(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 604 817**

(51) Int. CI.:

H04L 9/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.03.2013 PCT/JP2013/055661**

(87) Fecha y número de publicación internacional: **12.09.2013 WO13133158**

(96) Fecha de presentación y número de la solicitud europea: **01.03.2013 E 13757621 (1)**

(97) Fecha y número de publicación de la concesión europea: **19.10.2016 EP 2824652**

(54) Título: **Sistema de cifrado, método de cifrado y programa de cifrado**

(30) Prioridad:

06.03.2012 JP 2012049275

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.03.2017

(73) Titular/es:

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

(72) Inventor/es:

TAKASHIMA, KATSUYUKI y
OKAMOTO, TATSUAKI

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema de cifrado, método de cifrado y programa de cifrado

Campo técnico

La presente invención se refiere a un sistema criptográfico que permite adición de una categoría de atributo sin reeditar un parámetro público.

Antecedentes de la técnica

La Literatura no de Patente 29 describe un esquema de cifrado funcional.

Lista de referencias

Literatura no de Patente

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

Literatura no de Patente 2: Bethencourt, J., Sahai, A., Waters, B.: Ciphertex-policy attribute-based encryption. En: 2007 IEEE Symposium on Security and Privacy, páginas 321-334. IEEE Press (2007)

Literatura no de Patente 3: Boneh, D., Boyen, X.: Efficient selective-ID secure identity based encryption without random oracles. En: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, páginas 223-238. Springer Heidelberg (2004)

Literatura no de Patente 4: Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. En: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, páginas 443-459. Springer Heidelberg (2004)

Literatura no de Patente 5: Boneh, D., Boyen, X., Goh, E.: Hierarchical identity based encryption with constant size ciphertext. En: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, páginas 440-456. Springer Heidelberg (2005)

Literatura no de Patente 6: Boneh, D., Boyen, X., Shacham, H.: Short group signatures. En: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, páginas. 41-55. Springer, Heidelberg (2004)

Literatura no de Patente 7: Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. En: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, páginas. 213-229. Springer Heidelberg (2001)

Literatura no de Patente 8: Boneh, D., Hamburg, M.: Generalized identity based and broadcast encryption scheme. En: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, páginas 455-470. Springer Heidelberg (2008)

Literatura no de Patente 9: Boneh, D., Katz, J., Improved efficiency for CCA-secure cryptosystems built using identity based encryption. RSA-CT 2005, LNCS, Springer Verlag (2005)

Literatura no de Patente 10: Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. En: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, páginas 535-554. Springer Heidelberg (2007)

Literatura no de Patente 11: Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). En: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, páginas 290-307. Springer Heidelberg (2006)

Literatura no de Patente 12: Canetti, R., Halevi S., Katz J.: Chosen-ciphertext security from identity-based encryption. EUROCRYPT 2004, LNCS, Springer Heidelberg (2004)

Literatura no de Patente 13: Chase, M.: Multi-authority attribute based encryption. TCC. LNCS, páginas 515-534. Springer Heidelberg (2007).

Literatura no de Patente 14: Chase, M. and Chow, S.: Improving privacy and security in multi-authority attribute-based encryption. ACM Conference on Computer and Communications Security, páginas 121-130, ACM (2009).

Literatura no de Patente 15: Cocks, C.: An identity based encryption scheme based on quadratic residues. En: Honary, B. (ed.) IMA Int. Conf. LNCS, vol. 2260, páginas 360-363. Springer Heidelberg (2001)

Literatura no de Patente 16: Gentry, C.: Practical identity-based encryption without random oracles. En: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, páginas 445-464. Springer Heidelberg (2006)

Literatura no de Patente 17: Gentry, C., Halevi, S.: Hierarchical identity-based encryption with polynomially many levels. En: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, páginas 437-456. Springer Heidelberg (2009)

Literatura no de Patente 18: Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. En: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, páginas 548-566. Springer Heidelberg (2002)

Literatura no de Patente 19: Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. En: ACM Conference on Computer and Communication Security 2006, páginas 89-98, ACM (2006)

Literatura no de Patente 20: Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynominal equations and inner products. En: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, páginas 146-162. Springer Heidelberg (2008)

Literatura no de Patente 21: 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)

Literatura no de Patente 22: Lewko, A. B., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertext. En: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, páginas 455-479. Springer Heidelberg (2010)

Literatura no de Patente 23: Lewko, A. B., Waters, B.: Decentralizing Attribute-Based Encryption, las actas de Eurocrypt 2011. LNCS, Springer Heidelberg (2011).

Literatura no de Patente 24: Lewko, A. B., Waters, B.: Unbounded HIBE and attribute-based encryption, las actas de Eurocrypt 2011. LNCS, Springer Heidelberg (2011).

Literatura no de Patente 25: H. Lin, Z. Cao, X. Liang y J. Shao.: Secure threshold multi authority attribute based encryption without a central authority, INDOCRYPT, LNCS, vol. 5365, páginas 426-436, Springer Heidelberg (2008).

Literatura no de Patente 26: S. Müller, S. Katzenbeisser y C. Eckert.; On multi-authority ciphertext-policy attribute-based encryption, Bull. Korean Math Soc. 46, Nº 4, páginas 803-819 (2009).

Literatura no de Patente 27: Okamoto, T., Takashima, K.: Homomorphic encryption and signatures from vector decomposition. En: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, páginas 57-74. Springer Heidelberg (2008)

Literatura no de Patente 28: Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products, En: ASIACRYPT 2009, Springer Heidelberg (2009)

Literatura no de Patente 29: Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. En: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, páginas 191-208. Springer Heidelberg (2010). La versión completa está disponible en http://eprint.iacr.org/2010/563

Literatura no de Patente 30: Okamoto, T., Takashima, K.: Efficient attribute-based signatures for non-monotone predicates in the standard model. En: PKC 2011, Springer Heidelberg (2011)

Literatura no de Patente 31: Okamoto, T., Takashima, K.: Decentralized Attribute-Based Signatures http://eprint.iacr.org/2011/701

Literatura no de Patente 32: Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. En: ACM Conference on Computer and Communication Security 2007, páginas 195-203, ACM, (2007)

Literatura no de Patente 33: Pirretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure attribute-based systems. En: ACM Conference on Computer and Communication Security 2006, páginas 99-112, ACM, (2006)

Literatura no de Patente 34: Sahai, A., Waters, B.: Fuzzy identity-based encryption. En: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, páginas 457-473. Springer Heidelberg (2005)

Literatura no de Patente 35: Shi, E., Waters, B.: Delegating capability in predicate encryption systems. En: Aceto, L., Damgard, I., Goldberg, L.A., Halldorsson, M.M., Ingolfsdottir, A., Walukiewicz, I. (eds.) ICALP (2) 2008. LNCS, vol. 5126, páginas 560-578. Springer Heidelberg (2008)

Literatura no de Patente 36: Waters, B: Efficient identity based encryption without random oracles. Eurocrypt 2005, LNCS, vol. 3152, páginas 443-459. Springer Verlag (2005)

Literatura no de Patente 37: Waters, B: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. ePrint, IACR, http://eprint.iacr.org/2008/290

Literatura no de Patente 38: Waters, B: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. En: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, páginas 619-636. Springer Heidelberg (2009)

Compendio de la invención

Problema técnico

En el esquema de cifrado funcional descrito en la Literatura no de Patente 29, se requiere un par de una base B_t y una base B^*_t para cada categoría de atributo. Cuando va a ser añadida una categoría de atributo, necesita ser añadido un nuevo par de una base B_t y una base B^*_t. Esto hace necesario reeditar un parámetro público debido a que la base B_t se incluye en el parámetro público.

Es un objeto de la presente invención permitir la adición de una categoría de atributo sin reeditar un parámetro público.

Solución al problema

Un sistema criptográfico según la presente invención se configura para realizar un proceso usando una base B predeterminada y una base B* predeterminada y el sistema criptográfico incluye:

un dispositivo de transmisión configurado para generar un vector de transmisión lateral t_j para al menos un índice j de entre una pluralidad de índices j, el vector de transmisión lateral t_j que es un vector en el que información J asignada por adelantado al índice j se fija como un coeficiente de un vector de base predeterminado $b_{índice}$ de la base B y un parámetro Φ_j para el índice j se fija como un coeficiente de otro vector de base b_{att} de la base B; y

un dispositivo de recepción configurado para usar un vector de recepción lateral $r_{j'}$ para al menos un índice j' de entre una pluralidad de índices j', el vector de recepción lateral $r_{j'}$ que es un vector en el que información J' que tiene un producto interior de 0 con la información J asignada por adelantado al índice j que corresponde al índice j' se fija como un coeficiente de un vector de base $b^*_{índice}$ de la base B* que corresponde al vector de base $b_{índice}$ y un parámetro $\psi_{j'}$ para el índice j' se fija como un coeficiente de un vector de base b^*_{att} de la base B* que corresponde al vector de base b_{att} y calcula un producto de operaciones de emparejamiento sobre pares de los vectores de base correspondientes del vector de transmisión lateral t_j para el índice j y el vector de recepción lateral $r_{j'}$ para el índice j' que corresponde al índice j.

Efectos ventajosos de la invención

En un sistema criptográfico según la presente invención, información J que se asigna por adelantado al índice j se fija en un vector de transmisión lateral t_j e información J' que tiene un producto interior de 0 con la información J se fija en un vector de recepción lateral $r_{j'}$. Con esta disposición, una base B y una base B* se pueden usar comúnmente para todas las categorías de atributo con seguridad mantenida, eliminando de esta manera la necesidad de usar una base B_t y una base B^*_t para cada categoría. Como resultado, cuando va a ser añadida una categoría de atributo, no hay necesidad de generar nuevamente una base B_t y una base B^*_t, permitiendo de esta manera la adición de una categoría de atributo sin reeditar un parámetro público.

Breve descripción de los dibujos

La Fig. 1 es un dibujo explicativo de una matriz M^;

La Fig. 2 es un dibujo explicativo de una matriz M_{δ};

La Fig. 3 es un dibujo explicativo de s_0;

La Fig. 4 es un dibujo explicativo de $s^{\rightarrow T}$;

La Fig. 5 es un diagrama de configuración de un sistema criptográfico 10 que implementa un esquema KP-FE según la Realización 2;

La Fig. 6 es un diagrama de configuración de un dispositivo de generación de clave 100 según la Realización 2;

La Fig. 7 es un diagrama de configuración de un dispositivo de cifrado 200 según la Realización 2;

La Fig. 8 es un diagrama de configuración de un dispositivo de descifrado 300 según la Realización 2;

La Fig. 9 es un diagrama de flujo que ilustra el proceso de un algoritmo Setup según la Realización 2;

La Fig. 10 es un diagrama de flujo que ilustra el proceso de un algoritmo KeyGen según la Realización 2;

La Fig. 11 es un diagrama de flujo que ilustra el proceso de un algoritmo Enc según la Realización 2;

La Fig. 12 es un diagrama de flujo que ilustra el proceso de un algoritmo Dec según la Realización 2;

La Fig. 13 es un diagrama de configuración de un sistema criptográfico 10 que implementa un esquema CP-FE según la Realización 3;

La Fig. 14 es un diagrama de configuración de un dispositivo de generación de clave 100 según la Realización 3;

La Fig. 15 es un diagrama de configuración de un dispositivo de cifrado 200 según la Realización 3;

La Fig. 16 es un diagrama de configuración de un dispositivo de descifrado 300 según la Realización 3;

La Fig. 17 es un diagrama de flujo que ilustra el proceso de un algoritmo KeyGen según la Realización 3;

La Fig. 18 es un diagrama de flujo que ilustra el proceso de un algoritmo Enc según la Realización 3;

La Fig. 19 es un diagrama de flujo que ilustra el proceso de un algoritmo Dec según la Realización 3;

La Fig. 20 es un diagrama de configuración de un sistema criptográfico 10 que implementa un esquema HIPE según la Realización 4;

La Fig. 21 es un diagrama de configuración de un dispositivo de generación de clave 100 según la Realización 4;

La Fig. 22 es un diagrama de configuración de un dispositivo de cifrado 200 según la Realización 4;

La Fig. 23 es un diagrama de configuración de un dispositivo de descifrado 300 según la Realización 4;

La Fig. 24 es un diagrama de configuración de un dispositivo de delegación de clave 400 según la Realización 4;

La Fig. 25 es un diagrama de flujo que ilustra el proceso de un algoritmo Setup según la Realización 4;

La Fig. 26 es un diagrama de flujo que ilustra el proceso de un algoritmo KeyGen según la Realización 4;

La Fig. 27 es un diagrama de flujo que ilustra el proceso de un algoritmo Enc según la Realización 4;

La Fig. 28 es un diagrama de flujo que ilustra el proceso de un algoritmo Dec según la Realización 4;

La Fig. 29 es un diagrama de flujo que ilustra el proceso de un algoritmo Delegate_L según la Realización 4;

La Fig. 30 es un diagrama de configuración de un sistema criptográfico 10 que implementa un esquema de firma según la Realización 5;

La Fig. 31 es un diagrama de configuración de un dispositivo de generación de clave 100 según la Realización 5;

La Fig. 32 es un diagrama de configuración de un dispositivo de firma 500 según la Realización 5;

La Fig. 33 es un diagrama de configuración de un dispositivo de verificación 600 según la Realización 5;

La Fig. 34 es un diagrama de flujo que ilustra el proceso de un algoritmo Setup según la Realización 5;

La Fig. 35 es un diagrama de flujo que ilustra el proceso de un algoritmo KeyGen según la Realización 5;

La Fig. 36 es un diagrama de flujo que ilustra el proceso de un algoritmo Sig según la Realización 5;

La Fig. 37 es un diagrama de flujo que ilustra el proceso de un algoritmo Ver según la Realización 5;

La Fig. 38 es un dibujo explicativo de de autoridad múltiple;

La Fig. 39 es un dibujo explicativo de un esquema de cifrado funcional que permite la adición de una categoría de atributo en un caso de de autoridad múltiple; y

La Fig. 40 es un diagrama que ilustra un ejemplo de una configuración hardware del dispositivo de generación de clave 100, el dispositivo de cifrado 200, el dispositivo de descifrado 300, el dispositivo de delegación de clave 400, el dispositivo de firma 500 y el dispositivo de verificación 600.

Descripción de las realizaciones

Las realizaciones de la invención se describirán en lo sucesivo con referencia a los dibujos anexos.

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

Se describirán notaciones que se usan en la siguiente descripción.

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

[Fórmula 101]

$$y \xleftarrow{R} A$$

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

[Fórmula 102]

$$y \xleftarrow{U} A$$

La Fórmula 103 indica que y es un conjunto definido o sustituido por z.

[Fórmula 103]

y: = z

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

[Fórmula 104]

$A(x) \rightarrow a$

Por ejemplo,

$A(x) \rightarrow 1$

La Fórmula 105, esto es F_q, indica un campo finito de orden q.

[Fórmula 105]

$$\mathbb{F}_q$$

Un símbolo de vector indica una representación de vector sobre el campo finito F_q, como se indica en la Fórmula 106.

[Fórmula 106]

$\vec{x}$ indica

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

La Fórmula 107 indica el producto interior, indicado en la Fórmula 109, de dos vectores $\vec{x}$ y $\vec{v}$ indicados 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]

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

Señalar que X^T indica la traspuesta de una matriz X.

Cuando b_i (i = 1, …, n) es un elemento de un vector de un espacio V, que es cuando se establece la Fórmula 110, la Fórmula 111 indica un subespacio generado por la Fórmula 112.

[Fórmula 110]

$$b_i \in \mathbb{V} \ (i = 1,...,n)$$

[Fórmula 111]

$$\mathrm{span}\left\langle b_1,...,b_n \right\rangle \subseteq \mathbb{V} \ (\text{resp. } \mathrm{span}\left\langle \vec{x}_1,...,\vec{x}_n \right\rangle)$$

[Fórmula 112]

$$b_1,...,b_n \ (\text{resp. } \vec{x}_1,...,\vec{x}_n)$$

Para una base B y una base B* indicada en la Fórmula 113, se establece la Fórmula 114.

[Fórmula 113]

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

[Fórmula 114]

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

Señalar que $\vec{e}_j$ indica un vector de base ortonormal indicado en la Fórmula 115.

[Fórmula 115]

$$\vec{e}_j : (\overbrace{0 \cdots 0}^{j-1}, 1, \overbrace{0 \cdots 0}^{n-j}) \in \mathbb{F}_q^n \ \text{for } j = 1,...,n,$$

En la siguiente descripción, cuando “Vt” se muestra como un subíndice o superíndice, esta Vt indica V_t. Del mismo modo, cuando “δi,j” se muestra como un superíndice, este δi,j indica $\delta_{i,j}$.

Cuando “→” que representa un vector se une a un subíndice o superíndice, se supone que este “→” se une como un superíndice al subíndice o superíndice.

En la siguiente descripción, procesos de primitivas criptográficas incluyen no solamente un proceso criptográfico definido estrechamente para mantener la información segura de terceras partes, sino que también incluyen un proceso de firma. Los procesos de las primitivas criptográficas incluyen un proceso de generación de clave, un proceso de cifrado, un proceso de descifrado, un proceso de delegación de clave, un proceso de firma y un proceso de verificación.

Realización 1

Esta realización describe un concepto básico para implementar los procesos de las primitivas criptográficas que se describen en las siguientes realizaciones que permiten la adición de una categoría de atributo sin reeditar un parámetro público.

En primer lugar, se describirá la adición de una categoría de atributo.

En segundo lugar, se describirá brevemente un esquema de cifrado funcional y una construcción básica del esquema de cifrado funcional.

En tercer lugar, se describirá una técnica de clave para realizar la adición de una categoría de atributo sin reeditar un parámetro público.

En cuarto lugar, se describirá un espacio que tiene una estructura matemática rica llamada “espacios de vector de emparejamiento dual (DPVS)” que es un espacio para implementar el esquema de cifrado funcional.

En quinto lugar, se describirá un concepto para implementar el esquema de cifrado funcional. Aquí, se describirán “programa de tramo”, “producto interior de información de atributo y estructura de acceso” y “esquema de distribución de secreto (esquema de compartición de secreto)”.

<1. Adición de una categoría de atributo>

Una categoría de atributo es una clasificación de un atributo de cada usuario, tal como organización de pertenencia, departamento de pertenencia, posición en la empresa, edad y género.

Los procesos de las primitivas criptográficas que se describen en las siguientes realizaciones realizan control de acceso en base al atributo de usuario. Por ejemplo, con un proceso criptográfico definido estrechamente para asegurar la información de terceras partes, si el usuario puede descifrar o no un texto cifrado se controla en base al atributo del usuario.

Generalmente, las categorías de atributo usadas para control de acceso se determinan por adelantado en la etapa de diseño de un sistema. No obstante, puede haber un caso en el que las reglas operacionales del sistema se cambian en una etapa posterior, necesitando la adición de una categoría de atributo usada para control de acceso.

Por ejemplo, supongamos que un sistema criptográfico se construye bajo la suposición de que el sistema va a ser usado solamente dentro de la Empresa A. En este caso, se supone que las categorías de atributo a ser usadas son, por ejemplo, departamento de pertenencia, posición en la empresa e ID individual. No obstante, supongamos que las reglas operacionales se cambian en una etapa posterior de modo que el sistema criptográfico se usa no solamente en la Empresa A sino también en empresas asociadas de la Empresa A. En este caso, la empresa de pertenencia necesita ser fijada nuevamente como una categoría de atributo a ser usada.

