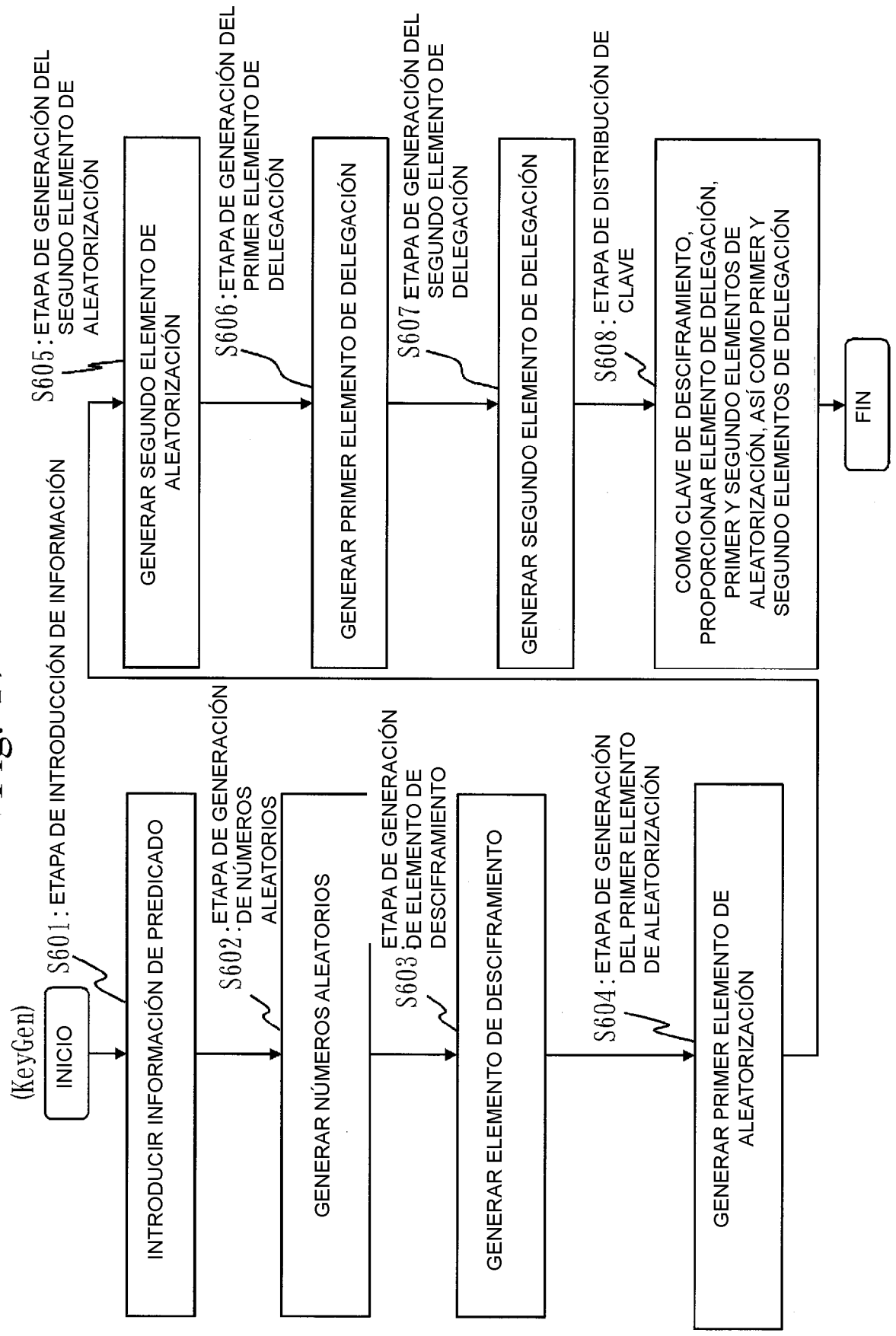

(KeyGen)
INICIO
S601 : ETAPA DE INTRODUCCIÓN DE INFORMACIÓN
INTRODUCIR INFORMACIÓN DE PREDICADO
S602 : ETAPA DE GENERACIÓN DE NÚMEROS ALEATORIOS
GENERAR NÚMEROS ALEATORIOS
S603 : ETAPA DE GENERACIÓN DE ELEMENTO DE DESCIFRAMIENTO
GENERAR ELEMENTO DE DESCIFRAMIENTO
S604 : ETAPA DE GENERACIÓN DEL PRIMER ELEMENTO DE ALEATORIZACIÓN
GENERAR PRIMER ELEMENTO DE ALEATORIZACIÓN
S605 : ETAPA DE GENERACIÓN DEL SEGUNDO ELEMENTO DE ALEATORIZACIÓN
GENERAR SEGUNDO ELEMENTO DE ALEATORIZACIÓN
S606 : ETAPA DE GENERACIÓN DEL PRIMER ELEMENTO DE DELEGACIÓN
GENERAR PRIMER ELEMENTO DE DELEGACIÓN
S607 : ETAPA DE GENERACIÓN DEL SEGUNDO ELEMENTO DE DELEGACIÓN
GENERAR SEGUNDO ELEMENTO DE DELEGACIÓN
S608 : ETAPA DE DISTRIBUCIÓN DE CLAVE
COMO CLAVE DE DESCIFRAMIENTO, PROPORCIONAR ELEMENTO DE DELEGACIÓN, PRIMER Y SEGUNDO ELEMENTOS DE ALEATORIZACIÓN, ASÍ COMO PRIMER Y SEGUNDO ELEMENTOS DE DELEGACIÓN
FIN