Si las categorías de atributo usadas para control de acceso se especifican por un parámetro público, añadir una categoría de atributo a una etapa posterior requiere que el parámetro público sea reeditado y redistribuido a cada usuario. Por esta razón, una categoría de atributo no se puede añadir fácilmente en una etapa posterior y un modo operacional que no se tuvo en consideración en la etapa de diseño del sistema no se puede adoptar con flexibilidad.

Por lo tanto, es importante permitir la adición de una categoría de atributo sin reeditar un parámetro público.

<2. Esquema de cifrado funcional>

El esquema de cifrado funcional es un esquema de cifrado que proporciona relaciones más sofisticadas y flexibles entre una clave de cifrado ek y una clave de descifrado dk.

Según el esquema de cifrado funcional, un parámetro Φ y un parámetro ψ se fijan en la clave de cifrado ek y la clave de descifrado dk, respectivamente. La clave de descifrado dk puede descifrar un texto cifrado cifrado con la clave de cifrado ek si y sólo si mantiene una relación $R(\Phi, \psi)$.

El esquema de cifrado funcional incluye un esquema de cifrado basado en atributo y un esquema de cifrado basado en ID.

Se describirá brevemente la construcción del esquema de cifrado funcional.

El esquema de cifrado funcional consta de cuatro algoritmos: Setup, KeyGen, Enc y Dec.

(Setup)

Un algoritmo Setup es un algoritmo que saca un parámetro público pk y una clave maestra sk.

(KeyGen)

Un algoritmo KeyGen es un algoritmo que toma como entrada el parámetro público pk, la clave maestra sk y un parámetro ψ y saca una clave de descifrado sk_{ψ}.

(Enc)

Un algoritmo Enc es un algoritmo que toma como entrada el parámetro público pk, un parámetro Φ y un mensaje m y saca un texto cifrado ct_{Φ}.

(Dec)

Un algoritmo Dec es un algoritmo que toma como entrada el parámetro público pk, la clave de descifrado sk_{ψ} y el texto cifrado ct_{Φ} y saca el mensaje m o un símbolo distinguido 1 $\perp$.

El texto cifrado ct_Φ se puede descifrar con la clave de descifrado sk_ψ para obtener el mensaje m si y sólo si el parámetro ψ y el parámetro Φ satisfacen la relación R (si mantiene R(Φ, ψ)).

Generalmente, el algoritmo Setup se ejecuta solamente una vez en la configuración del sistema. El algoritmo KeyGen se ejecuta cada vez que va a ser generada una clave de descifrado sk_ψ de un usuario. El algoritmo Enc se ejecuta cada vez que va a ser cifrado un mensaje m. El algoritmo Dec se ejecuta cada vez que va a ser descifrado un texto cifrado ct_Φ.

<3. Técnica de clave>

La técnica de clave para realizar la adición de una categoría de atributo sin reeditar un parámetro público es aplicar una técnica de indexación a cifrado de sistema dual en los espacios de vector de emparejamiento dual.

En el cifrado de sistema dual en los espacios de vector de emparejamiento dual, se generan aleatoriamente un par de bases duales, una base B y una base B*. Entonces, una parte de la base B (base B^) se usa como un parámetro público.

En el esquema de cifrado funcional descrito en la Literatura no de Patente 29, una base $B^_1$, … y una base $B^_d$ se generan como un parámetro público. Una categoría de atributo se asigna a cada base $B^_t$ que corresponde a cada entero t = 1, …, d. Es decir, se pueden manejar d piezas de categorías de atributo.

Como es evidente a partir del hecho de que la base $B^_1$, … y la base $B^_d$ se usan como el parámetro público, el parámetro público necesita ser reeditado para añadir una base B^, es decir, para aumentar el valor de d, en una etapa posterior. En otras palabras, el valor de d está limitado por el parámetro público.

En el esquema de cifrado funcional que se describe en las siguientes realizaciones, una base B^ se genera como un parámetro público. Los vectores de índice bidimensional $\sigma_t(1, t)$ y $\mu_i(t, -1)$, que corresponden a cada entero t = 1, …, d se fija en un texto cifrado c y una clave secreta k*, respectivamente, de manera que una categoría de atributo se asigna a cada entero t. Es decir, se pueden manejar d piezas de categorías de atributo.

Señalar aquí que el parámetro público incluye la base B^ pero no los vectores de índice. Por lo tanto, cuando los vectores de índice van a ser añadidos en una etapa posterior para aumentar el valor de d, no hay necesidad de reeditar el parámetro público. En otras palabras, el valor de d no está limitado por el parámetro público.

<4. Espacios de vector de emparejamiento dual>

En primer lugar, se describirán grupos de emparejamiento bilineal simétrico.

Los grupos de emparejamiento bilineal simétrico (q, G, G^T, g, e) son una tupla de un 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 calculable polinomio-tiempo $e : G \times G \rightarrow G_T$. El emparejamiento bilineal no degenerado significa $e(sg, tg) = e(g, g)^{st}$ y $e(g, g) \neq 1$.

En la siguiente descripción, permitamos que G_{bpg} sea un algoritmo que toma como entrada 1^λ y saca valores de un parámetro $param_G := (q, G, G^T, g, e)$ de grupos de emparejamiento bilineal con un parámetro de seguridad λ.

Se describirán ahora espacios de vector de emparejamiento dual.

Los espacios de vector de emparejamiento dual (q, V, G_T, A, e) se pueden construir por un producto directo de los grupos de emparejamiento bilineal simétrico ($param_G$:=(q, G, G_T, g, e)). Los espacios de vector de emparejamiento dual (q, V, G_T, A, e) son una tupla de un primo q, un espacio de vector N dimensional V sobre F_q indicado en la Fórmula 116, un grupo cíclico G_T de orden q y una base canónica $A := (a_1, \ldots, a_N)$ del espacio V y tienen las siguientes operaciones (1) y (2), en las que a_i es como se indica en la Fórmula 117.

[Fórmula 116]

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

[Fórmula 117]

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

Operación (1): Emparejamiento bilineal no degenerado

Un emparejamiento en el espacio V se define por la Fórmula 118.

[Fórmula 118]

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

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 $\in$ 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 $\in G_T$.

Operación (2): Mapas de distorsión

Las transformaciones lineales $\varphi_{i,j}$ en el espacio V indicado en la Fórmula 119 puede lograr la Fórmula 120.

[Fórmula 119]

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

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

[Fórmula 120]

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

donde

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

Las transformaciones lineales $\varphi_{i,j}$ se llamarán mapas de distorsión.

En la siguiente descripción, permitamos que G_{dpvs} sea un algoritmo que toma como entrada 1^{λ} ($\lambda \in$ número natural), N $\in$ número natural y valores de un parámetro $param_G$:= (q, G, G_T, A, e) de grupos de emparejamiento bilineal y saca valores de un parámetro $param_V$:= (q, V, G_T, A, e) de espacios de vector de emparejamiento dual con un parámetro de seguridad λ y un espacio N dimensional V.

Una descripción se dirigirá en la presente memoria a un caso en el que los espacios de vector de emparejamiento dual se construyen usando los grupos de emparejamiento bilineal simétrico descritos anteriormente. Los espacios de vector de emparejamiento dual también se pueden construir usando grupos de emparejamiento bilineal asimétrico. La siguiente descripción se puede adaptar fácilmente a un caso en el que los espacios de vector de emparejamiento dual se construyen usando grupos de emparejamiento bilineal asimétrico.

<5. Concepto para implementar cifrado funcional>

<5.1. Programa de tramo>

La Fig. 1 es un dibujo explicativo de una matriz M^.

Permitamos que {p_1, …, p_n} sea un conjunto de variables. M^ := (M, ρ) es una matriz etiquetada. La matriz M es una matriz (L filas x r columnas) sobre F_q y ρ es una etiqueta de columnas de la matriz M y se relaciona con uno de los literales {p_1, …, p_n, ¬p_1, …, ¬p_n}. Una etiqueta ρ_i (i = 1, …, L) de cada fila de M se relaciona con uno de los literales. Es decir, ρ : {1, …, L} → {p_1, …, p_n, ¬p_1, …, ¬p_n}.

Para cada secuencia de entrada $\delta \in \{0, 1\}^n$, se define una submatriz M_δ de la matriz M. La matriz M_δ es una submatriz que consta de aquellas filas de la matriz M las etiquetas ρ de la cual se relacionan con un valor “1” por la secuencia de entrada δ. Es decir, la matriz M_δ es una submatriz que consta de las filas de la matriz M que se relacionan con p_i de manera que δ_i = 1 y las filas de la matriz M que se relacionan con ¬p_i de manera que δ_i = 0.

La Fig. 2 es un dibujo explicativo de la matriz M_δ. En la Fig. 2, señalar que n = 7, L = 6 y r = 5. Es decir, el conjunto de variables es $\{p_1, \ldots, p_7\}$ y la matriz M es una matriz (6 filas x 5 columnas). En la Fig. 2, suponemos que las etiquetas ρ se relacionan de manera que ρ_1 se relaciona con $\neg p_2$, ρ_2 con p_1, ρ_3 con p_4, ρ_4 con $\neg p_5$, ρ_5 con $\neg p_3$ y ρ_6 con p_5.

Supongamos que en una secuencia de entrada $\delta \in \{0, 1\}^7$, $\delta_1 = 1$, $\delta_2 = 0$, $\delta_3 = 1$, $\delta_4 = 0$, $\delta_5 = 0$, $\delta_6 = 1$ y $\delta_7 = 1$. En este caso, una submatriz que consta de las filas de la matriz M que se relacionan con los literales (p_1, p_3, p_6, p_7,, $\neg p_2$, $\neg p_4$, $\neg p_5$) rodeados por líneas discontinuas es la matriz M_δ. Es decir, la submatriz que consta de la primera fila (M_1), segunda fila (M_2) y cuarta fila (M_4) de la matriz M es la matriz M_δ.

En otras palabras, cuando el mapa $\gamma : \{1, \ldots, L\} \rightarrow \{0, 1\}$ es $[\rho(j) = p_i] \wedge [\delta_i = 1]$ o $[\rho(j) = \neg p_i] \wedge [\delta_i = 0]$, entonces $\gamma(j) = 1$; de otra manera $\gamma(j) = 0$. En este caso, $M_\delta := (M_j)_{\gamma(j)=1}$. Señalar que M_j es la fila de orden j de la matriz M.

Es decir, en la Fig. 2, el mapa $\gamma(j) = 1$ (j = 1, 2, 4) y el mapa $\gamma(j) = 0$ (j = 3, 5, 6). Por lo tanto, $(M_j)_{\gamma(j)=1}$ es M_1, M_2 y M_4 y la matriz M_δ.

Más específicamente, si la fila de orden j de la matriz M se incluye o no en la matriz M_δ se determina mediante si el valor del mapa $\gamma(j)$ es “0” o “1”.

El programa de tramo M^ acepta una secuencia de entrada δ si y sólo si $1^{\rightarrow} \in \text{span}<M_\delta>$ y rechaza la secuencia de entrada δ de otra manera. Es decir, el programa de tramo M^ acepta la secuencia de entrada δ si y sólo si la combinación lineal de las filas de la matriz M_δ que se obtienen a partir de la matriz M^ por la secuencia de entrada δ da $1^{\rightarrow}$. $1^{\rightarrow}$ es un vector de fila que tiene un valor de “1” en cada elemento.

Por ejemplo, en la Fig. 2, el programa de tramo M^ acepta la secuencia de entrada δ si y sólo si la combinación lineal de las filas respectivas de la matriz M_δ que consta de la 1ª, 2ª y 4ª filas de la matriz M da $1^{\rightarrow}$. Es decir, si existe α_1, α_2 y α_4 con los cuales $\alpha_1(M_1) + \alpha_2(M_2) + \alpha_4(M_4) = 1^{\rightarrow}$, el programa de tramo M^ acepta la secuencia de entrada δ.

El programa de tramo se llama monótono si sus etiquetas ρ se relacionan solamente con los literales positivos $\{p_1, \ldots, p_n\}$. El programa de tramo se llama no monótono si sus etiquetas ρ se relacionan con los literales $\{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$. Se supone en la presente memoria que el programa de tramo es no monótono. Una estructura de acceso (estructura de acceso no monótona) se constituye usando el programa de tramo no monótono. Abreviadamente, una estructura de acceso controla el acceso a cifrado, es decir, controla si un texto cifrado va a ser descifrado o no.

Como se describe en detalle más tarde, el programa de tramo que es no monótono, en lugar de ser monótono, permite una gama más amplia de aplicaciones del esquema de cifrado funcional constituido usando el programa de tramo.

<5-2. Producto interior de información de atributo y estructura de acceso>

El mapa descrito anteriormente $\gamma(j)$ se calcula usando el producto interior de información de atributo. Es decir, el producto interior de información de atributo se usa para determinar qué fila de la matriz M va a ser incluida en la matriz M_δ.

U_t (t = 1, …, d y $U_t \subset \{0, 1\}^*$) es un subuniverso y un conjunto de atributos. Cada U_t incluye información de identificación (t) del subuniverso y un vector n dimensional ($v^{\rightarrow}$). Es decir, U_t es (t, $v^{\rightarrow}$), donde $t \in \{1, \ldots, d\}$ y $v^{\rightarrow} \in F_q^n$.

Permitamos que $U_t := (t, v^{\rightarrow})$ sea una variable p del programa de tramo $M^\wedge := (M, \rho)$. Es decir, $p := (t, v^{\rightarrow})$. Permitamos que el programa de tramo $M^\wedge := (M, \rho)$ que tiene la variable $(p := (t, v^{\rightarrow}), (t', v'^{\rightarrow}), \ldots)$ sea una estructura de acceso S.

Es decir, la estructura de acceso $S := (M, \rho)$ y $\rho : \{1, \ldots, L\} \rightarrow \{(t, v^{\rightarrow}), (t', v'^{\rightarrow}), \ldots, \neg(t, v^{\rightarrow}), \neg(t', v'^{\rightarrow}), \ldots\}$.

Permitamos que Γ sea un conjunto de atributos. Es decir, $\Gamma := \{(t, x^{\rightarrow}_t) \mid x^{\rightarrow}_t \in F_q^n, 1 \leq t \leq d\}$.

Cuando Γ se da a la estructura de acceso S, el mapa γ: $\{1, \ldots, L\} \rightarrow \{0, 1\}$ para el programa de tramo $M^\wedge := (M, \rho)$ se define como sigue. Para cada entero i = 1, …, L, fijar $\gamma(j) = 1$ si $[\rho(i) = (t, v^{\rightarrow}_i)] \wedge [(t, x^{\rightarrow}_t) \in \Gamma] \wedge [v^{\rightarrow}_i \cdot x^{\rightarrow}_t = 0]$ o $[\rho(i) = \neg(t, v^{\rightarrow}_i)] \wedge [(t, x^{\rightarrow}_t) \in \Gamma] \wedge [v^{\rightarrow}_i \cdot x^{\rightarrow}_t \neq 0]$. Fijar $\gamma(j) = 0$ de otra manera.

Es decir, el mapa γ se calcula en base al producto interior de la información de atributo $v^{\rightarrow}$ y $x^{\rightarrow}$. Como se describió anteriormente, qué fila de la matriz M va a ser incluida en la matriz M_δ se determina por el mapa γ. Más específicamente, qué fila de la matriz M va a ser incluida en la matriz M_δ se determina por el producto interior de la información de atributo $v^{\rightarrow}$ y $x^{\rightarrow}$. La estructura de acceso $S := (M, \rho)$ acepta Γ si y sólo si $1^{\rightarrow} \in \text{span}<(M_i)_{\gamma(i)=1}>$.

<5-3. Esquema de distribución de secreto>

Se describirá un esquema de distribución de secreto para la estructura de acceso $S := (M, \rho)$.

El esquema de distribución de secreto está distribuyendo información secreta para reproducir información distribuida sin sentido. Por ejemplo, la información secreta s se distribuye en 10 piezas para generar 10 piezas de información distribuida. Cada una de las 10 piezas de información distribuida no tiene información sobre la información secreta s. Por lo tanto, incluso cuando se obtiene una de las piezas de información distribuida, no se puede obtener ninguna información sobre la información secreta s. Por otra parte, si se obtienen todas de las 10 piezas de información distribuida, se puede recuperar la información secreta s.

Otro esquema de distribución de secreto también está disponible de según el cual la información secreta s se puede recuperar si se puede obtener alguna (por ejemplo, 8 piezas) de información distribuida, sin obtener todas de las 10 piezas de información distribuida. Un caso como este en el que la información secreta s se puede recuperar usando 8 piezas de entre 10 piezas de información distribuida se llamará 8 de entre 10. Es decir, un caso en el que la información secreta s se puede recuperar usando t piezas de entre n piezas de información distribuida se llamará t de entre n. Esta t se llamará un umbral.

Aún otro esquema de distribución de secreto está disponible según el cual cuando se generan 10 piezas de información distribuida d_1, …, d_{10}, la información secreta s se puede recuperar con 8 piezas de información distribuida d_1, …, d_8, pero la información secreta s no se puede recuperar con 8 piezas de información distribuida d_3, …, d_{10}. En otras palabras, los esquemas de distribución de secreto incluyen un esquema según el cual si la información secreta s se puede recuperar o no se controla no solamente por el número de piezas de información distribuida obtenido, sino también la combinación de información distribuida obtenida.

La Fig. 3 es un dibujo explicativo de s_0. La Fig. 4 es un dibujo explicativo de $\vec{s}^{T}$.

Permitamos que una matriz M sea una matriz (L filas x r columnas). Permitamos que $\vec{f}^{T}$ sea un vector de columna indicado en la Fórmula 121.

[Fórmula 121]

$$\vec{f}^{T} := (f_1, \ldots f_r)^T \xleftarrow{U} \mathbb{F}_q^r$$

Permitamos que s_0 indicado en la Fórmula 122 sea información secreta que se comparte.

[Fórmula 122]

$$s_0 := \vec{1} \cdot \vec{f}^{T} := \sum_{k=1}^{r} f_k$$

Permitamos que $\vec{s}^{T}$ indicado en la Fórmula 123 sea un vector de L piezas de información distribuida de s_0.

[Fórmula 123]

$$\vec{s}^{T} := (s_1, \ldots s_L)^T := M \cdot \vec{f}^{T}$$

Permitamos que la información distribuida s_i pertenezca a ρ(i).

Si la estructura de acceso S := (M, ρ) acepta Γ, es decir, $1^{\rightarrow} \in \text{span}\langle (M_i)_{\gamma(i)=1} \rangle$ para γ : {1, …, L} → {0, 1}, entonces existen constantes $\{\alpha_i \in F_q \mid i \in I\}$ de manera que $I \subseteq \{i \in \{1, \ldots, L\} \mid \gamma(i) = 1\}$.

Esto es obvio a partir de la explicación acerca del ejemplo de la Fig. 2 que si existen α_1, α_2 y α_4 con los cuales $\alpha_1(M_1) + \alpha_2(M_2) + \alpha_4(M_4) = 1^{\rightarrow}$, el programa de tramo M^ acepta la secuencia de entrada δ. Es decir, si el programa de tramo M^ acepta la secuencia de entrada δ cuando existen α_1, α_2 y α_4 con los cuales $\alpha_1(M_1) + \alpha_2(M_2) + \alpha_4(M_4) = 1^{\rightarrow}$, entonces existen α_1, α_2 y α_4 con los cuales $\alpha_1(M_1) + \alpha_2(M_2) + \alpha_4(M_4) = 1^{\rightarrow}$.

Señalar la Fórmula 124.

[Fórmula 124]

$$\sum_{i \in I} \alpha_i s_i := s_0$$

Señalar que las constantes $\{\alpha_i\}$ se pueden calcular en polinomio de tiempo en el tamaño de la matriz M.

Con el esquema de cifrado funcional según las siguientes realizaciones, una estructura de acceso se construye aplicando el predicado de producto interior y el esquema de distribución de secreto al programa de tramo, como se describió anteriormente. Por lo tanto, se puede diseñar un control de acceso diseñado flexiblemente diseñando la matriz M en el programa de tramo y la información de atributo x y la información de atributo v (información de

predicado) en el predicado de producto interior. Es decir, se puede diseñar un control de acceso muy flexiblemente. El diseño de la matriz M corresponde al diseño de condiciones tales como un umbral del esquema de distribución de secreto.

Por ejemplo, el esquema de cifrado basado en atributo descrito anteriormente corresponde a un caso en el que el diseño del predicado de producto interior está limitado a una cierta condición en la estructura de acceso en el esquema de cifrado funcional según las siguientes realizaciones. Es decir, cuando se compara con la estructura de acceso en el esquema de cifrado funcional según las siguientes realizaciones, la estructura de acceso en el esquema de cifrado basado en atributo tiene una flexibilidad menor en el diseño de control de acceso debido a que carece de la flexibilidad en el diseño de la información de atributo x y la información de atributo v (información de predicado) en el predicado de producto interior. Más específicamente, el esquema de cifrado basado en atributo corresponde a un caso en el que información de atributo $\{\vec{x}_t\}_{t\in\{1,\ldots,d\}}$ y $\{\vec{v}_t\}_{t\in\{1,\ldots,d\}}$ se limitan a vectores bidimensionales para la relación de igualdad, por ejemplo, $\vec{x}_t := (1, x_t)$ y $\vec{v}_t := (v_t, -1)$.

Un esquema de cifrado de predicado de producto común corresponde a un caso en el que el diseño de la matriz M en el programa de tramo está limitado a una cierta condición en la estructura de acceso en el esquema de cifrado funcional según las siguientes realizaciones. Es decir, cuando se compara con la estructura de acceso en el esquema de cifrado funcional según las siguientes realizaciones, la estructura de acceso en el esquema de cifrado de predicado de producto interior tiene una flexibilidad menor en el diseño de control de acceso debido a que carece de la flexibilidad en el diseño de la matriz M en el programa de tramo. Más específicamente, el esquema de cifrado de predicado de producto interior corresponde a un caso en el que el esquema de distribución de secreto está limitado a 1 de entre 1 (o d de entre d).

En particular, la estructura de acceso en el esquema de cifrado funcional según las siguientes realizaciones constituye una estructura de acceso no monótona que usa un programa de tramo no monótono. De esta manera, mejora la flexibilidad en el diseño de control de acceso.

Más específicamente, dado que el programa de tramo no monótono incluye un literal negativo (¬p), se puede fijar una condición negativa. Por ejemplo, supongamos que una Primera Empresa incluye cuatro departamentos, A, B, C y D. Supongamos que el control de acceso va a ser realizado de manera que solamente usuarios pertenecientes a departamentos distintos del departamento B de la Primera Empresa son capaces de acceso (capaces de descifrado). En este caso, si no se puede fijar una condición negativa, se debe fijar una condición de que “el usuario pertenece a cualquiera de los departamentos A, C y D de la Primera Empresa”. Por otra parte, si se puede fijar una condición negativa, se puede fijar una condición de que “el usuario es un empleado de la Primera Empresa y pertenece a un departamento distinto del departamento B”. En otras palabras, dado que se puede fijar una condición negativa, es posible un ajuste de condición natural. Aunque el número de departamentos es pequeño en este caso, este esquema es muy efectivo en un caso en el que el número de departamentos es grande.

Realización 2

Esta realización describe un esquema de procesamiento criptográfico definido estrechamente. En particular, esta realización describe un esquema de cifrado funcional de política de clave (KP-FE).

Señalar que política de clave significa que una política, esto es una estructura de acceso, se incrusta en una clave de descifrado.

En primer lugar, se describirá la construcción del esquema KP-FE.

En segundo lugar, se describirá la configuración de un sistema criptográfico 10 que implementa el esquema KP-FE.

En tercer lugar, se describirá en detalle el esquema KP-FE.

<1. Construcción de esquema KP-FE>

El esquema KP-FE consta de cuatro algoritmos: Setup, KeyGen, Enc y Dec.

(Setup)

Un algoritmo Setup es un algoritmo probabilístico que toma como entrada un parámetro de seguridad λ y saca un parámetro público pk y una clave maestra sk.

(KeyGen)

Un algoritmo KeyGen es un algoritmo probabilístico que toma como entrada una estructura de acceso $S := (M, \rho)$, el parámetro público pk y la clave maestra sk y saca una clave de descifrado sk_S.

(Enc)

Un algoritmo Enc es un algoritmo probabilístico que toma como entrada un mensaje m, un conjunto de atributos $\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in F_q^n, 1 \leq t \leq d\}$ y el parámetro público pk y saca un texto cifrado ct_Γ.

(Dec)

Un algoritmo Dec es un algoritmo que toma como entrada el texto cifrado ct_Γ cifrado bajo el conjunto de atributos Γ, la clave de descifrado sk_S para la estructura de acceso S y el parámetro público pk y saca el mensaje m o un símbolo distinguido 1 $\perp$.

<2. Configuración de sistema criptográfico 10 que implementa un esquema KP-FE>

La Fig. 5 es un diagrama de configuración del sistema criptográfico 10 que implementa el esquema KP-FE según la Realización 2.

El sistema criptográfico 10 incluye un dispositivo de generación de clave 100, un dispositivo de cifrado 200 y un dispositivo de descifrado 300.

El dispositivo de generación de clave 100 ejecuta el algoritmo Setup tomando como entrada un parámetro de seguridad λ y de esta manera genera un parámetro público pk y una clave maestra sk. Entonces, el dispositivo de generación de clave 100 publica el parámetro público generado pk. El dispositivo de generación de clave 100 también ejecuta el algoritmo KeyGen tomando como entrada una estructura de acceso S y de esta manera genera una clave de descifrado sk_S y distribuye la clave de descifrado sk_S al dispositivo de descifrado 300 en secreto.

El dispositivo de cifrado 200 ejecuta el algoritmo Enc tomando como entrada un mensaje m, un conjunto de atributos Γ y el parámetro público pk y de esta manera genera un texto cifrado ct_Γ. El dispositivo de cifrado 200 transmite el texto cifrado ct_Γ generado al dispositivo de descifrado 300.

El dispositivo de descifrado 300 ejecuta el algoritmo Dec tomando como entrada el parámetro público pk, la clave de descifrado sk_S y el texto cifrado ct_Γ y de esta manera saca el mensaje m o un símbolo distinguido 1 $\perp$.

<3. Esquema KP-FE en detalle>

Con referencia a las Fig. 6 a 12, se describirá el esquema KP-FE y se describirá la función y operación del sistema criptográfico 10 que implementa el esquema KP-FE.

La Fig. 6 es un diagrama de configuración del dispositivo de generación de clave 100 según la Realización 2. La Fig. 7 es un diagrama de configuración del dispositivo de cifrado 200 según la Realización 2. La Fig. 8 es un diagrama de configuración del dispositivo de descifrado 300 según la Realización 2.

Las Fig. 9 y 10 son diagramas de flujo que ilustran la operación del dispositivo de generación de clave 100. La Fig. 9 es un diagrama de flujo que ilustra el proceso del algoritmo Setup y la Fig. 10 es un diagrama de flujo que ilustra el proceso del algoritmo KeyGen. La Fig. 11 es un diagrama de flujo que ilustra la operación del dispositivo de cifrado 200 y que ilustra el proceso del algoritmo Enc. La Fig. 12 es un diagrama de flujo que ilustra la operación del dispositivo de descifrado 300 y que ilustra el proceso del algoritmo Dec.

En la siguiente descripción, se supone que $x_{t,1} := 1$.

Se describirá la función y operación del dispositivo de generación de clave 100.

El dispositivo de generación de clave 100 incluye una unidad de generación de clave maestra 110, una unidad de almacenamiento de clave maestra 120, una unidad de entrada de información 130, una unidad de generación de clave de descifrado 140 y una unidad de distribución de clave 150. La unidad de generación de clave de descifrado 140 incluye una unidad de generación de vector f 141, una unidad de generación de vector s 142, una unidad de generación de número aleatorio 143 y una unidad de generación de elemento de clave 144.

En primer lugar, con referencia a la Fig. 9, se describirá el proceso del algoritmo de Setup.

(S101: Paso de generación de base ortonormal)

Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 calcula la Fórmula 125 y de esta manera genera un parámetro param, una base B_0 y una base B^*_0 y una base B_1 (base B) y una base B^*_1 (base B*).

[Fórmula 125]

(1) introducir 1^λ

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

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

$$N_0 := 1 + u_0 + 1 + w_0 + z_0, \quad N_1 := 2 + n + u + w + z$$

El proceso (4) hasta (8) se ejecuta para cada t = 0, 1.

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

(5) $X_t := (\chi_{t,i,j})_{i,j=1,\ldots,N_t} \xleftarrow{U} GL(N_t, \mathbb{F}_q)$

(6) $X_t^* := (\vartheta_{t,i,j})_{i,j=1,\ldots,N_t} := \psi \cdot (X_t^T)^{-1}$

(7) $\boldsymbol{b}_{t,i} := (\vec{\chi}_{t,i})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \chi_{t,i,j} \boldsymbol{a}_{t,j}$ para *i = 1, …, N_t,*

$$\mathbb{B}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,N_t})$$

(8) $\boldsymbol{b}_{t,i}^* := (\vec{\vartheta}_{t,i})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \vartheta_{t,i,j} \boldsymbol{a}_{t,j}$ para *i = 1, …, N_t,*

$$\mathbb{B}_t^* := (\boldsymbol{b}_{t,1}^*, \ldots, \boldsymbol{b}_{t,N_t}^*)$$

(9) $g_T := e(g,g)^{\psi}$,

$$\text{param} := (\{\text{param}_{\mathbb{V}_t}\}_{t=0,1}, g_T)$$

Es decir, la unidad de generación de clave maestra 110 ejecuta el siguiente proceso.

(1) Usando el dispositivo de entrada, la unidad de generación de clave maestra 110 toma como entrada un parámetro de seguridad λ (1^{λ}).

(2) Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 ejecuta el algoritmo G_{bpg} tomando como entrada el parámetro de seguridad λ (1^{λ}) introducido en (1) y de esta manera genera valores de un parámetro $\text{param}_G := (q, G, G_T, g, e)$ de grupos de emparejamiento bilineal.

(3) Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 genera un número aleatorio ψ y fija $1 + u_0 + 1 + w_0 + z_0$ en N_0 y $2 + n + u + w + z$ en N_1, donde n es un entero de 1 o más y u_0, w_0, z_0, u, w y z son enteros de 0 o más.

Entonces, la unidad de generación de clave maestra 110 ejecuta el siguiente proceso (4) hasta (8) para cada t = 0, 1.

(4) Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 ejecuta el algoritmo G_{dpvs} tomando como entrada el parámetro de seguridad λ (1^{λ}) introducido en (1), N_t fijado en (3) y los valores de $\text{param}_G := (q, G, G_T, g, e)$ generado en (2) y de esta manera genera valores de un parámetro $\text{param}_{Vt} := (q, V_t, G_T, A_t, e)$ de espacios de vector de emparejamiento dual.

(5) Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 toma como entrada N_t fijado en (3) y F_q y genera aleatoriamente una transformación lineal $X_t := (\chi_{t,i,j})_{i,j}$. Señalar que GL significa lineal general. En otras palabras, GL es un grupo lineal general, un conjunto de matrices cuadradas con determinantes no cero y un grupo bajo multiplicación. Señalar que $(\chi_{t,i,j})_{i,j}$ indica una matriz que concierne a los sufijos i y j de la matriz $\chi_{t,i,j}$, donde i, j = 1, …, N_t.

(6) Usando el dispositivo de procesamiento y en base al número aleatorio ψ y la transformación lineal X_t, la unidad de generación de clave maestra 110 genera $(v_{t,i,j})_{i,j} := \psi \cdot (X_t^T)^{-1}$. Como $(\chi_{t,i,j})_{i,j}$, $(v_{t,i,j})_{i,j}$ indica una matriz que concierne a los sufijos i y j de la matriz $v_{t,i,j}$, donde i, j = 1, …, N_t.

(7) Usando el dispositivo de procesamiento y en base a la transformación lineal X_t generada en (5), la unidad de generación de clave maestra 110 genera una base B_t a partir de una base ortonormal A_t generada en (4). Señalar que $\vec{x}_{t,i}$, indica la fila de orden i de la transformación lineal X_t.

(8) Usando el dispositivo de procesamiento y en base a $(v_{t,i,j})_{i,j}$ generado en (6), la unidad de generación de clave maestra 110 genera una base B^*_t a partir de la base ortonormal A_t generada en (4). Señalar que $\vec{v}_{t,i}$ indica la fila de orden i de la transformación lineal X^*_t.

(9) Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 fija $e(g, g)^{\psi}$ en g_T. La unidad de generación de clave maestra 110 también fija $\{param_{Vt}\}_{t=0,1}$ generado en (4) y g_T en param.

En resumen, en (S101), la unidad de generación de clave maestra 110 ejecuta un algoritmo G_{ob} indicado en la Fórmula 126 y de esta manera genera param, la base B_0 y la base B^*_0 y la base B_1 (base B) y la base B^*_1 (base B*).

[Fórmula 126]

$$\mathcal{G}_{ob}(1^{\lambda}):$$

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

$$N_0 := 1 + u_0 + 1 + w_0 + z_0, \quad N_1 := 2 + n + u + w + z,$$

para $t = 0,1$

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

$$X_t := (\chi_{t,i,j})_{i,j=1,\ldots,N_t} \xleftarrow{U} GL(N_t, \mathbb{F}_q),$$

$$X_t^* := (\vartheta_{t,i,j})_{i,j=1,\ldots,N_t} := \psi \cdot (X_t^T)^{-1},$$

a partir de entonces, $\vec{\chi}_{t,i}$

y $\vec{\vartheta}_{t,i}$ indican las filas de orden i de X_t y X^*_t para $i = 1, ,,,, N_t$, respectivamente,

$$\boldsymbol{b}_{t,i} := (\vec{\chi}_{t,i})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \chi_{t,i,j} \boldsymbol{a}_{t,j} \quad \text{para } i = 1, ,,,, N_t, \quad \mathbb{B}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,N_t}),$$

$$\boldsymbol{b}^*_{t,i} := (\vec{\vartheta}_{t,i})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \vartheta_{t,i,j} \boldsymbol{a}_{t,j} \quad \text{para } i = 1, ,,,, N_t, \quad \mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,N_t}),$$

$$g_T := e(g,g)^{\psi}, \quad \mathsf{param} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,1}, g_T),$$

devolver $(\mathsf{param}, \mathbb{B}_t, \mathbb{B}^*_t)$.

En la siguiente descripción, por simplicidad, la base B_1 y la base B^*_1 se describirán como la base B y la base B*.

(S102: Paso de generación de parámetro público)

Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 genera una subbase $\hat{B}_0$ de la base B_0 y una subbase $\hat{B}$ de la base B, como se indica en la Fórmula 127, las bases B_0 y B que se han generado en (S101).

[Fórmula 127]

$$\hat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,1+u_0+1}, \boldsymbol{b}_{0,1+u_0+1+w_0+1}, \ldots, \boldsymbol{b}_{0,1+u_0+1+w_0+z_0}),$$

$$\hat{\mathbb{B}} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{2+n}, \boldsymbol{b}_{2+n+u+w+1}, \ldots, \boldsymbol{b}_{2+n+u+w+z})$$

La unidad de generación de clave maestra 110 genera un parámetro público pk poniendo juntos la subbase $\hat{B}_0$ y la subbase $\hat{B}$ generadas, el parámetro de seguridad λ (1^{λ}) introducido en (S101) y param generado en (S101).

(S103: Paso de generación de clave maestra)

Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 genera una subbase $B^{\wedge *}_0$ de la base B^*_0 y una subespacio $B^{\wedge *}$ de la base B^*, como se indica en la Fórmula 128, las bases B^*_0 y $B^{\wedge *}$ que se han generado en (S101).

[Fórmula 128]

$$\hat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1},\ \boldsymbol{b}^*_{0,1+u_0+1},\ \boldsymbol{b}^*_{0,1+u_0+1+1,\ldots,}\boldsymbol{b}_{0,1+u_0+1+w_0}),$$

$$\hat{\mathbb{B}}^* := (\boldsymbol{b}^*_1,..,\boldsymbol{b}^*_{2+n},\ \boldsymbol{b}^*_{2+n+u+1},..,\ \boldsymbol{b}^*_{2+n+u+w})$$

La unidad de generación de clave maestra 110 genera una clave maestra sk que está constituida por la subbase $B^{\wedge *}_0$ y la subbase $B^{\wedge *}$ generadas.

(S104: Paso de almacenamiento de clave maestra)

La unidad de almacenamiento de clave maestra 120 almacena el parámetro pk generado en (S102) en el dispositivo de almacenamiento. La unidad de almacenamiento de clave maestra 120 también almacena la clave maestra sk generada en (S103) en el dispositivo de almacenamiento.

En resumen, en (S101) hasta (S103), el dispositivo de generación de clave 100 ejecuta el algoritmo Setup indicado en la Fórmula 129 y de esta manera genera el parámetro público pk y la clave maestra sk. En (S104), el dispositivo de generación de clave 100 almacena el parámetro público pk y la clave maestra sk generados en el dispositivo de almacenamiento.

El parámetro público se publica, por ejemplo, a través de la red y se pone a disposición del dispositivo de cifrado 200 y el dispositivo de descifrado 300.