Fig. 18

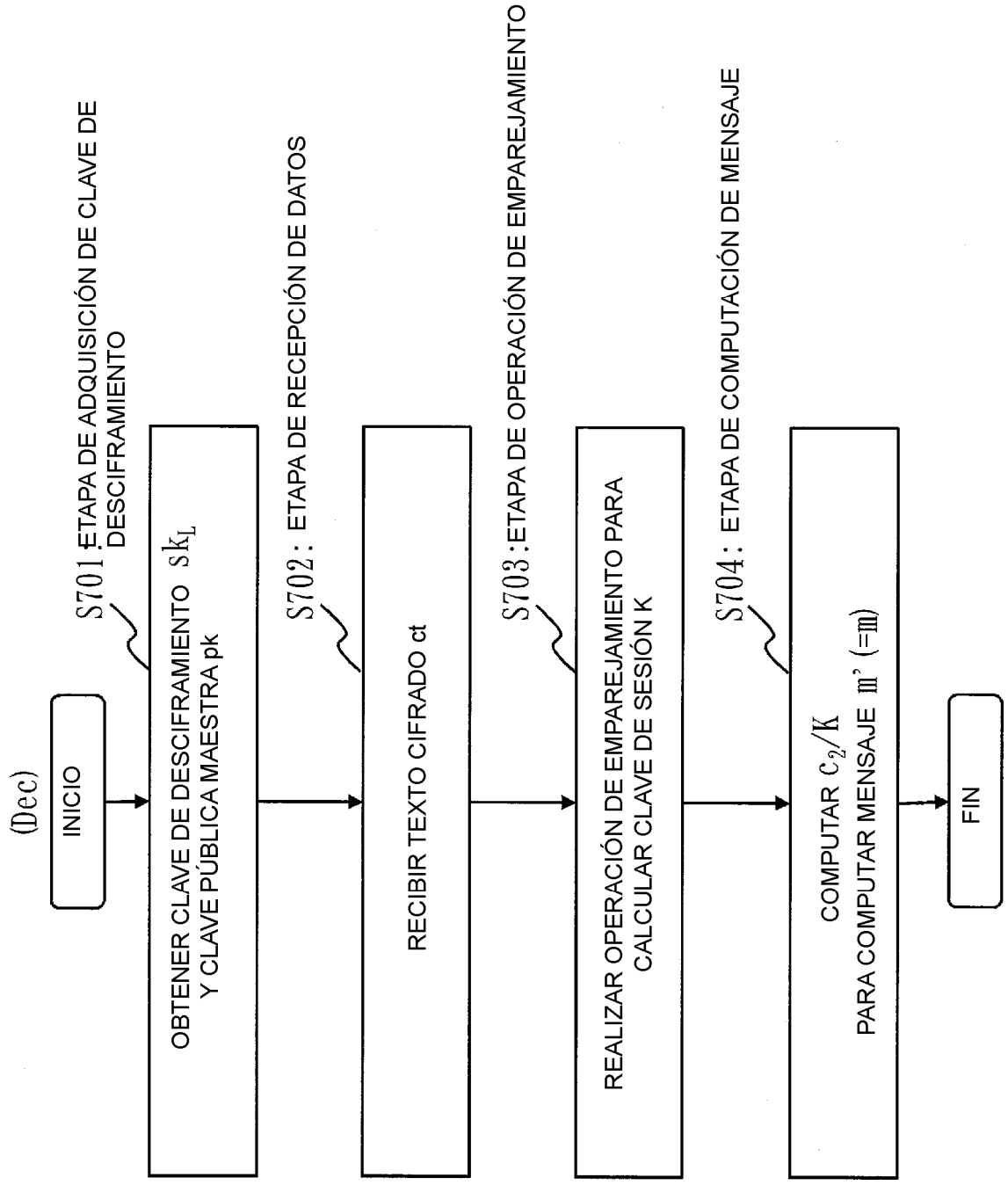

(Dec)
INICIO
S701 :ETAPA DE ADQUISICIÓN DE CLAVE DE DESCIFRAMIENTO
OBTENER CLAVE DE DESCIFRAMIENTO sk_L Y CLAVE PÚBLICA MAESTRA pk
S702 : ETAPA DE RECEPCIÓN DE DATOS
RECIBIR TEXTO CIFRADO ct
S703 :ETAPA DE OPERACIÓN DE EMPAREJAMIENTO
REALIZAR OPERACIÓN DE EMPAREJAMIENTO PARA CALCULAR CLAVE DE SESIÓN K
S704 : ETAPA DE COMPUTACIÓN DE MENSAJE
COMPUTAR c_2/K PARA COMPUTAR MENSAJE m' (=m)
FIN