[Fórmula 129]

$$\begin{aligned}
&\mathrm{Setup}(1^\lambda):\\
&(\mathrm{param},(\mathbb{B}_0,\mathbb{B}^*_0),(\mathbb{B},\mathbb{B}^*)) \xleftarrow{R} \mathcal{G}_{\mathrm{ob}}(1^\lambda),\\
&\hat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1},\ \boldsymbol{b}_{0,1+u_0+1},\ \boldsymbol{b}_{0,1+u_0+1+w_0+1},\ldots,\boldsymbol{b}_{0,1+u_0+1+w_0+z_0}),\\
&\hat{\mathbb{B}} := (\boldsymbol{b}_1,..,\boldsymbol{b}_{2+n},\ \boldsymbol{b}_{2+n+u+w+1},..,\ \boldsymbol{b}_{2+n+u+w+z}),\\
&\hat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1},\ \boldsymbol{b}^*_{0,1+u_0+1},\ \boldsymbol{b}^*_{0,1+u_0+1+1,\ldots,}\boldsymbol{b}_{0,1+u_0+1+w_0}),\\
&\hat{\mathbb{B}}^* := (\boldsymbol{b}^*_1,..,\boldsymbol{b}^*_{2+n},\ \boldsymbol{b}^*_{2+n+u+1},..,\ \boldsymbol{b}^*_{2+n+u+w}),\\
&\text{devolver } \mathrm{pk} := (1^\lambda,\ \mathrm{param},\ \hat{\mathbb{B}}_0,\hat{\mathbb{B}}),\ \mathrm{sk} := (\hat{\mathbb{B}}^*_0,\hat{\mathbb{B}}^*).
\end{aligned}$$

Con referencia a la Fig. 10, se describirá el proceso del algoritmo KeyGen.

(S201: Paso de entrada de información)

Usando el dispositivo de entrada, la unidad de entrada de información 130 toma como entrada la estructura de acceso descrita anteriormente S := (M, ρ). Señalar que la matriz M de la estructura de acceso S va a ser fijada según las condiciones de un sistema que se implementa. Señalar también que la información de atributo del usuario de una clave de descifrado sk_S se fija en ρ de la estructura de acceso S, por ejemplo.

(S202: Paso de generación de vector f)

Usando el dispositivo de procesamiento, la unidad de generación de vector f 141 genera aleatoriamente un vector $\vec{f}$ que tiene r piezas de elementos, como se indica en la Fórmula 130.

[Fórmula 130]

$$\vec{f} \xleftarrow{U} \mathbb{F}_q^r$$

(S203: Paso de generación de vector s)

Usando el dispositivo de procesamiento y en base a la matriz M (L filas x r columnas) incluida en la estructura de acceso S introducida en (S201) y el vector $\vec{f}$ generado en (S202), la unidad de generación de vector s 142 genera un vector $\vec{s}^T := (s_1, \ldots, s_L)^T$, como se indica en la Fórmula 131.

[Fórmula 131]

$$\vec{s}^{\mathrm{T}} := (s_1,\ldots,s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$$

Usando el dispositivo de procesamiento y en base al vector $\vec{f}$ generado en (S202), la unidad de generación de vector s 142 también genera un valor s_0, como se indica en la Fórmula 132.

[Fórmula 132]

$$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$$

(S204: Paso de generación de número aleatorio)

Usando el dispositivo de procesamiento, la unidad de generación de número aleatorio 143 genera números aleatorios, como se indica en la Fórmula 133.

[Fórmula 133]

$$\vec{\eta}_0 := (\eta_{0,1},\ldots,\eta_{0,w_0}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_0},$$

$$\mu_i,\ \theta_i \xleftarrow{\mathrm{U}} \mathbb{F}_q,\ \vec{\eta}_i := (\eta_{i,1},\ldots,\eta_{i,w}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w} \quad \text{para } i = 1, \ldots, L$$

(S205: Paso de generación de elemento de clave)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de clave 144 genera un elemento k^*_0 de la clave de descifrado sk_S, como se indica en la Fórmula 134.

[Fórmula 134]

$$\boldsymbol{k}_0^* := (-s_0,\ \overbrace{0^{u_0},}^{u_0}\ 1,\ \overbrace{\vec{\eta}_0,}^{w_0}\ \overbrace{0^{z_0},}^{z_0}\ )_{\mathbb{B}_0^*}$$

Como se describió anteriormente, para la base B y la base B* indicadas en la Fórmula 113, se establece la Fórmula 114. De esta manera, la Fórmula 134 supone que $-s_0$ se fija como el coeficiente de un vector de base $b^*_{0,1}$ de la base B^*_0, 0 se fija como el coeficiente de los vectores de base $b^*_{0,1+1}, \ldots, b^*_{0,1+u0}$, 1 se fija como el coeficiente de un vector de base $b^*_{0,1+u0+1}$, $\eta_{0,1}, \ldots, \eta_{0,w0}$ se fijan respectivamente como el coeficiente de los vectores de base $b^*_{0,1+u0+1+1}, \ldots, b^*_{0,1+u0+1+w0}$ y 0 se fija como el coeficiente de los vectores de base $b^*_{0,1+u0+1+w0+1}, \ldots, b^*_{0,1+u0+1+w0+z0}$, donde u0, w0 y z0 indican respectivamente u_0, w_0 y z_0.

Usando el dispositivo de procesamiento, la unidad de generación de elemento de clave 144 también genera un elemento k^*_i de la clave de descifrado sk_S para cada entero i = 1, …, L, como se indica en la Fórmula 135.

[Fórmula 135]

para $i = 1, \ldots, L$

si $\rho(i) = (t, \vec{v}_i)$,

$$\boldsymbol{k}_i^* := (\overbrace{\mu_i(t,\ -1,),\ s_i\vec{e}_1 + \theta_i\vec{v}_i}^{2+n}\ \overbrace{0^u,}^{u}\ \overbrace{\vec{\eta}_i,}^{w}\ \overbrace{0^z}^{z}\ )_{\mathbb{B}^*},$$

si $\rho(i) = \neg(t, \vec{v}_i)$,

$$\boldsymbol{k}_i^* := (\overbrace{\mu_i(t,\ -1,),\ s_i\vec{v}_i,}^{2+n}\ \overbrace{0^u,}^{u}\ \overbrace{\vec{\eta}_i,}^{w}\ \overbrace{0^z}^{z}\ )_{\mathbb{B}^*}$$

Es decir, como la Fórmula 134, el significado de la Fórmula 135 es como se explica a continuación. Cuando ρ(i) es un conjunto positivo $(t, \vec{v}_i)$, $\mu_i t$ se fija como el coeficiente de un vector de base b^*_1 de la base B*, $-\mu_i$ se fija como el coeficiente de un vector de base b^*_2, $s_i+\theta_i v_{i,1}$ se fija como el coeficiente de un vector de base b^*_{2+1}, $\theta_i v_{i,2}, \ldots, \theta_i v_{i,n}$ se fijan respectivamente como los coeficientes de los vectores de base $b^*_{2+2}, \ldots, b^*_{2+n}$, 0 se fija como el coeficiente de

los vectores de base b^*_{2+n+1}, …, b^*_{2+n+u}, $\eta_{i,1}$, …, $\eta_{i,w}$ se fijan respectivamente como el coeficiente de los vectores de base $b^*_{2+n+u+1}$, …, $b^*_{2+n+u+w}$ y 0 se fija como el coeficiente de los vectores de base $b^*_{2+n+u+w+1}$, …, $b^*_{2+n+u+w+z}$.

Por otra parte, cuando ρ(i) es un conjunto negativo $\neg(t, \vec{v}_i)$, $\mu_i t$ se fija como el coeficiente del vector de base b^*_1 de la base B*, $-\mu_i$ se fija como el coeficiente del vector de base b^*_2, $s_i v_{i,1}$, …, $s_i v_{i,n}$ se fijan respectivamente como el coeficiente de los vectores de base b^*_{2+1}, …, b^*_{2+n}, 0 se fija como el coeficiente de los vectores de base b^*_{2+n+1}, …, b^*_{2+n+u}, $\eta_{i,1}$, …, $\eta_{i,w}$ se fijan respectivamente como el coeficiente de los vectores de base $b^*_{2+n+u+1}$, …, $b^*_{2+n+u+w}$ y 0 se fija como el coeficiente de los vectores de base $b^*_{2+n+u+w+1}$, …, $b^*_{2+n+u+w+z}$.

(S206: Paso de distribución de clave)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de distribución de clave 150 distribuye la clave de descifrado sk_S que tiene, como elementos, la estructura de acceso S introducida en (S201) y k^*_0, k^*_1, … y k^*_L generados en (S205) al dispositivo de descifrado 300 en secreto. Como una cuestión de rutina, la clave de descifrado sk_S se puede distribuir al dispositivo de descifrado 300 mediante otro método.

En resumen, en (S201) hasta (S205), el dispositivo de generación de clave 100 ejecuta el algoritmo KeyGen indicado en la Fórmula 136 y de esta manera genera la clave de descifrado sk_S. En (S206), el dispositivo de generación de clave 100 distribuye la clave de descifrado sk_S generada al dispositivo de descifrado 300.

[Fórmula 136]

$$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \mathbb{S} := (M, \rho)):$$

$$\vec{f} \xleftarrow{\cup} \mathbb{F}_q^r,$$

$$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}},\ \vec{s}^{\mathrm{T}} := (s_1, \ldots, s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}},$$

$$\vec{\eta}_0 \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$

$$\boldsymbol{k}_0^* := (-s_0, \overbrace{0^{u_0}}^{u_0}, 1, \overbrace{\vec{\eta}_0}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*},$$

para $i = 1, \ldots, L$, $\mu_i, \theta_i \xleftarrow{\cup} \mathbb{F}_q, \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^w,$

si $\rho(i) = (t, \vec{v}_i)$,

$$\boldsymbol{k}_i^* := (\overbrace{\mu_i(t, -1,), s_i\vec{e}_1 + \theta_i\vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{\vec{\eta}_i}^{w}, \overbrace{0^z}^{z})_{\mathbb{B}^*},$$

si $\rho(i) = \neg(t, \vec{v}_i)$,

$$\boldsymbol{k}_i^* := (\overbrace{\mu_i(t, -1,), s_i\vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{\vec{\eta}_i}^{w}, \overbrace{0^z}^{z})_{\mathbb{B}^*},$$

devolver $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_0^*, \boldsymbol{k}_1^*, \ldots, \boldsymbol{k}_L^*)$.

Se describirá la función y operación del dispositivo de cifrado 200.

El dispositivo de cifrado 200 incluye una unidad de adquisición de parámetro público 210, una unidad de entrada de información 220, una unidad de generación de datos de cifrado 230 y una unidad de transmisión de datos 240. La unidad de generación de datos de cifrado 230 incluye una unidad de generación de número aleatorio 231 y una unidad de generación de elemento de cifrado 232.

Con referencia a la Fig. 11, se describirá el proceso del algoritmo Enc.

(S301: Paso de adquisición de parámetro público)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de adquisición de parámetro público 210 obtiene el parámetro público pk generado por el dispositivo de generación de clave 100.

(S302: Paso de entrada de información)

Usando el dispositivo de entrada, la unidad de entrada de información 220 toma como entrada un mensaje m que se transmite al dispositivo de descifrado 300. Usando el dispositivo de entrada, la unidad de entrada de información 220 también toma como entrada un conjunto de atributos $\Gamma := \{t, \vec{x}_t := (x_{t,1}, \ldots, x_{t,n}) \in F_q^n)) \mid 1 \leq t \leq d\}$. Señalar que t puede ser al menos algunos enteros de 1 a d, en lugar de ser todos los enteros de 1 a d. Señalar que la información sobre los atributos del usuario capaz de descifrado se fija en el conjunto de atributos Γ, por ejemplo.

(S303: Paso de generación de número aleatorio)

Usando el dispositivo de procesamiento, la unidad de generación de número aleatorio 231 genera números aleatorios, como se indica en la Fórmula 137.

[Fórmula 137]

$$\omega, \zeta \xleftarrow{U} \mathbb{F}_q,\ \vec{\varphi}_0 := (\varphi_{0,1}, \ldots, \varphi_{0,z_0}) \xleftarrow{U} \mathbb{F}_q^{z_0},$$

$$\sigma_t \xleftarrow{U} \mathbb{F}_q,\ \vec{\varphi}_t := (\varphi_{t,1}, \ldots, \varphi_{t,z}) \xleftarrow{U} \mathbb{F}_q^{z} \text{ para } (t, \vec{x}_t) \in \Gamma$$

(S304: Paso de generación de elemento de cifrado)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de cifrado 232 genera un elemento c_0 de un texto cifrado ct_Γ, como se indica en la Fórmula 138.

[Fórmula 138]

$$c_0 := (\omega, \overbrace{0^{u_0}}^{u_0}, \zeta, \overbrace{0^{w_0}}^{w_0}, \overbrace{\vec{\varphi}_0}^{z_0})_{\mathbb{B}_0}$$

Usando el dispositivo de procesamiento, la unidad de generación de elemento de cifrado 232 también genera un elemento c_t del texto cifrado ct_Γ para cada entero t incluido en la información de atributo Γ, como se indica en la Fórmula 139.

[Fórmula 139]

$$c_t = (\overbrace{\sigma_t(1, t), \vec{\omega x}_t}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\varphi}_t}^{z})_{\mathbb{B}}$$

Usando el dispositivo de procesamiento, la unidad de generación de elemento de cifrado 232 también genera un elemento c_{d+1} del texto cifrado ct_Γ, como se indica en la Fórmula 140.

[Fórmula 140]

$$c_{d+1} := g_T^{\zeta} m$$

(S305: Paso de transmisión de datos)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de transmisión de datos 240 transmite el texto cifrado ct_Γ que tiene, como elementos, el conjunto de atributos Γ introducido en (S302) y c_0, c_t y c_{d+1} generados en (S304) al dispositivo de descifrado 300. Como una cuestión de rutina, el texto cifrado ct_Γ se puede transmitir al dispositivo de descifrado 300 mediante otro método.

En resumen, en (S301) hasta (S304), el dispositivo de cifrado 200 ejecuta el algoritmo Enc indicado en la Fórmula 141 y de esta manera genera el texto cifrado ct_Γ. En (S305), el dispositivo de cifrado 200 transmite el texto cifrado ct_Γ generado al dispositivo de descifrado 300.

[Fórmula 141]

$$\mathsf{Enc}(\ \mathsf{pk},\ m,\ \Gamma := \{(t,\vec{x_t} := (x_{t,1},\ldots,x_{t,n}) \in \mathbb{F}_q^n \setminus \{\vec{0}\}) \mid 1 \le t \le d\}):$$

$$\omega,\zeta \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\varphi}_0 \xleftarrow{\cup} \mathbb{F}_q^{z_0},$$

$$c_0 := (\omega,\ \overbrace{0^{u_0}}^{u_0},\ \zeta,\ \overbrace{0^{w_0}}^{w_0},\ \overbrace{\vec{\varphi}_0}^{z_0})_{\mathbb{B}_0},\ c_{d+1} := g_T^{\zeta} m,$$

$$\text{para}(t,\vec{x_t}) \in \Gamma,\ \sigma_t \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\varphi}_t \xleftarrow{\cup} \mathbb{F}_q^{z},$$

$$c_t = (\overbrace{\sigma_t(1,t),\ \omega\vec{x_t},}^{2+n}\ \overbrace{0^{u},}^{u}\ \overbrace{0^{w},}^{w}\ \overbrace{\vec{\varphi}_t}^{z})_{\mathbb{B}},$$

$$\text{devolver } \mathsf{ct}_\Gamma := (\Gamma, c_0, \{c_t\}_{(t,\vec{x_t})\in\Gamma}, c_{d+1}).$$

Se describirá la función y operación del dispositivo de descifrado 300.

El dispositivo de descifrado 300 incluye una unidad de adquisición de clave de descifrado 310, una unidad de recepción de datos 320, una unidad de cálculo de programa de tramo 330, una unidad de cálculo de coeficiente complementario 340, una unidad de operación de emparejamiento 350 y una unidad de cálculo de mensaje 360.

Con referencia a la Fig. 12, se describirá el proceso del algoritmo Dec.

(S401: Paso de adquisición de clave de descifrado)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de adquisición de clave de descifrado 310 obtiene la clave de descifrado $sk_S := (S, k^*_0, k^*_1, \ldots, k^*_L)$ distribuida por el dispositivo de generación de clave 100. La unidad de adquisición de clave de descifrado 310 también obtiene el parámetro público pk generado por el dispositivo de generación de clave 100.

(S402: Paso de recepción de datos)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de recepción de datos 320 recibe el texto cifrado ct_Γ transmitido por el dispositivo de cifrado 200.

(S403: Paso de cálculo de programa de tramo)

Usando el dispositivo de procesamiento, la unidad de cálculo de programa de tramo 330 comprueba si la estructura de acceso S incluida en la clave de descifrado sk_S obtenida en (S401) acepta o no Γ incluido en el texto cifrado ct_Γ recibido en (S402). El método para comprobar si la estructura de acceso S acepta o no Γ es el mismo que el descrito en “5. Concepto para implementar cifrado funcional en la Realización 1”.

Si la estructura de acceso S acepta Γ (aceptar en S403), la unidad de cálculo de programa de tramo 330 avanza el proceso a (S404). Si la estructura de acceso S rechaza Γ (rechazar en S403), la unidad de cálculo de programa de tramo 330 determina que el texto cifrado ct_Γ no se puede descifrar con la clave de descifrado sk_S y finaliza el proceso.

(S404: Paso de cálculo de coeficiente complementario)

Usando el dispositivo de procesamiento, la unidad de cálculo de coeficiente complementario 340 calcula I y una constante (coeficiente complementario) $\{\alpha_i\}_{i\in I}$ de manera que se satisface la Fórmula 142.

[Fórmula 142]

$\vec{1} = \sum_{i\in I} \alpha_i M_i$, donde M_i es la fila de orden i de M,

e $I \subseteq \{i \in \{1,\ldots,L\} \mid [\rho(i) = (t,\vec{v_i}) \wedge (t,\vec{x_t}) \in \Gamma \wedge \vec{v_i}\cdot\vec{x_t} = 0]$

$$\vee [\rho(i) = \neg(t,\vec{v_i}) \wedge (t,\vec{x_t}) \in \Gamma \wedge \vec{v_i}\cdot\vec{x_t} \neq 0]\}$$

(S405: Paso de operación de emparejamiento)

Usando el dispositivo de procesamiento, la unidad de operación de emparejamiento 350 calcula la Fórmula 143 y de esta manera genera la clave de sesión $K=g_T^{\zeta}$.

[Fórmula 143]

$$K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \prod_{i \in I \wedge \rho(i)=(t,\vec{v}_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i} \prod_{i \in I \wedge \rho(i)=\neg(t,\vec{v}_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i/(\vec{v}_i \cdot \vec{x}_t)}$$

Como se indica en la Fórmula 144, la clave $K = g_T^{\zeta}$ se puede obtener calculando la Fórmula 143.

[Fórmula 144]

$$\begin{aligned} & e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot \prod_{i \in I \wedge \rho(i)=(t,\vec{v}_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i} \\ & \quad \cdot \prod_{i \in I \wedge \rho(i)=\neg(t,\vec{v}_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i/(\vec{v}_i \cdot \vec{x}_t)} \\ & = g_T^{-\omega s_0 + \zeta} \prod_{i \in I \wedge \rho(i)=(t,\vec{v}_i)} g_T^{\omega \alpha_i s_i} \prod_{i \in I \wedge \rho(i)=\neg(t,\vec{v}_i)} g_T^{\omega \alpha_i s_i (\vec{v}_i \cdot \vec{x}_t)(\vec{v}_i \cdot \vec{x}_t)} \\ & = g_T^{\omega(-s_0 + \sum_{i \in I} \alpha_i s_i) + \zeta} \\ & = g_T^{\zeta}. \end{aligned}$$

(S406: Paso de cálculo de mensaje)

Usando el dispositivo de procesamiento, la unidad de cálculo de mensaje 360 calcula $m' = c_{d+1}/K$ y de esta manera genera un mensaje m' (= m). Señalar que c_{d+1} es $g_T^{\zeta}m$, como se indica en la Fórmula 142 y que K es g_T^{ζ}. Por lo tanto, el mensaje m se puede obtener calculando $m' = c_{d+1}/K$.

En resumen, en (S401) hasta (S406), el dispositivo de descifrado 300 ejecuta el algoritmo Dec indicado en la Fórmula 145 y de esta manera genera el mensaje m' (= m).

[Fórmula 145]

$$\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_1^*, ..., \boldsymbol{k}_L^*), \ \mathsf{ct}_{\Gamma} := (\Gamma, \{\boldsymbol{c}_t\}_{\vec{x}_t \in \Gamma}, c_{d+1})):$$

si $\mathbb{S} := (M, \rho)$ acepta $\Gamma := \{(t, \vec{x}_t)\}$, entonces calcular I y $\{\alpha_i\}_{i \in I}$ de manera que

$\vec{1} = \sum_{i \in I} \alpha_i M_i$, donde M_i es la fila de orden i de M e

$$\begin{aligned} I \subseteq \{i \in \{1,...,L\} \mid & [\rho(i) = (t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t = 0] \\ & \vee [\rho(i) = \neg(t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t \neq 0]\}, \end{aligned}$$

$$K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \prod_{i \in I \wedge \rho(i)=(t,\vec{v}_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i} \prod_{i \in I \wedge \rho(i)=\neg(t,\vec{v}_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i/(\vec{v}_i \cdot \vec{x}_t)},$$

devolver $m' := c_{d+1}/K$.

Como se describió anteriormente, en el sistema criptográfico 10 según la Realización 2, $\mu_i t$ y $-\mu_i$ se fijan respectivamente como el coeficiente de los vectores de base b^*_1 y b^*_2 para el elemento k^*_i de la clave de descifrado sk_S. En el sistema criptográfico 10, σ_t y $\sigma_t t$ se fijan respectivamente como el coeficiente de los vectores de base b_1 y b_2 para el elemento c_1 del texto cifrado ct_Γ.

Debido a estas disposiciones, cuando se realiza una operación de emparejamiento sobre el elemento k^*_i y el elemento c_t para el índice correspondiente t, se obtiene un producto interior de 0 para partes constituidas por los vectores de base b^*_1 y b^*_2 y los vectores de base b_1 y b_2, que se cancelan de esta manera. Es decir, cuando se realiza una operación de emparejamiento sobre el elemento k^*_i y el elemento c_t para el índice correspondiente t, las partes de índice que se fijan como los coeficientes de los vectores de base (partes constituidas por los vectores de base b^*_1 y b^*_2 y los vectores de base b_1 y b_2) se cancelan y se puede obtener un resultado de la operación de emparejamiento para las partes restantes.

En el sistema criptográfico 10 según la Realización 2, se proporcionan las partes de índice, de manera que las bases que se usa para cada categoría de atributo se pueden construir como las bases comunes (base B y base B*). Como resultado, solamente la base B y la base B* necesitan ser incluidas en un parámetro público, eliminando la necesidad de reeditar el parámetro público cuando va a ser añadida una categoría de atributo en una etapa posterior.

En el sistema criptográfico 10 según la Realización 2, el parámetro público y la clave secreta maestra son de tamaños más pequeños comparados con los del esquema de cifrado funcional descrito en la Literatura no de Patente 29. Por lo tanto, se pueden realizar eficientemente cálculos usando el parámetro público y la clave secreta maestra.

Para las partes de índice, se requiere que 0 sea obtenido como resultado de una operación de producto interior de las partes de índice. Por lo tanto, aunque las partes de índice bidimensional, esto es los vectores de base b^*_1 y b^*_2 y los vectores de base b_1 y b_2, se emplean en la descripción anterior, las partes de índice no están limitadas a bidimensional y pueden ser tridimensional o de dimensión más alta. Los valores asignados a las partes de índice no están limitados a los descritos anteriormente y se puede emplear una disposición de asignación diferente.

El esquema de cifrado funcional se ha descrito anteriormente. Como se indica en la Fórmula 146 hasta la Fórmula 149, no obstante, el esquema de cifrado funcional descrito anteriormente se puede modificar a un esquema de cifrado basado en atributo. Señalar que N_0 es 1 + 1 + 1 + 1 + 1 = 5 y N_1 es 2 + 2 + 8 + 2 + 2 = 16 en la Fórmula 146 hasta la Fórmula 149. Es decir, $u_0 = 1$, $w_0 = 1$, $z_0 = 1$, $n = 2$, $u = 8$, $w = 2$ y $z = 2$. Incluso en este caso, se puede probar la seguridad.

[Fórmula 146]

$$\mathsf{Setup}(1^\lambda):$$

$$(\mathsf{param},(\mathbb{B}_0,\mathbb{B}_0^*),(\mathbb{B},\mathbb{B}^*)) \xleftarrow{R} \mathcal{G}_{\mathrm{ob}}(1^\lambda), \quad /*\ N=16\ */$$

$$\hat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1},\ \boldsymbol{b}_{0,3},\ \boldsymbol{b}_{0,5}),\ \hat{\mathbb{B}} := (\boldsymbol{b}_1,..,\boldsymbol{b}_4,\ \boldsymbol{b}_{15},\ \boldsymbol{b}_{16}),$$

$$\hat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*,\ \boldsymbol{b}_{0,3}^*,\ \boldsymbol{b}_{0,4}^*),\ \hat{\mathbb{B}}^* := (\boldsymbol{b}_1^*,..,\boldsymbol{b}_4^*,\ \boldsymbol{b}_{13}^*,\ \boldsymbol{b}_{14}^*),$$

$$\text{devolver } \mathsf{pk} := (1^\lambda,\ \mathsf{param},\ \hat{\mathbb{B}}_0,\hat{\mathbb{B}}),\ \mathsf{sk} := (\hat{\mathbb{B}}_0^*,\hat{\mathbb{B}}^*).$$

$$\mathcal{G}_{\mathrm{ob}}(1^\lambda):$$

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

$$N_0 := 5,\ N_1 := 16,$$

para $t = 0, 1,$ $\mathsf{param}_{\mathbb{V}_t} := (q,\mathbb{V}_t,\mathbb{G}_T,\mathbb{A}_t,e) := \mathcal{G}_{\mathrm{dpvs}}(1^\lambda, N_t, \mathsf{param}_{\mathbb{G}}),$

$$X_t := (\chi_{t,i,j})_{i,j=1,..,N_t} \xleftarrow{U} GL(N_t,\mathbb{F}_q),$$

$$X_t^* := (\vartheta_{t,i,j})_{i,j=1,..,N_t} := \psi\cdot(X_t^T)^{-1},$$

a partir de entonces, $\vec{\chi}_{t,i}$ y $\vec{\vartheta}_{t,i}$ indican las filas de orden i de X_t y X^*_t para $i = 1, \ldots, N_t$, respectivamente,

$$\boldsymbol{b}_{t,i} := (\vec{\chi}_{t,i})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \chi_{t,i,j}\boldsymbol{a}_{t,j} \text{ para } i = 1, \ldots, N_t,\ \mathbb{B}_t := (\boldsymbol{b}_{t,1},...,\boldsymbol{b}_{t,N_t}),$$

$$\boldsymbol{b}_{t,i}^* := (\vec{\vartheta}_{t,i})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \vartheta_{t,i,j}\boldsymbol{a}_{t,j} \text{ para } i = 1, \ldots, N_t,\ \mathbb{B}_t^* := (\boldsymbol{b}_{t,1}^*,...,\boldsymbol{b}_{t,N_t}^*),$$

$$g_T := e(g,g)^\psi,\ \mathsf{param} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,1},g_T),$$

$$\text{devolver } (\mathsf{param},\mathbb{B},\mathbb{B}^*).$$

[Fórmula 147]

KeyGen(pk, sk, $\mathbb{S} := (M, \rho)$):

$\vec{f} \xleftarrow{U} \mathbb{F}_q^r$, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$,

$\vec{s}^{\mathrm{T}} := (s_1, ..., s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, \eta_0 \xleftarrow{U} \mathbb{F}_q$,

$\boldsymbol{k}_0^* := (-s_0,\ 0,\ 1,\ \eta_0,\ 0)_{\mathbb{B}_0^*}$,

para $i = 1, \ldots, L$, $\mu_i,\ \theta_i,\ \eta_{i,1},\ \eta_{i,2} \xleftarrow{U} \mathbb{F}_q$,

si $\rho(i) = (t, v_i)$,

$$\boldsymbol{k}_i^* := (\overbrace{\mu_i(t,\ -1,),\ s_i + \theta_i v_i, -\theta_i}^{4}\ \overbrace{0^8,}^{8}\ \overbrace{\eta_{i,1},\ \eta_{i,2},}^{2}\ \overbrace{0^2}^{2})_{\mathbb{B}^*},$$

si $\rho(i) = \neg(t, v_i)$,

$$\boldsymbol{k}_i^* := (\overbrace{\mu_i(t,\ -1,),\ s_i(v_i, -1),}^{4}\ \overbrace{0^8,}^{8}\ \overbrace{\eta_{i,1},\ \eta_{i,2},}^{2}\ \overbrace{0^2}^{2})_{\mathbb{B}^*},$$

devolver $\mathrm{sk}_{\mathbb{S}} := (\mathbb{S},\ \boldsymbol{k}_0^*, \boldsymbol{k}_1^*, ..., \boldsymbol{k}_L^*)$.

[Fórmula 148]

Enc(pk, m, $\Gamma := \{(t, x_t) \mid 1 \le t \le d\}$):

$\omega, \zeta, \varphi_0 \xleftarrow{U} \mathbb{F}_q$,

$c_0 := (\omega,\ 0,\ \zeta,\ 0,\ \varphi_0)_{\mathbb{B}_0}$, $\boldsymbol{c}_{d+1} := g_T^{\zeta} m$,

para $(t, x_t) \in \Gamma$, $\sigma_t, \varphi_{t,1}, \varphi_{t,2} \xleftarrow{U} \mathbb{F}_q$,

$$\boldsymbol{c}_t = (\overbrace{\sigma_i(1,\ t),\ \omega(1,\ x_t),}^{4}\ \overbrace{0^8,}^{8}\ \overbrace{0^2,}^{2}\ \overbrace{\varphi_{t,1},\ \varphi_{t,2}}^{2})_{\mathbb{B}},$$

devolver $\mathrm{ct}_{\Gamma} := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,x_t)\in\Gamma}, c_{d+1})$.

[Fórmula 149]

Dec(pk, $\mathrm{sk}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{k}_1^*, ..., \boldsymbol{k}_L^*)$, $\mathrm{ct}_{\Gamma} := (\Gamma, \{\boldsymbol{c}_t\}_{x_t\in\Gamma}, c_{d+1})$):

si $\mathbb{S} := (M, \rho)$ acepta $\Gamma := \{(t, x_t)\}$, entonces calcular I y $\{\alpha_i\}_{i\in I}$ de manera que

$\vec{1} = \sum_{i\in I} \alpha_i M_i$, donde M_i es la fila de orden i de M e

$$I \subseteq \{i \in \{1, ..., L\} \mid [\rho(i) = (t, v_i) \wedge (t, x_t) \in \Gamma] \vee [\rho(i) = \neg(t, v_i) \wedge (t, x_t) \in \Gamma \wedge v_i \neq x_t]\},$$

$$K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \prod_{i\in I \wedge \rho(i)=(t,v_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i} \prod_{i\in I \wedge \rho(i)=\neg(t,v_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i/(v_i - x_t)},$$

devolver $m' := c_{d+1}/K$.

Realización 3

Como la Realización 2, esta realización describe un esquema de procesamiento criptográfico definido estrechamente. En particular, esta realización describe un esquema de cifrado funcional de política de texto cifrado (CP-FE).

Señalar que política de texto cifrado significa que una política, esto es una estructura de acceso, se incrusta en un texto cifrado.

En primer lugar, se describirá la construcción del esquema CP-FE.

En segundo lugar, se describirá la configuración de un sistema criptográfico 10 que implementa el esquema CP-FE.

En tercer lugar, se describirá en detalle el esquema CP-FE.

<1. Construcción de esquema CP-FE>

El esquema CP-FE consta de cuatro algoritmos: Setup, KeyGen, Enc y Dec.

(Setup)

Un algoritmo Setup es un algoritmo probabilístico que toma como entrada un parámetro de seguridad λ y saca un parámetro público pk y una clave maestra sk.

(KeyGen)

Un algoritmo KeyGen es un algoritmo probabilístico que toma como entrada un conjunto de atributos $\Gamma := \{(t, \vec{x_t}) \mid \vec{x_t} \in F_q^n, 1 \leq t \leq d\}$, el parámetro público pk y la clave maestra sk y saca una clave de descifrado sk_Γ.

(Enc)

Un algoritmo Enc es un algoritmo probabilístico que toma como entrada un mensaje m, una estructura de acceso $S := (M, \rho)$ y el parámetro público pk y saca un texto cifrado ct_S.

(Dec)

Un algoritmo Dec es un algoritmo que toma como entrada el texto cifrado ct_S cifrado bajo la estructura de acceso S, la clave de descifrado sk_Γ para el conjunto de atributos Γ y el parámetro público pk y saca el mensaje m o un símbolo distinguido 1 $\perp$.

<2. Configuración de sistema criptográfico 10 que implementa un esquema CP-FE>

La Fig. 13 es un diagrama de configuración del sistema criptográfico 10 que implementa el esquema CP-FE según la Realización 3.

El sistema criptográfico 10 incluye un dispositivo de generación de clave 100, un dispositivo de cifrado 200 y un dispositivo de descifrado 300.

El dispositivo de generación de clave 100 ejecuta el algoritmo Setup tomando como entrada un parámetro de seguridad λ y de esta manera genera un parámetro público pk y una clave maestra sk. Entonces, el dispositivo de generación de clave 100 publica el parámetro público pk generado. El dispositivo de generación de clave 100 también ejecuta el algoritmo KeyGen tomando como entrada un conjunto de atributos Γ y de esta manera genera una clave de descifrado sk_Γ y distribuye la clave de descifrado sk_Γ al dispositivo de descifrado 300 en secreto.

El dispositivo de cifrado 200 ejecuta el algoritmo Enc tomando como entrada un mensaje m, una estructura de acceso S y el parámetro público pk y de esta manera genera un texto cifrado ct_S. El dispositivo de cifrado 200 transmite el texto cifrado ct_S generado al dispositivo de descifrado 300.

El dispositivo de descifrado 300 ejecuta el algoritmo Dec tomando como entrada el parámetro público pk, la clave de descifrado sk_S y el texto cifrado ct_S y saca el mensaje m o un símbolo distinguido 1 $\perp$.

<3. Esquema CP-FE en detalle>

Con referencia a las Fig. 14 a 19, se describirá el esquema CP-FE y se describirá la función y operación del sistema criptográfico 10 que implementa el esquema CP-FE.

La Fig. 14 es un diagrama de configuración del dispositivo de generación de clave 100 según la Realización 3. La Fig. 15 es un diagrama de configuración del dispositivo de cifrado 200 según la Realización 3. La Fig. 16 es un diagrama de configuración del dispositivo de descifrado 300 según la Realización 3.

La Fig. 17 es un diagrama de flujo que ilustra la operación del dispositivo de generación de clave 100 y que ilustra el proceso del algoritmo KeyGen. La Fig. 18 es un diagrama de flujo que ilustra la operación del dispositivo de cifrado 200 y que ilustra el proceso del algoritmo Enc. La Fig. 19 es un diagrama de flujo que ilustra la operación del dispositivo de descifrado 300 y que ilustra el proceso del algoritmo Dec.

En la siguiente descripción, se supone que $x_{t,1} := 1$.

El proceso del algoritmo Setup es el mismo que el proceso descrito en la Realización 2 y de esta manera no se describirá.

Se describirá la función y operación del dispositivo de generación de clave 100.

El dispositivo de generación de clave 100 incluye una unidad de generación de clave maestra 110, una unidad de almacenamiento de clave maestra 120, una unidad de entrada de información 130, una unidad de generación de clave de descifrado 140 y una unidad de distribución de clave 150. La unidad de generación de clave de descifrado 140 incluye una unidad de generación de número aleatorio 143 y una unidad de generación de elemento de clave 144.

Con referencia a la Fig. 17, se describirá el proceso del algoritmo KeyGen.

(S501: Paso de entrada de información)

Usando el dispositivo de entrada, la unidad de entrada de información 130 toma como entrada un conjunto de atributos $\Gamma := \{(t, \vec{x}_t := (x_{t,1}, \ldots, x_{t,n} \in F_q^n)) \mid 1 \leq t \leq d\}$. Señalar que la información de atributo del usuario de una clave de descifrado sk_Γ se fija en el conjunto de atributos Γ, por ejemplo.

(S502: Paso de generación de número aleatorio)

Usando el dispositivo de procesamiento, la unidad de generación de número aleatorio 143 genera números aleatorios, como se indica en la Fórmula 150.

[Fórmula 150]

$$\omega \xleftarrow{U} \mathbb{F}_q, \vec{\varphi}_0 := (\varphi_{0,1}, \ldots, \varphi_{0,w_0}) \xleftarrow{U} \mathbb{F}_q^{w_0},$$

$$\sigma_t \xleftarrow{U} \mathbb{F}_q, \vec{\varphi}_t := (\varphi_{t,1}, \ldots, \varphi_{t,w}) \xleftarrow{U} \mathbb{F}_q^{w} \text{ para } (t, \vec{x}_t) \in \Gamma$$

(S503: Paso de generación de elemento de clave)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de clave 144 genera un elemento k^*_0 de la clave de descifrado sk_Γ, como se indica en la Fórmula 151.

[Fórmula 151]

$$\boldsymbol{k}_0^* := (\omega, \overbrace{0^{u_0}}^{u_0}, 1, \overbrace{\vec{\varphi}_0}^{w_0}, \overbrace{0^{z_0}}^{z_0},)_{\mathbb{B}_0^*}$$

Usando el dispositivo de procesamiento, la unidad de generación de elemento de clave 144 también genera un elemento k^*_t de la clave de descifrado sk_Γ para cada entero t incluido en el conjunto de atributos Γ, como se indica en la Fórmula 152.

[Fórmula 152]

$$\boldsymbol{k}_t^* := (\overbrace{\sigma_t(1, t), \omega\vec{x}_t,}^{2+n} \overbrace{0^u,}^{u} \overbrace{\vec{\varphi}_t,}^{w} \overbrace{0^z}^{z})_{\mathbb{B}^*}$$

(S504: Paso de distribución de clave)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de distribución de clave 150 distribuye la clave de descifrado sk_Γ que tiene, como elementos, el conjunto de atributos Γ introducido en (S501) y k^*_0 y k^*_t generados en (S503) al dispositivo de descifrado 300 en secreto. Como una cuestión de rutina, la clave de descifrado sk_Γ se puede distribuir al dispositivo de descifrado 300 mediante otro método.

En resumen, en (S501) hasta (S503), el dispositivo de generación de clave 100 ejecuta el algoritmo KeyGen indicado en la Fórmula 153 y de esta manera genera la clave de descifrado sk_Γ. En (S504), el dispositivo de generación de clave 100 distribuye la clave de descifrado sk_Γ generada al dispositivo de descifrado 300.