Fig. 19

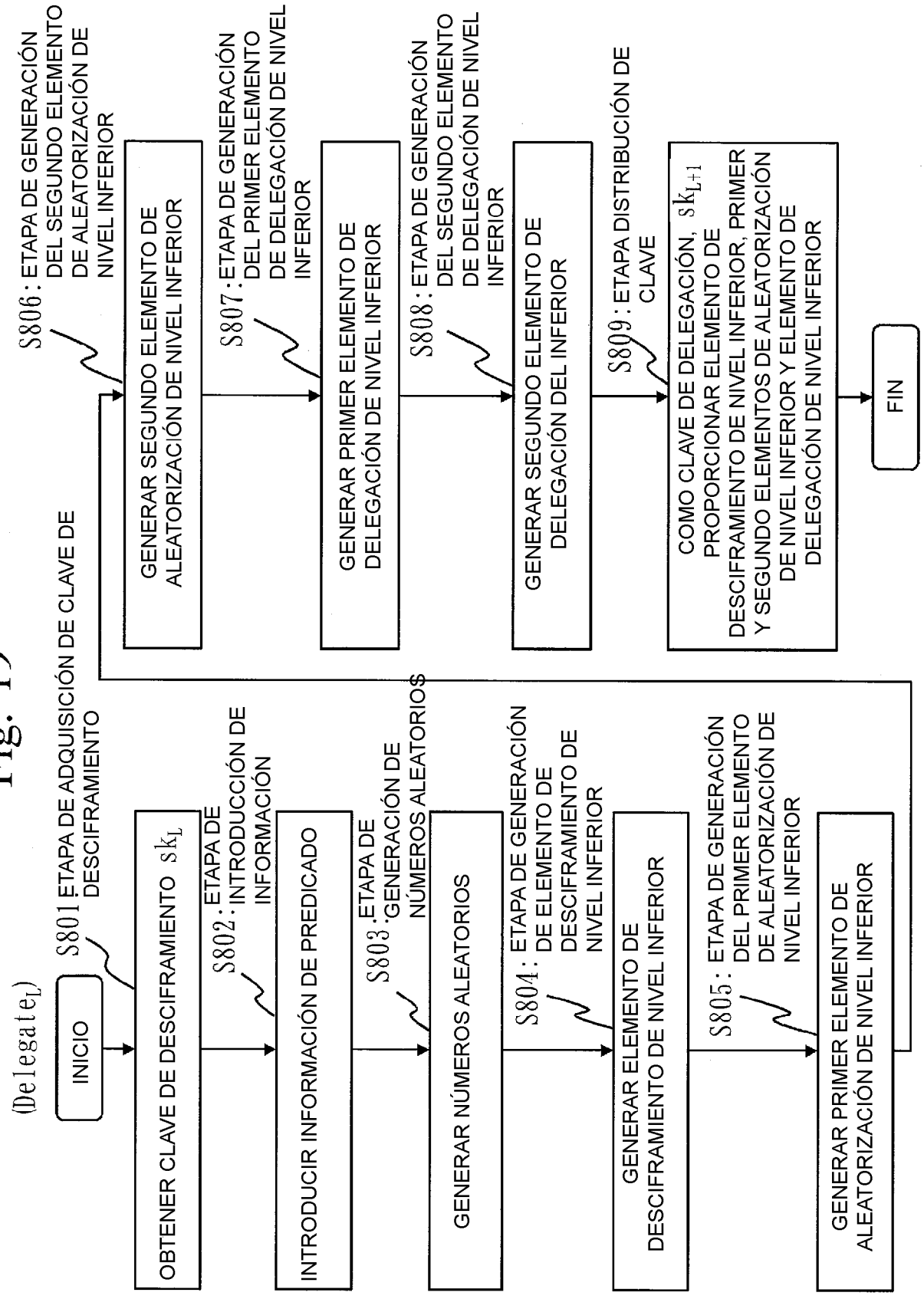