[Fórmula 153]

KeyGen(pk, sk, $\Gamma := \{(t, \vec{x}_t := (x_{t,1}, \ldots, x_{t,n}) \in \mathbb{F}_q^n \setminus \{\vec{0}\}) \mid 1 \le t \le d\})$:

$$\omega \xleftarrow{U} \mathbb{F}_q, \vec{\varphi}_0 \xleftarrow{U} \mathbb{F}_q^{w_0},$$

$$\boldsymbol{k}_0^* := (\omega, \overbrace{0^{u_0}}^{u_0}, 1, \overbrace{\vec{\varphi}_0}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*},$$

para $(t, \vec{x}_t) \in \Gamma$, $\sigma_t \xleftarrow{U} \mathbb{F}_q, \vec{\varphi}_t \xleftarrow{U} \mathbb{F}_q^w,$

$$\boldsymbol{k}_t^* := (\overbrace{\sigma_t(1, t), \omega\vec{x}_t}^{2+n}, \overbrace{0^u}^{u}, \overbrace{\vec{\varphi}_t}^{w}, \overbrace{0^z}^{z})_{\mathbb{B}^*},$$

devolver $\mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\vec{x}_t)\in\Gamma})$.

Se describirá la función y operación del dispositivo de cifrado 200.

El dispositivo de cifrado 200 incluye una unidad de adquisición de parámetro público 210, una unidad de entrada de información 220, una unidad de generación de datos de cifrado 230 y una unidad de transmisión de datos 240. La unidad de generación de datos de cifrado 230 incluye una unidad de generación de número aleatorio 231, una unidad de generación de elemento de cifrado 232, una unidad de generación de vector f 233 y una unidad de generación de vector s 234.

Con referencia a la Fig. 18, se describirá el proceso del algoritmo Enc.

(S601: Paso de adquisición de parámetro público)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de adquisición de parámetro público 210 obtiene el parámetro público pk generado por el dispositivo de generación de clave 100.

(S602: Paso de entrada de información)

Usando el dispositivo de entrada, la unidad de entrada de información 220 toma como entrada una estructura de acceso S := (M, ρ). Señalar que la estructura de acceso S va a ser fijada según las condiciones del sistema que se implementa. Señalar también que la información de atributo del usuario capaz de descifrado se fija en ρ de la estructura de acceso S, por ejemplo.

Usando el dispositivo de entrada, la unidad de entrada de información 220 también toma como entrada un mensaje m que se transmite al dispositivo de descifrado 300.

(S603: Paso de generación de vector f)

Usando el dispositivo de procesamiento, la unidad de generación de vector f 233 genera aleatoriamente un vector $\vec{f}$ que tiene r piezas de elementos, como se indica en la Fórmula 154.

[Fórmula 154]

$$\vec{f} \xleftarrow{U} \mathbb{F}_q^r$$

(S604: Paso de generación de vector s)

Usando el dispositivo de procesamiento y en base a una matriz M (L filas x r columnas) incluida en la estructura de acceso S introducida en (S602) y el vector $\vec{f}$ generado en (S603), la unidad de generación de vector s 234 genera un vector $\vec{s}^T := (s_1, \ldots, s_L)^T$, como se indica en la Fórmula 155.

[Fórmula 155]

$$\vec{s}^{\,T} := (s_1, \ldots, s_L)^T := M \cdot \vec{f}^{\,T}$$

Usando el dispositivo de procesamiento y en base al vector $\vec{f}$ generado en (S603), la unidad de generación de vector s 234 también genera un valor s_0, como se indica en la Fórmula 156.

[Fórmula 156]

$$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$$

(S605: Paso de generación de número aleatorio)

Usando el dispositivo de procesamiento, la unidad de generación de número aleatorio 231 genera números aleatorios, como se indica en la Fórmula 157.

[Fórmula 157]

$$\zeta \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_0 := (\eta_{0,1},\ldots,\eta_{0,z_0}) \xleftarrow{\cup} \mathbb{F}_q^{z_0},$$

para *i = 1, …, L*

$$\text{si } \rho(i) = (t, \vec{v}_i), \quad \mu_i,\ \theta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i := (\eta_{i,1},\ldots,\eta_{i,z}) \xleftarrow{\cup} \mathbb{F}_q^{z},$$
$$\text{si } \rho(i) = \neg(t, \vec{v}_i), \quad \mu_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i := (\eta_{i,1},\ldots,\eta_{i,z}) \xleftarrow{\cup} \mathbb{F}_q^{z}$$

(S606: Paso de generación de elemento de cifrado)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de cifrado 232 genera un elemento c_0 de datos de cifrado c, como se indica en la Fórmula 158.

[Fórmula 158]

$$\boldsymbol{c}_0 := (-s_0, \overbrace{0^{u_0}}^{u_0},\ \zeta,\ \overbrace{0^{w_0}}^{w_0},\ \overbrace{\vec{\eta}_0}^{z_0})_{\mathbb{B}_0}$$

Usando el dispositivo de procesamiento, la unidad de generación de elemento de cifrado 232 también genera un elemento c_i de los datos de cifrado c para cada entero i = 1, …, L, como se indica en la Fórmula 159.

[Fórmula 159]

para *i = 1, …, L*

$$\text{si } \rho(i) = (t, \vec{v}_i),$$
$$\boldsymbol{c}_i := (\overbrace{\mu_i(t, -1),\ s_i\vec{e}_1 + \theta_i\vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\eta}_i}^{z})_{\mathbb{B}},$$
$$\text{si } \rho(i) = \neg(t, \vec{v}_i),$$
$$\boldsymbol{c}_i := (\overbrace{\mu_i(t, -1),\ s_i\vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\eta}_i}^{z})_{\mathbb{B}}$$

Usando el dispositivo de procesamiento, la unidad de generación de elemento de cifrado 232 también genera un elemento c_{d+1} de los datos de cifrado c, como se indica en la Fórmula 160.

[Fórmula 160]

$$\boldsymbol{c}_{d+1} := g_T^{\zeta} m$$

(S607: Paso de transmisión de datos)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de transmisión de datos 240 transmite un texto cifrado ct_S que tiene, como elementos, la estructura de acceso S introducida en (S602) y c_0, c_1, …, c_L y c_{d+1} generados en (S606) al dispositivo de descifrado 300. Como una cuestión de rutina, el texto cifrado ct_S se puede transmitir al dispositivo de descifrado 300 mediante otro método.

En resumen, en (S601) hasta (S606), el dispositivo de cifrado 200 ejecuta el algoritmo Enc indicado en la Fórmula 161 y de esta manera genera el texto cifrado ct_S. En (S607), el dispositivo de cifrado 200 transmite el texto cifrado ct_S generado al dispositivo de descifrado 300.

[Fórmula 161]

$\mathsf{Enc}(\mathsf{pk}, m, \mathbb{S} := (M, \rho))$:

$\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$,

$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}, \vec{s}^{\mathrm{T}} := (s_1, ..., s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$,

$\zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\eta}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0}$,

$c_0 := (-s_0, \overbrace{0^{u_0}}^{u_0}, \zeta, \overbrace{0^{w_0}}^{w_0}, \overbrace{\vec{\eta}_0}^{z_0})_{\mathbb{B}_0}$,

para *i = 1, …, L,*

si $\rho(i) = (t, \vec{v}_i)$, $\mu_i, \theta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^z$,

$c_i := (\overbrace{\mu_i(t, -1), s_i\vec{e}_1 + \theta_i\vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\eta}_i}^{z})_{\mathbb{B}}$,

si $\rho(i) = \neg(t, \vec{v}_i)$, $\mu_i \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^z$,

$c_i := (\overbrace{\mu_i(t, -1), s_i\vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\eta}_i}^{z})_{\mathbb{B}}$,

$c_{d+1} := g_T^{\zeta} m$,

devolver $\mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, c_0, c_1, ..., c_L, c_{d+1})$.

Se describirá la función y operación del dispositivo de descifrado 300.

El dispositivo de descifrado 300 incluye una unidad de adquisición de clave de descifrado 310, una unidad de recepción de datos 320, una unidad de cálculo de programa de tramo 330, una unidad de cálculo de coeficiente complementario 340, una unidad de operación de emparejamiento 350 y una unidad de cálculo de mensaje 360.

Con referencia a la Fig. 15, se describirá el proceso del algoritmo Dec.

(S701: Paso de adquisición de clave de descifrado)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de adquisición de clave de descifrado 310 obtiene la clave de descifrado sk_Γ distribuida por el dispositivo de generación de clave 100. La unidad de adquisición de clave de descifrado 310 también obtiene el parámetro público pk generado por el dispositivo de generación de clave 100.

(S702: Paso de recepción de datos)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de recepción de datos 320 recibe el texto cifrado ct_S transmitido por el dispositivo de cifrado 200.

(S703: Paso de cálculo de programa de tramo)

Usando el dispositivo de procesamiento, la unidad de cálculo de programa de tramo 330 comprueba si la estructura de acceso S incluida en el texto cifrado ct_S obtenida en (S702) acepta o no Γ incluido en la clave de descifrado sk_Γ recibida en (S701). El método para comprobar si la estructura de acceso S acepta o no Γ es el mismo que el descrito en “5. Concepto para implementar cifrado funcional en la Realización 1”.

Si la estructura de acceso S acepta Γ (aceptar en S703), la unidad de cálculo de programa de tramo 330 avanza el proceso a (S704). Si la estructura de acceso S rechaza Γ (rechazar en S703), la unidad de cálculo de programa de tramo 330 determina que el texto cifrado ct_S no se puede descifrar con la clave de descifrado sk_Γ y finaliza el proceso.

(S704) hasta (S706) son sustancialmente los mismos que (S404) hasta (S406) en la Realización 2 mostrada en la Fig. 12.

En resumen, en (S701) hasta (S706), el dispositivo de cifrado 200 ejecuta el algoritmo Dec indicado en la Fórmula 162 y de esta manera genera el mensaje m’ (= m).

[Fórmula 162]

$\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\vec{x}_t)\in\Gamma}),\ \mathsf{ct}_\mathbb{S} := (\mathbb{S}, \boldsymbol{c}_0, \boldsymbol{c}_1, ..., \boldsymbol{c}_L, c_{d+1})):$

si $\mathbb{S} := (M, \rho)$ acepta $\Gamma := \{(t, \vec{x}_t)\}$, entonces calcular *I* y $\{\alpha_i\}_{i\in I}$ de manera que

$\vec{1} = \sum_{i\in I} \alpha_i M_i$, donde M_i es la fila de orden i de *M* e

$$I \subseteq \{i \in \{1,...,L\} \mid [\rho(i) = (t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t = 0]$$
$$\vee\ [\rho(i) = \neg(t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t \neq 0]\ \}.$$

$$K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \prod_{i\in I \wedge \rho(i)=(t,\vec{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}_t^*)^{\alpha_i} \prod_{i\in I \wedge \rho(i)=\neg(t,\vec{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}_t^*)^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)}$$

devolver $m' := c_{d+1}/K$.

Como se describió anteriormente, como en el sistema criptográfico 10 según la Realización 2, en el sistema criptográfico 10 según la Realización 3, se proporcionan las partes de índice, de manera que las bases que se usan para cada categoría de atributo se pueden construir como las bases comunes (base B y base B*). Como resultado, solamente la base B y la base B* necesitan ser incluidas en un parámetro público, eliminando la necesidad de reeditar el parámetro público cuando una categoría de atributo va a ser añadida en una etapa posterior.

Como en la Realización 2, para las partes de índice, se requiere que 0 sea obtenido como resultado de una operación de producto interior de las partes de índice. Por lo tanto, aunque las partes de índice bidimensionales, esto es los vectores de base b^*_1 y b^*_2 y los vectores de base b_1 y b_2, se emplean en la descripción anterior, las partes de índice no están limitadas a bidimensional y pueden ser tridimensional o de dimensión más alta. Los valores asignados a las partes de índice no están limitados a los descritos anteriormente y se puede emplear una disposición de asignación diferente.

El esquema de cifrado funcional se ha descrito anteriormente. Como se indica en la Fórmula 163 hasta la Fórmula 167, no obstante, el esquema de cifrado funcional se puede modificar a un esquema de cifrado basado en atributo. Señalar que N_0 es 1 + 1 + 1 + 1 + 1 = 5 y N_1 es 2 + 2 + 8 + 2 + 2 = 16 en la Fórmula 163 hasta la Fórmula 167. Es decir, $u_0 = 1$, $w_0 = 1$, $z_0 = 1$, n = 2, u = 8, w = 2 y z = 2. Incluso en este caso, se puede probar la seguridad.

[Fórmula 163]

$\mathsf{Setup}(1^\lambda):$

$(\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}(1^\lambda),\ \ /*\ N = 16\ */$

$\hat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5}),\ \hat{\mathbb{B}} := (\boldsymbol{b}_1, .., \boldsymbol{b}_4, \boldsymbol{b}_{15}, \boldsymbol{b}_{16}),$

$\hat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*, \boldsymbol{b}_{0,4}^*),\ \hat{\mathbb{B}}^* := (\boldsymbol{b}_1^*, .., \boldsymbol{b}_4^*, \boldsymbol{b}_{13}^*, \boldsymbol{b}_{14}^*),$

$\mathsf{pk} := (1^\lambda, \mathsf{param}, \hat{\mathbb{B}}_0, \hat{\mathbb{B}}),\ \mathsf{sk} := (\hat{\mathbb{B}}_0^*, \hat{\mathbb{B}}^*),$

devolver pk, sk.

$\mathcal{G}_{\mathsf{ob}}(1^\lambda):$

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

$N_0 := 5,\ N_1 := 16,$

para $t = 0,1,\quad \mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N_t, \mathsf{param}_\mathbb{G}),$

$X_t := (\chi_{t,i,j})_{i,j=1,..,N_t} \xleftarrow{U} GL(N_t, \mathbb{F}_q),$

$X_t^* := (\vartheta_{t,i,j})_{i,j=1,..,N_t} := \psi \cdot (X_t^T)^{-1}$, en lo sucesivo, $\vec{\chi}_{t,i}$

y $\vec{\vartheta}_{t,i}$ indican las filas de orden i de X_t y X^*_t para $i = 1, \ldots, N_t$, respectivamente,

$$\boldsymbol{b}_{t,i} := (\vec{\chi}_{t,i})\mathbb{A}_t = \sum_{j=1}^{N_t} \chi_{t,i,j}\boldsymbol{a}_{t,j} \text{ para } i = 1,...,N_t,\ \mathbb{B}_t := (\boldsymbol{b}_{t,1},...,\boldsymbol{b}_{t,N_t}),$$

$$\boldsymbol{b}^*_{t,i} := (\vec{\vartheta}_{t,i})\mathbb{A}_t = \sum_{j=1}^{N_t} \vartheta_{t,i,j}\boldsymbol{a}_{t,j} \text{ para } i = 1,...,N_t,\ \mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1},...,\boldsymbol{b}^*_{t,N_t}),$$

$$g_T := e(g,g)^{\psi},\ \text{param} := (\{\text{param}_{\mathbb{V}_t}\}_{t=0,1}, g_T),$$

devolver $(\text{param}, \mathbb{B}, \mathbb{B}^*)$.

[Fórmula 164]

KeyGen(pk, sk, $\Gamma := \{(t,x_t) \mid 1 \le t \le d\}$):

$$\omega, \varphi_0 \xleftarrow{U} \mathbb{F}_q,$$

$$\boldsymbol{k}^*_0 := (\omega,\ 0,\ 1,\ \varphi_0,\ 0)_{\mathbb{B}^*_0},$$

para $(t,x_t) \in \Gamma$, $\sigma_t,\ \varphi_{t,1},\ \varphi_{t,2} \xleftarrow{U} \mathbb{F}_q$,

$$\boldsymbol{k}^*_t := (\overbrace{\sigma_t(1,\ t),\ \omega(1,x_t),}^{4}\ \overbrace{0^8,}^{8}\ \overbrace{\varphi_{t,1},\ \varphi_{t,2},}^{2}\ \overbrace{0^2}^{2})_{\mathbb{B}^*},$$

devolver $\text{sk}_\Gamma := (\Gamma,\ \boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{(t,x_t)\in\Gamma})$.

[Fórmula 165]

Enc(pk, m, $\mathbb{S} := (M,\rho)$):

$$\vec{f} \xleftarrow{U} \mathbb{F}_q^r,\ s_0 := \vec{1}\cdot\vec{f}^{\mathrm{T}},$$

$$\vec{s}^{\mathrm{T}} := (s_1,...,s_L)^{\mathrm{T}} := M\cdot\vec{f}^{\mathrm{T}},\ \zeta,\ \eta_0 \xleftarrow{U} \mathbb{F}_q,$$

$$\boldsymbol{c}_0 := (-s_0,\ 0,\ \zeta,\ 0,\ \eta_0)_{\mathbb{B}_0},$$

para $i = 1, \ldots, L$,

si $\rho(i) = (t,v_i)$, $\mu_i,\ \theta_i,\ \eta_{i,1},\ \eta_{i,2} \xleftarrow{U} \mathbb{F}_q$,

$$\boldsymbol{c}_i := (\overbrace{\mu_i(t,\ -1),\ s_i+\theta_i v_i,\ -\theta_i}^{4}\ \overbrace{0^8,}^{8}\ \overbrace{0^2,}^{2}\ \overbrace{\eta_{i,1},\ \eta_{i,2}}^{2})_{\mathbb{B}},$$

si $\rho(i) = \neg(t,v_i)$, $\mu_i,\ \eta_{i,1},\ \eta_{i,2} \xleftarrow{U} \mathbb{F}_q$,

$$\boldsymbol{c}_i := (\overbrace{\mu_i(t,\ -1),\ s_i(v_i,-1),}^{4}\ \overbrace{0^8,}^{8}\ \overbrace{0^2,}^{2}\ \overbrace{\eta_{i,1},\ \eta_{i,2}}^{2})_{\mathbb{B}},$$

$$\boldsymbol{c}_{d+1} := g_T^{\zeta} m,$$

devolver $\text{ct}_{\mathbb{S}} := (\mathbb{S},\ \boldsymbol{c}_0, \boldsymbol{c}_1,...,\boldsymbol{c}_L, c_{d+1})$.

[Fórmula 166]

Dec(pk, $\text{sk}_\Gamma := (\Gamma, \boldsymbol{k}^*_0,\ \{\boldsymbol{k}^*_t\}_{(t,x_t)\in\Gamma})$, $\text{ct}_{\mathbb{S}} := (\mathbb{S},\ \boldsymbol{c}_0,\ \boldsymbol{c}_1,...,\ \boldsymbol{c}_L, c_{d+1})$):

si $\mathbb{S} := (M,\rho)$ acepta $\Gamma := \{(t,x_t)\}$, entonces calcular I y $\{\alpha_i\}_{i\in I}$ de manera que

$\vec{1} = \sum_{i\in I}\alpha_i M_i$, donde M_i es la fila de orden i de M e

$$I \subseteq \{i \in \{1,...,L\} \mid [\rho(i) = (t, v_i) \wedge (t, x_t) \in \Gamma \wedge v_i = x_t] \vee [\rho(i) = \neg(t, v_i) \wedge (t, x_t) \in \Gamma \wedge v_i \neq x_t]\}.$$

$$K := e(c_0, k_0^*) \prod_{i \in I \wedge \rho(i) = (t, v_i)} e(c_i, k_t^*)^{\alpha_i} \prod_{i \in I \wedge \rho(i) = \neg(t, v_i)} e(c_i, k_t^*)^{\alpha_i / (v_i - x_t)}$$

devolver $m' := c_{d+1}/K$.

En la Realización 2, se ha descrito el esquema KP-FE. En la Realización 3, se ha descrito el esquema CP-FE. Como con estos esquemas, el esquema de política unificada (UP-FE) descrito en la Literatura no de Patente 30 se puede construir de manera que no hay necesidad de reeditar un parámetro público cuando va a ser añadida una categoría de atributo.

Realización 4

Como las Realizaciones 2 y 3, esta realización describe un esquema de procesamiento criptográfico definido estrechamente. En particular, esta realización describe un esquema de cifrado de predicado de producto interior jerárquico (HIPE).

El esquema HIPE es un esquema de cifrado de predicado de producto interior que es capaz de delegación. Delegación significa que un usuario que tiene una clave de nivel más alto genera una clave de nivel más bajo que tiene capacidades más limitadas que la clave de usuario (nivel más alto). Las capacidades limitadas suponen que la clave de nivel más bajo puede descifrar solamente algunos de los textos cifrados que se pueden descifrar con la clave de nivel más alto. Como se explicó en la Realización 1, el esquema de cifrado de predicado de producto interior corresponde a un caso en el que está limitado el diseño de la estructura de acceso en el esquema de cifrado funcional.

El esquema HIPE incluye un primer esquema que es eficiente y un segundo esquema que es menos eficiente que el primer esquema, pero garantiza seguridad de incluso información de atributo que se fija en un texto cifrado (ver la Literatura no de Patente 29). Aquí, como ejemplo del segundo esquema, se describirá un esquema que permite la adición de una categoría de atributo sin reeditar un parámetro público. No obstante, haciendo modificaciones similares a los algoritmos descritos en la Literatura no de Patente 29, el primer esquema se puede construir también para permitir la adición de una categoría de atributo sin reeditar un parámetro público.

En primer lugar, se describirá la construcción del esquema HIPE.

En segundo lugar, se describirá la configuración de un sistema criptográfico 10 que implementa el esquema HIPE.

En tercer lugar, se describirá en detalle el esquema HIPE.

<1. Construcción de esquema HIPE>

El esquema HIPE consta de cinco algoritmos: Setup, KeyGen, Enc, Dec y Delegate_L.

(Setup)

Un algoritmo Setup es un algoritmo probabilístico que toma como entrada un parámetro de seguridad 1^λ y saca una clave pública maestra pk y una clave secreta maestra sk. La clave secreta maestra sk es una clave de nivel superior.

(KeyGen)

Un algoritmo KeyGen es un algoritmo probabilístico que toma como entrada la clave pública maestra pk, la clave secreta maestra sk y la información de predicado $(\vec{v}_1, \ldots, \vec{v}_L)$ $(1 \leq L \leq d)$ y saca una clave secreta de nivel de orden L sk_L.

(Enc)

Un algoritmo Enc es un algoritmo probabilístico que toma como entrada la clave pública maestra pk, la información de atributo $(\vec{x}_1, \ldots, \vec{x}_h)$ $(1 \leq h \leq d)$ y un mensaje m y saca un texto cifrado ct.

(Dec)

Un algoritmo Dec es un algoritmo probabilístico que toma como entrada la clave pública maestra pk, la clave secreta de nivel de orden L sk_L y el texto cifrado ct y saca el mensaje m o un símbolo distinguido 1 $\perp$.

(Delegate_L)

$Delegate_L$ es un algoritmo probabilístico que toma como entrada la clave pública maestra pk, la clave secreta de nivel de orden L sk_L y la información de predicado de nivel de orden (L+1) $\vec{v}_{L+1}$ (L+1 $\leq$ d) y saca una clave secreta de nivel de orden (L+1) sk_{L+1}. Es decir, el algoritmo $Delegate_L$ saca una clave secreta de nivel más bajo.

<2. Configuración de sistema criptográfico 10 que implementa un esquema HIPE>

La Fig. 20 es un diagrama de configuración del sistema criptográfico 10 que implementa el esquema HIPE según la Realización 4.

El sistema criptográfico 10 incluye un dispositivo de generación de clave 100, un dispositivo de cifrado 200, un dispositivo de descifrado 300 y un dispositivo de delegación de clave 400. Se supone en la siguiente descripción que el dispositivo de descifrado 300 incluye el dispositivo de delegación de clave 400. No obstante, el dispositivo de delegación de clave 400 se puede proporcionar separadamente del dispositivo de descifrado 300.

El dispositivo de generación de clave 100 ejecuta el algoritmo Setup tomando como entrada un parámetro de seguridad λ y de esta manera genera una clave pública maestra pk y una clave secreta maestra sk. Entonces, el dispositivo de generación de clave 100 publica la clave pública maestra pk generada. El dispositivo de generación de clave 100 también ejecuta el algoritmo KeyGen tomando como entrada la clave pública maestra pk, la clave secreta maestra sk y la información de predicado ($\vec{v}_1$, …, $\vec{v}_L$) (1 $\leq$ L $\leq$ d) y de esta manera genera una clave secreta de nivel de orden L sk_L y distribuye la clave secreta de nivel de orden L sk_L al dispositivo de descifrado de nivel de orden L 300 en secreto.

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

El dispositivo de descifrado 300 ejecuta el algoritmo Dec tomando como entrada la clave pública maestra pk, la clave secreta de nivel de orden L sk_L y el texto cifrado ct y saca el mensaje m o un símbolo distinguido 1 $\perp$.

El dispositivo de delegación de clave 400 ejecuta el algoritmo $Delegate_L$ tomando como entrada la clave pública maestra pk, la clave secreta de nivel de orden L sk_L e información de predicado de nivel de orden (L+1) $\vec{v}_{L+1}$ (L+1 $\leq$ d) y de esta manera genera una clave secreta de nivel de orden (L+1) sk_{L+1} y distribuye la clave secreta de nivel de orden (L+1) sk_{L+1} al dispositivo de descifrado de nivel de orden (L+1) 300 en secreto.

<3. Esquema HIPE en detalle>

Con referencia a las Fig. 21 a 29, se describirá el esquema HIPE y la operación y función del sistema criptográfico 10 que implementa el esquema HIPE según la Realización 4.

La Fig. 21 es un diagrama de configuración del dispositivo de generación de clave 100 según la Realización 4. La Fig. 22 es un diagrama de configuración del dispositivo de cifrado 200 según la Realización 4. La Fig. 23 es un diagrama de configuración del dispositivo de descifrado 300 según la Realización 4. La Fig. 24 es un diagrama de configuración del dispositivo de delegación de clave 400 según la Realización 4.

Las Fig. 25 y 26 muestran diagramas de flujo que ilustran la operación del dispositivo de generación de clave 100. La Fig. 25 es un diagrama de flujo que ilustra el proceso del algoritmo Setup. La Fig. 26 es un diagrama de flujo que ilustra el proceso del algoritmo KeyGen. La Fig. 27 es un diagrama de flujo que ilustra la operación del dispositivo de cifrado 200 y que ilustra el proceso del algoritmo Enc. La Fig. 28 es un diagrama de flujo que ilustra la operación del dispositivo de descifrado 300 y que ilustra el proceso del algoritmo Dec. La Fig. 29 es un diagrama de flujo que ilustra la operación del dispositivo de delegación de clave 400 y que ilustra el proceso del algoritmo $Delegate_L$.

Se describirá la función y operación del dispositivo de generación de clave 100.

El dispositivo de generación de clave 100 incluye una unidad de generación de clave maestra 110, una unidad de almacenamiento de clave maestra 120, una unidad de entrada de información 130, una unidad de generación de clave de descifrado 140 y una unidad de distribución de clave 150. La unidad de generación de clave de descifrado 140 incluye una unidad de generación de número aleatorio 143, una unidad de generación de elemento de clave 144, una unidad de generación de elemento de aleatorización 145 y una unidad de generación de elemento de delegación 146.

Con referencia a la Fig. 25, se describirá el proceso del algoritmo Setup.

S801 es sustancialmente el mismo que (S101) en la Realización 2 mostrada en la Fig. 9.

(S802: Paso de generación de parámetro público)

Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 genera una subbase $B\hat{}_0$ de la base B_0, una subbase B^ de la base B, una subbase $B\hat{}^*_{0,pk}$ de la base B^*_0 y una subbase $B\hat{}^*_{pk}$ de la base B*, como se indica en la Fórmula 167, las bases B_0, B^, B y B^*_0 que se han generado en (S801).

[Fórmula 167]

$$\hat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1},\ \boldsymbol{b}_{0,1+u_0+1},\ \boldsymbol{b}_{0,1+u_0+1+w_0+1},\ldots,\boldsymbol{b}_{0,1+u_0+1+w_0+z_0}),$$

$$\hat{\mathbb{B}} := (\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{2+n},\ \boldsymbol{b}_{2+n+u+w+1},\ldots,\ \boldsymbol{b}_{2+n+u+w+z}),$$

$$\hat{\mathbb{B}}^*_{0,\mathsf{pk}} := \boldsymbol{b}^*_{0,1+u_0+1+1},\ldots,\boldsymbol{b}^*_{0,1+u_0+1+w_0},$$

$$\hat{\mathbb{B}}^*_{\mathsf{pk}} := (\boldsymbol{b}^*_1,\ \boldsymbol{b}^*_2,\ \boldsymbol{b}^*_{2+n+u+1},\ldots,\ \boldsymbol{b}^*_{2+n+u+w})$$

La unidad de generación de clave maestra 110 genera un parámetro público pk poniendo juntos la subbase B^$_0$, la subbase B^, la subbase B^*$_{0,pk}$ y la subbase B^*$_{pk}$ generadas, el parámetro de seguridad λ (1^λ) introducido en (S801) y param generado en (S801).

(S803: Paso de generación de clave maestra)

Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 genera una subbase B^*$_{0,sk}$ de la base B*$_0$ y una subbase B^*$_{sk}$ de la base B*, como se indica en la Fórmula 168, las bases B*$_0$ y B* que se han generado en (S801).

[Fórmula 168]

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

$$\hat{\mathbb{B}}^*_{\mathsf{sk}} := (\boldsymbol{b}^*_{2+1},\ldots,\ \boldsymbol{b}^*_{2+n})$$

La unidad de generación de clave maestra 110 genera una clave maestra sk que está constituida por la subbase B^*$_0$ y la subbase B^* generadas.

(S804: Paso de almacenamiento de clave maestra)

La unidad de almacenamiento de clave maestra 120 almacena el parámetro público pk generado en (S802) en el dispositivo de almacenamiento. La unidad de almacenamiento de clave maestra 120 también almacena la clave maestra sk generada en (S803) en el dispositivo de almacenamiento.

En resumen, en (S801) hasta (S803), el dispositivo de generación de clave 100 ejecuta el algoritmo Setup indicado en la Fórmula 169 y de esta manera genera el parámetro público pk y la clave maestra sk. En (S804), el dispositivo de generación de clave 100 almacena el parámetro público pk y la clave maestra sk generados en el dispositivo de almacenamiento.

El parámetro público se publica a través de la red, por ejemplo y se pone a disposición del dispositivo de cifrado 200 y del dispositivo de descifrado 300.

[Fórmula 169]

$$\mathsf{Setup}(1^\lambda):$$

$$(\mathsf{param},(\mathbb{B}_0,\mathbb{B}^*_0),(\mathbb{B},\mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda),$$

$$\hat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1},\ \boldsymbol{b}_{0,1+u_0+1},\ \boldsymbol{b}_{0,1+u_0+1+w_0+1},\ldots,\boldsymbol{b}_{0,1+u_0+1+w_0+z_0}),$$

$$\hat{\mathbb{B}} := (\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{2+n},\ \boldsymbol{b}_{2+n+u+w+1},\ldots,\ \boldsymbol{b}_{2+n+u+w+z}),$$

$$\hat{\mathbb{B}}^*_{0,\mathsf{pk}} := \boldsymbol{b}^*_{0,1+u_0+1+1},\ldots,\boldsymbol{b}^*_{0,1+u_0+1+w_0},\ \ \hat{\mathbb{B}}^*_{0,\mathsf{sk}} := (\boldsymbol{b}^*_{0,1},\boldsymbol{b}^*_{0,1+u_0+1}),$$

$$\hat{\mathbb{B}}^*_{\mathsf{pk}} := (\boldsymbol{b}^*_1,\ \boldsymbol{b}^*_2,\ \boldsymbol{b}^*_{2+n+u+1},\ldots,\ \boldsymbol{b}^*_{2+n+u+w}),\ \ \hat{\mathbb{B}}^*_{\mathsf{sk}} := (\boldsymbol{b}^*_{2+1},\ldots,\ \boldsymbol{b}^*_{2+n}),$$

$$\text{devolver } \mathsf{pk} := (1^\lambda,\mathsf{param},\hat{\mathbb{B}}_0,\hat{\mathbb{B}},\hat{\mathbb{B}}^*_{0,\mathsf{pk}},\hat{\mathbb{B}}^*_{\mathsf{pk}}),\ \mathsf{sk} := (\hat{\mathbb{B}}^*_{0,\mathsf{sk}},\hat{\mathbb{B}}^*_{\mathsf{sk}}).$$

Con referencia a la Fig. 26, se describirá el proceso del algoritmo KeyGen que se ejecuta por el dispositivo de generación de clave 100.

(S901: Paso de entrada de información)

Usando el dispositivo de entrada, la unidad de entrada de información 130 toma como entrada información de predicado ($\vec{v}_1, \ldots, \vec{v}_L$). Señalar que $\vec{v}_i := v_{i,1}, \ldots, v_{i,n}$ para cada entero i = 1, …, L. Señalar que el atributo del usuario de la clave se introduce como la información de predicado.

(S902: Paso de generación de número aleatorio)

Usando el dispositivo de procesamiento, la unidad de generación de número aleatorio 143 genera números aleatorios, como se indica en la Fórmula 170.

[Fórmula 170]

para *j = 1, …, 2L; τ = L+1, …, d; t = 1, …, n;*

$$\psi, \mu_{\mathrm{dec},t}, \mu_{\mathrm{ran},1,j,t}, s_{\mathrm{dec},t}, s_{\mathrm{ran},1,j,t},$$
$$\theta_{\mathrm{dec},t}, \theta_{\mathrm{ran},1,j,t} \xleftarrow{\cup} \mathbb{F}_q \quad \text{para } t = 1,\ldots,L,$$
$$\mu_{\mathrm{del},(\tau,t),t}, \mu_{\mathrm{ran},2,\tau,t}, s_{\mathrm{del},(\tau,t),t}, s_{\mathrm{ran},2,\tau,t},$$
$$\theta_{\mathrm{del},(\tau,t),t}, \theta_{\mathrm{ran},2,\tau,t} \xleftarrow{\cup} \mathbb{F}_q \quad \text{para } t = 1,\ldots,L+1,$$
$$\vec{\eta}_{\mathrm{dec},0} := \eta_{\mathrm{dec},0,1},\ldots,\eta_{\mathrm{dec},0,w_0}, \vec{\eta}_{\mathrm{ran},1,j,0} := \eta_{\mathrm{ran},1,j,0,1},\ldots,\eta_{\mathrm{ran},1,j,0,w_0},$$
$$\vec{\eta}_{\mathrm{del},(\tau,t),0} := \eta_{\mathrm{del},(\tau,t),0,1},\ldots,\eta_{\mathrm{del},(\tau,t),0,w_0},$$
$$\vec{\eta}_{\mathrm{ran},2,\tau,0} := \eta_{\mathrm{ran},2,\tau,0,1},\ldots,\eta_{\mathrm{ran},2,\tau,0,w_0} \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$
$$\vec{\eta}_{\mathrm{dec},t} := \eta_{\mathrm{dec},t,1},\ldots,\eta_{\mathrm{dec},t,w},$$
$$\vec{\eta}_{\mathrm{ran},1,j,t} := \eta_{\mathrm{ran},1,j,t,1},\ldots,\eta_{\mathrm{ran},1,j,t,w} \xleftarrow{\cup} \mathbb{F}_q^{w} \quad \text{para } t = 1,\ldots,L,$$
$$\vec{\eta}_{\mathrm{del},(\tau,t),t} := \eta_{\mathrm{del},(\tau,t),t,1},\ldots,\eta_{\mathrm{del},(\tau,t),t,w},$$
$$\vec{\eta}_{\mathrm{ran},2,\tau,t} := \eta_{\mathrm{ran},2,\tau,t,1},\ldots,\eta_{\mathrm{ran},2,\tau,t,w} \xleftarrow{\cup} \mathbb{F}_q^{w} \quad \text{para } t = 1,\ldots,L+1$$

La unidad de generación de número aleatorio 143 también fija $s_{\mathrm{dec},0}$, $s_{\mathrm{ran},1,j,0}$, $s_{\mathrm{ran},2,\tau,0}$ y $s_{\mathrm{del},(\tau,t),0}$, como se indica en la Fórmula 171.

[Fórmula 171]

$$s_{\mathrm{dec},0} := \sum_{t=1}^{L} s_{\mathrm{dec},t},$$
$$s_{\mathrm{ran},1,j,0} := \sum_{t=1}^{L} s_{\mathrm{ran},1,j,t},$$
$$s_{\mathrm{ran},2,\tau,0} := \sum_{t=1}^{L+1} s_{\mathrm{ran},2,\tau,t},$$
$$s_{\mathrm{del},(\tau,t),0} := \sum_{t=1}^{L+1} s_{\mathrm{del},(\tau,t),t}$$

(S903: Paso de generación de elemento de clave)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de clave 144 genera un elemento de clave $k^*_{L,\mathrm{dec}}$ que es un elemento de la clave de descifrado sk_L, como se indica en la Fórmula 172.

[Fórmula 172]

$$k^*_{L,\mathrm{dec}} := ((-s_{\mathrm{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathrm{dec},0}, 0^{z_0})_{\mathbb{B}_0^*},$$
$$(\mu_{\mathrm{dec},t}(t,-1), s_{\mathrm{dec},t}\vec{e}_1 + \theta_{\mathrm{dec},t}\vec{v}_t, 0^{u}, \vec{\eta}_{\mathrm{dec},t}, 0^{z})_{\mathbb{B}^*}$$
$$: t = 1,\ldots,L)$$

(S904: Paso de generación de primer elemento de aleatorización)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de aleatorización 145 genera un primer elemento de aleatorización $k^*_{L,\mathrm{ran},1,j}$ que es un elemento de la clave de descifrado sk_L, para cada entero j = 1, …, 2L, como se indica en la Fórmula 173.