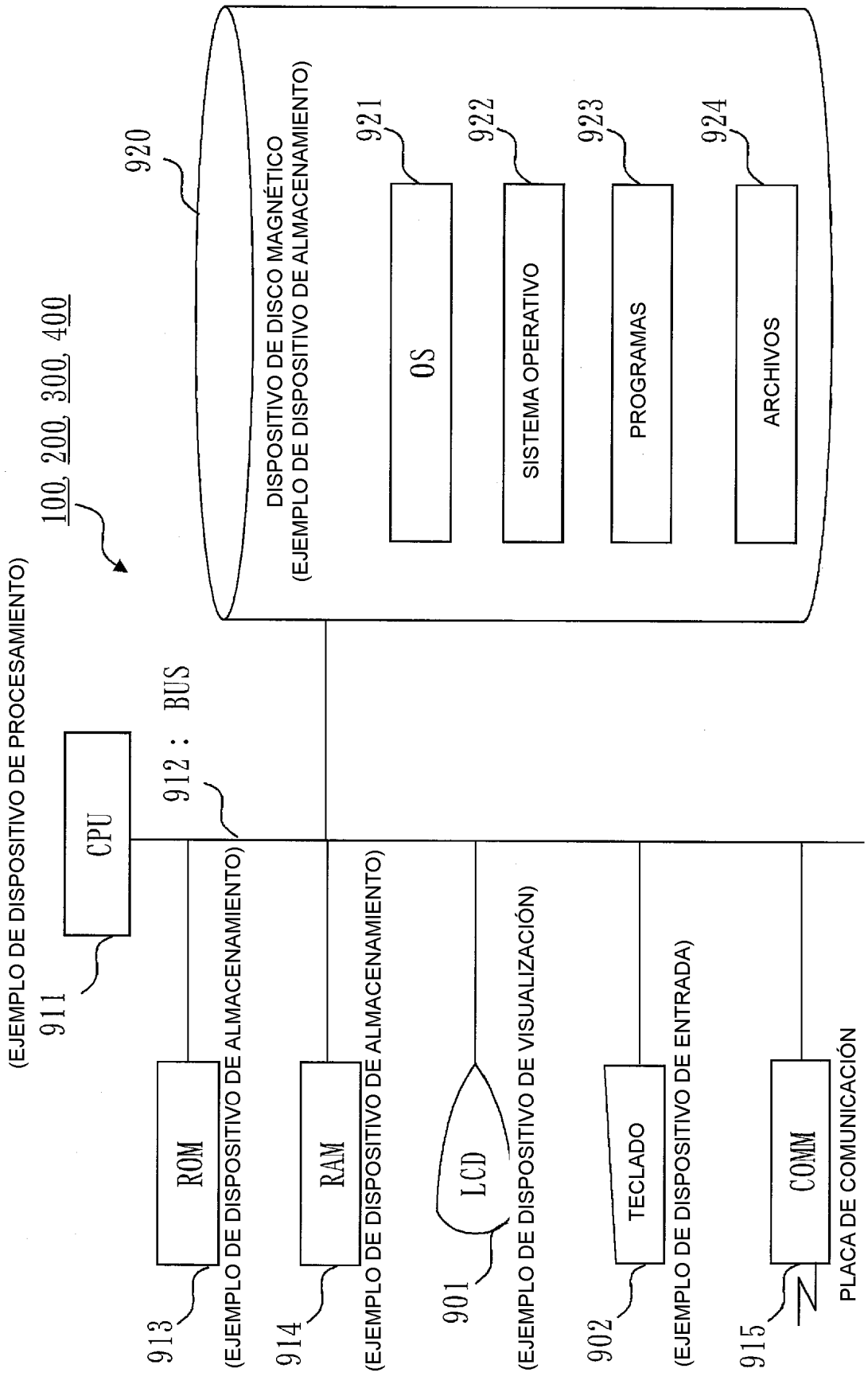

(Delegate_L)
INICIO
S801 ETAPA DE ADQUISICIÓN DE CLAVE DE DESCIFRAMIENTO
OBTENER CLAVE DE DESCIFRAMIENTO sk_L
S802: ETAPA DE INTRODUCCIÓN DE INFORMACIÓN
INTRODUCIR INFORMACIÓN DE PREDICADO
S803: ETAPA DE GENERACIÓN DE NÚMEROS ALEATORIOS
GENERAR NÚMEROS ALEATORIOS
S804: ETAPA DE GENERACIÓN DE ELEMENTO DE DESCIFRAMIENTO DE NIVEL INFERIOR
GENERAR ELEMENTO DE DESCIFRAMIENTO DE NIVEL INFERIOR
S805: ETAPA DE GENERACIÓN DEL PRIMER ELEMENTO DE ALEATORIZACIÓN DE NIVEL INFERIOR
GENERAR PRIMER ELEMENTO DE ALEATORIZACIÓN DE NIVEL INFERIOR
S806: ETAPA DE GENERACIÓN DEL SEGUNDO ELEMENTO DE ALEATORIZACIÓN DE NIVEL INFERIOR
GENERAR SEGUNDO ELEMENTO DE ALEATORIZACIÓN DE NIVEL INFERIOR
S807: ETAPA DE GENERACIÓN DEL PRIMER ELEMENTO DE DELEGACIÓN DE NIVEL INFERIOR
GENERAR PRIMER ELEMENTO DE DELEGACIÓN DE NIVEL INFERIOR
S808: ETAPA DE GENERACIÓN DEL SEGUNDO ELEMENTO DE DELEGACIÓN DE NIVEL INFERIOR
GENERAR SEGUNDO ELEMENTO DE DELEGACIÓN DEL INFERIOR
S809: ETAPA DISTRIBUCIÓN DE CLAVE
COMO CLAVE DE DELEGACIÓN, sk_{L+1} PROPORCIONAR ELEMENTO DE DESCIFRAMIENTO DE NIVEL INFERIOR, PRIMER Y SEGUNDO ELEMENTOS DE ALEATORIZACIÓN DE NIVEL INFERIOR Y ELEMENTO DE DELEGACIÓN DE NIVEL INFERIOR
FIN

Fig. 20


100, 200, 300, 400
920
DISPOSITIVO DE DISCO MAGNÉTICO
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
921
OS
922
SISTEMA OPERATIVO
923
PROGRAMAS
924
ARCHIVOS
(EJEMPLO DE DISPOSITIVO DE PROCESAMIENTO)
911
CPU
912 : BUS
913
ROM
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
914
RAM
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
901
LCD
(EJEMPLO DE DISPOSITIVO DE VISUALIZACIÓN)
902
TECLADO
(EJEMPLO DE DISPOSITIVO DE ENTRADA)
915
COMM
PLACA DE COMUNICACIÓN