[Fórmula 173]

$$\boldsymbol{k}^{*}_{L,\mathrm{ran},1,j} := (\ (-s_{\mathrm{ran},1,j,0},\ 0^{u_0},\ 0,\ \vec{\eta}_{\mathrm{ran},1,j,0},\ 0^{z_0})_{\mathbb{B}^{*}_{0}},$$
$$(\mu_{\mathrm{ran},1,j,t}(t,-1),\ s_{\mathrm{ran},1,j,t}\vec{e}_1 + \theta_{\mathrm{ran},1,j,t}\vec{v}_t,\ 0^{u},$$
$$\vec{\eta}_{\mathrm{ran},1,j,t},\ 0^{z})_{\mathbb{B}^{*}} :\ t = 1,\ldots,L)$$

(S905: Paso de generación de segundo elemento de aleatorización)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de aleatorización 145 genera un segundo elemento de aleatorización $k^{*}_{L,\mathrm{ran},2,\tau}$ que es un elemento de la clave de descifrado sk_L, para cada entero τ = L+1, …, d, como se indica en la Fórmula 174.

[Fórmula 174]

$$\boldsymbol{k}^{*}_{L,\mathrm{ran},2,\tau} := (\ (-s_{\mathrm{ran},2,\tau,0},\ 0^{u_0},\ 0,\ \vec{\eta}_{\mathrm{ran},2,\tau,0},\ 0^{z_0})_{\mathbb{B}^{*}_{0}},$$
$$(\mu_{\mathrm{ran},2,\tau,t}(t,-1),\ s_{\mathrm{ran},2,\tau,t}\vec{e}_1 + \theta_{\mathrm{ran},2,\tau,t}\vec{v}_t,\ 0^{u},$$
$$\vec{\eta}_{\mathrm{ran},2,\tau,t},\ 0^{z})_{\mathbb{B}^{*}} :\ t = 1,\ldots,L,$$
$$(\mu_{\mathrm{ran},2,\tau,L+1}(\tau,-1),\ s_{\mathrm{ran},2,\tau,L+1}\vec{e}_1,\ 0^{u},\ \vec{\eta}_{\mathrm{ran},2,\tau,L+1},\ 0^{z})_{\mathbb{B}^{*}})$$

(S906: Paso de generación de elemento de delegación)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de delegación 146 genera un elemento de delegación $k^{*}_{L,\mathrm{del},(\tau,t)}$ que es un elemento de la clave de descifrado sk_L, para cada entero τ = L+1, …, d y cada entero τ = 1, 2 con respecto a cada entero τ , como se indica en la Fórmula 175.

[Fórmula 175]

$$\boldsymbol{k}^{*}_{L,\mathrm{del},(\tau,t)} := (\ (-s_{\mathrm{del},(\tau,t),0},\ 0^{u_0},\ 0,\ \vec{\eta}_{\mathrm{del},(\tau,t),0},\ 0^{z_0})_{\mathbb{B}^{*}_{0}},$$
$$(\mu_{\mathrm{del},(\tau,t),t}(t,-1),\ s_{\mathrm{del},(\tau,t),t}\vec{e}_1 + \theta_{\mathrm{del},(\tau,t),t}\vec{v}_t,\ 0^{u},$$
$$\vec{\eta}_{\mathrm{del},(\tau,t),t},\ 0^{z})_{\mathbb{B}^{*}} :\ t = 1,\ldots,L,$$
$$(\mu_{\mathrm{del},(\tau,t),L+1}(\tau,-1),\ s_{\mathrm{del},(\tau,1),L+1}\vec{e}_1 + \psi\vec{e}_t,\ 0^{u},$$
$$\vec{\eta}_{\mathrm{del},(\tau,2),L+1},\ 0^{z})_{\mathbb{B}^{*}})$$

(S907: Paso de distribución de clave)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de distribución de clave 150 distribuye la clave de descifrado sk_L que tiene, como elementos, el elemento de clave $k^{*}_{L,dec}$, el primer elemento de aleatorización $k^{*}_{L,ran,1,j}$, el segundo elemento de aleatorización $k^{*}_{L,\mathrm{ran},2,\tau}$ y el elemento de delegación $k^{*}_{L,\mathrm{del},(\tau,t)}$ al dispositivo de descifrado 300 en secreto. Como una cuestión de rutina, la clave de descifrado sk_L se puede distribuir al dispositivo de descifrado 300 mediante otro método.

En resumen, en (S901) hasta (S906), el dispositivo de generación de clave 100 ejecuta el algoritmo KeyGen indicado en la Fórmula 176 y la Fórmula 177 y de esta manera genera la clave de descifrado sk_L. En (S907), el dispositivo de generación de clave 100 distribuye la clave de descifrado sk_L generada al dispositivo de descifrado 300.

[Fórmula 176]

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ (\vec{v}_1,...,\vec{v}_L)\in \mathbb{F}_q^n\times\cdots\times\mathbb{F}_q^n)$:

para $j=1,...,2L;\ \tau=L+1,...,d;\ t=1,...,\mathrm{n};$

$\psi,\mu_{\mathsf{dec},t},\mu_{\mathsf{ran},1,j,t},\ s_{\mathsf{dec},t},s_{\mathsf{ran},1,j,t},$

$\theta_{\mathsf{dec},t},\theta_{\mathsf{ran},1,j,t}\xleftarrow{\mathsf{U}}\mathbb{F}_q$ para $t=1,...,L$,

$\mu_{\mathsf{del},(\tau,\iota),t},\mu_{\mathsf{ran},2,\tau,t},\ s_{\mathsf{del},(\tau,\iota),t},s_{\mathsf{ran},2,\tau,t},$

$\theta_{\mathsf{del},(\tau,\iota),t},\theta_{\mathsf{ran},2,\tau,t}\xleftarrow{\mathsf{U}}\mathbb{F}_q$ para $t=1,...,L+1$,

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

$s_{\mathsf{ran},1,j,0}:=\sum_{t=1}^{L}s_{\mathsf{ran},1,j,t},\ s_{\mathsf{ran},2,\tau,0}:=\sum_{t=1}^{L+1}s_{\mathsf{ran},2,\tau,t},$

$\vec{\eta}_{\mathsf{dec},0},\vec{\eta}_{\mathsf{ran},1,j,0},\vec{\eta}_{\mathsf{del},(\tau,\iota),0},\vec{\eta}_{\mathsf{ran},2,\tau,0}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{w_0},$

$\vec{\eta}_{\mathsf{dec},t},\vec{\eta}_{\mathsf{ran},1,j,t}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{w}$ para $t=1,...,L$,

$\vec{\eta}_{\mathsf{del},(\tau,\iota),t},\vec{\eta}_{\mathsf{ran},2,\tau,t}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{w}$ para $t=1,...,L+1$,

[Fórmula 177]

$$\boldsymbol{k}^*_{L,\mathsf{dec}}:=(\ (-s_{\mathsf{dec},0},\ 0^{u_0},\ 1,\ \vec{\eta}_{\mathsf{dec},0},\ 0^{z_0})_{\mathbb{B}^*_0},$$
$$(\mu_{\mathsf{dec},t}(t,-1),\ s_{\mathsf{dec},t}\vec{e}_1+\theta_{\mathsf{dec},t}\vec{v}_t,\ 0^{\mathrm{u}},\ \vec{\eta}_{\mathsf{dec},t},\ 0^{\mathrm{z}})_{\mathbb{B}^*}\ :t=1,...,L),$$

$$\boldsymbol{k}^*_{L,\mathsf{del},(\tau,\iota)}:=(\ (-s_{\mathsf{del},(\tau,\iota),0},\ 0^{u_0},\ 0,\ \vec{\eta}_{\mathsf{del},(\tau,\iota),0},\ 0^{z_0})_{\mathbb{B}^*_0},$$
$$(\mu_{\mathsf{del},(\tau,\iota),t}(t,-1),\ s_{\mathsf{del},(\tau,\iota),t}\vec{e}_1+\theta_{\mathsf{del},(\tau,\iota),t}\vec{v}_t,\ 0^{\mathrm{u}},$$
$$\vec{\eta}_{\mathsf{del},(\tau,\iota),t},\ 0^{\mathrm{z}})_{\mathbb{B}^*}\ :\ t=1,...,L,$$
$$(\mu_{\mathsf{del},(\tau,\iota),L+1}(\tau,-1),\ s_{\mathsf{del},(\tau,1),L+1}\vec{e}_1+\psi\vec{e}_t,\ 0^{\mathrm{u}},$$
$$\vec{\eta}_{\mathsf{del},(\tau,2),L+1},\ 0^{\mathrm{z}})_{\mathbb{B}^*})$$

$$\boldsymbol{k}^*_{L,\mathsf{ran},1,j}:=(\ (-s_{\mathsf{ran},1,j,0},\ 0^{u_0},\ 0,\ \vec{\eta}_{\mathsf{ran},1,j,0},\ 0^{z_0})_{\mathbb{B}^*_0},$$
$$(\mu_{\mathsf{ran},1,j,t}(t,-1),\ s_{\mathsf{ran},1,j,t}\vec{e}_1+\theta_{\mathsf{ran},1,j,t}\vec{v}_t,\ 0^{\mathrm{u}},$$
$$\vec{\eta}_{\mathsf{ran},1,j,t},\ 0^{\mathrm{z}})_{\mathbb{B}^*}\ :\ t=1,...,L),$$

$$\boldsymbol{k}^*_{L,\mathsf{ran},2,\tau}:=(\ (-s_{\mathsf{ran},2,\tau,0},\ 0^{u_0},\ 0,\ \vec{\eta}_{\mathsf{ran},2,\tau,0},\ 0^{z_0})_{\mathbb{B}^*_0},$$
$$(\mu_{\mathsf{ran},2,\tau,t}(t,-1),\ s_{\mathsf{ran},2,\tau,t}\vec{e}_1+\theta_{\mathsf{ran},2,\tau,t}\vec{v}_t,\ 0^{\mathrm{u}},$$
$$\vec{\eta}_{\mathsf{ran},2,\tau,t},\ 0^{\mathrm{z}})_{\mathbb{B}^*}\ :\ t=1,...,L,$$
$$(\mu_{\mathsf{ran},2,\tau,L+1}(\tau,-1),\ s_{\mathsf{ran},2,\tau,L+1}\vec{e}_1,\ 0^{\mathrm{u}},\ \vec{\eta}_{\mathsf{ran},2,\tau,L+1},\ 0^{\mathrm{z}})_{\mathbb{B}^*}),$$

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

devolver sk_L.

Se describirá la función y operación del dispositivo de cifrado 200.

El dispositivo de cifrado 200 incluye una unidad de adquisición de parámetro público 210, una unidad de entrada de información 220, una unidad de generación de datos de cifrado 230 y una unidad de transmisión de datos 240. La unidad de generación de datos de cifrado 230 incluye una unidad de generación de número aleatorio 231 y una unidad de generación de elemento de cifrado 232.

Con referencia a la Fig. 27, se describirá el proceso del algoritmo Enc que se ejecuta por el dispositivo de cifrado 200.

(S1001: Paso de adquisición de clave pública maestra)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de adquisición de parámetro público 210 obtiene la clave pública maestra pk generada por el dispositivo de generación de clave 100.

(S1002: Paso de entrada de información)

Usando el dispositivo de entrada, la unidad de entrada de información 220 toma como entrada información de atributo ($\vec{x}_1, \ldots, \vec{x}_L$), donde $\vec{x}_i := x_{i,1}, \ldots, x_{i,L}$ para cada entrada i = 1, …, L. Señalar que el atributo de una persona capaz de descifrar un mensaje cifrado se introduce como la información de atributo.

Usando el dispositivo de entrada, la unidad de entrada de información 220 también toma como entrada un mensaje m que se cifra.

(S1003: Paso de generación de número aleatorio)

Usando el dispositivo de procesamiento, la unidad de generación de número aleatorio 231 genera números aleatorios, como se indica en la Fórmula 178.

[Fórmula 178]

$$\omega,\zeta \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\varphi}_0 := \varphi_{0,1},\ldots,\varphi_{0,z_0} \xleftarrow{\cup} \mathbb{F}_q^{z_0},$$
$$\vec{\varphi}_t := \varphi_{t,1},\ldots,\varphi_{t,z} \xleftarrow{\cup} \mathbb{F}_q^{z},\ \sigma_t \xleftarrow{\cup} \mathbb{F}_q \ \text{para}\ t = 1,\ldots,L$$

(S1004: Paso de generación de elemento de cifrado c1)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de cifrado 232 genera un elemento de cifrado c_1 que es un elemento de un texto cifrado ct, como se indica en la Fórmula 179.

[Fórmula 179]

$$c_1 := ((\omega,0^{u_0},\zeta,0^{w_0},\vec{\varphi}_0)_{\mathbb{B}_0},\ (\sigma_t(1,t),\ \omega\vec{x}_t,\ 0^u,0^w,\vec{\varphi}_t)_{\mathbb{B}} : t = 1,\ldots,L)$$

(S1005: Paso de generación de elemento de cifrado c2)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de cifrado 232 genera un elemento de cifrado c_2 que es un elemento del texto cifrado ct, como se indica en la Fórmula 180.

[Fórmula 180]

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

(S1006: Paso de transmisión de datos)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de transmisión de datos 240 transmite el texto cifrado ct que incluye el elemento de cifrado c_1 y el elemento de cifrado c_2 al dispositivo de descifrado 300. Como una cuestión de rutina, el texto cifrado ct se puede transmitir al dispositivo de descifrado 300 mediante otro método.

En resumen, en (S1001) hasta (S1005), el dispositivo de cifrado 200 ejecuta el algoritmo Enc indicado en la Fórmula 181 y de esta manera genera el texto cifrado ct. En (S1006), el dispositivo de cifrado 200 transmite el texto cifrado ct generado al dispositivo de descifrado 300.

[Fórmula 181]

$\mathsf{Enc}(\mathsf{pk},\ m \in \mathbb{G}_T, (\vec{x}_1,\ldots,\vec{x}_L) \in \mathbb{F}_q^n \times \cdots \times \mathbb{F}_q^n)$:

$\omega, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0},$

para *i = 1, …, L,*

$\vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^z,\ \sigma_t \xleftarrow{\mathsf{U}} \mathbb{F}_q,$

$\boldsymbol{c}_1 := ((\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0},\ (\sigma_t(1,t),\ \omega\vec{x}_t,\ 0^u, 0^w, \vec{\varphi}_t)_{\mathbb{B}} : t = 1,\ldots,L),$

$c_2 := g_T^{\zeta} m,\ \ \mathsf{ct} := (\boldsymbol{c}_1, c_2),$

devolver ct.

Se describirá la función y operación del dispositivo de descifrado 300.

El dispositivo de descifrado 300 incluye una unidad de adquisición de clave de descifrado 310, una unidad de recepción de datos 320, una unidad de operación de emparejamiento 350 y una unidad de cálculo de mensaje 360.

Con referencia a la Fig. 28, se describirá el proceso del algoritmo Dec que se ejecuta por el dispositivo de descifrado 300.

(S1101: Paso de adquisición de clave de descifrado)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de adquisición de clave de descifrado 310 obtiene la clave de descifrado sk_L. La unidad de adquisición de clave de descifrado 310 también obtiene el parámetro público pk generado por el dispositivo de generación de clave 100.

(S1102: Paso de recepción de datos)

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

(S1103: Paso de operación de emparejamiento)

Usando el dispositivo de procesamiento, la unidad de operación de emparejamiento 350 realiza una operación de emparejamiento indicada en la Fórmula 182 y de esta manera calcula la clave de sesión $K = g_T^{\zeta}$.

[Fórmula 182]

$$e(\boldsymbol{c}_1, \boldsymbol{k}^*_{L,\mathsf{dec}})$$

(S1104: Paso de cálculo de mensaje)

Usando el dispositivo de procesamiento, la unidad de cálculo de mensaje 360 calcula un mensaje m' (= m) dividiendo el elemento de cifrado c2 por la clave de sesión K.

En resumen, en (S1101) hasta (S1104), el dispositivo de descifrado 300 ejecuta el algoritmo Dec indicado en la Fórmula 183 y de esta manera calcula el mensaje m' (= m).

[Fórmula 183]

$\mathsf{Dec}(\mathsf{pk},\ \boldsymbol{k}^*_{L,\mathsf{dec}}, \mathsf{ct})$:

$m' := c_2 / e(\boldsymbol{c}_1, \boldsymbol{k}^*_{L,\mathsf{dec}}),$

devolver m'.

Se describirá la función y operación del dispositivo de delegación de clave 400.

El dispositivo de delegación de clave 400 incluye una unidad de adquisición de clave de descifrado 410, una unidad de entrada de información 420, una unidad de generación de clave de delegación 430 y una unidad de distribución de clave 440. La unidad de generación de clave de delegación 430 incluye una unidad de generación de número aleatorio 431, una unidad de generación de elemento de clave de nivel más bajo 432, una unidad de generación de elemento de aleatorización de nivel más bajo 433 y una unidad de generación de elemento de delegación de nivel más bajo 434.

Con referencia a la Fig. 29, se describirá el proceso del algoritmo Delegate_L que se ejecuta por el dispositivo de delegación de clave 400.

(S1201: Paso de adquisición de clave de descifrado)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de adquisición de clave de descifrado 410 obtiene la clave de descifrado sk_L. La unidad de adquisición de clave de descifrado 410 también obtiene el parámetro público pk generado por el dispositivo de generación de clave 100.

(S1202: Paso de entrada de información)

Usando el dispositivo de entrada, la unidad de entrada de información 420 toma como entrada información de predicado $\vec{v}_{L+1} := (v_{L+1,i} \ (i = 1, \ldots, n_{L+1}))$. Señalar que el atributo de una persona a la que la clave va a ser delegada se introduce como la información de predicado.

(S1203: Paso de generación de número aleatorio)

Usando el dispositivo de procesamiento, la unidad de generación de número aleatorio 431 genera números aleatorios, como se indica en la Fórmula 184.

[Fórmula 184]

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

$$\mu'_{\text{del},(\tau,\iota)},\ \mu'_{\text{ran},2,\tau},\ \phi_{\text{del},(\tau,\iota)},\ \phi_{\text{ran},2,\tau},\ \psi' \xleftarrow{\text{U}} \mathbb{F}_q,$$

$$\boldsymbol{p}^*_{\text{dec}}, \boldsymbol{p}^*_{\text{del},(\tau,\iota)}, \boldsymbol{p}^*_{\text{ran},1,j'}, \boldsymbol{p}^*_{\text{ran},2,\tau} \xleftarrow{\text{R}} \text{CoreDel}_L(\text{pk}, \text{sk}_L, v_{L+1}),$$

$$\text{donde } \text{CoreDel}_L(\text{pk}, \text{sk}_L, v_{L+1}):$$

$$\mu'_t, \xi, \alpha_j \xleftarrow{\text{U}} \mathbb{F}_q \ \text{ para } t = 1,\ldots,L+1;\ j = 1,\ldots,2L+1,$$

$$\text{devolver } \boldsymbol{p}^* := \sum_{t=1}^{L+1} \mu'_t (t\boldsymbol{b}^*_1 - \boldsymbol{b}^*_2)^{\langle t \rangle} + \xi \left(\sum_{i=1}^{n} v_{L+1,i} \boldsymbol{k}^*_{L,\text{del}(L+1,i)} \right)$$
$$+ \sum_{j=1}^{2L} \alpha_j \boldsymbol{k}^*_{L,\text{ran},1,j} + \alpha_{2L+1} \boldsymbol{k}^*_{L,\text{ran},2,L+1},$$

$$\boldsymbol{r}^*_{\text{dec}}, \boldsymbol{r}^*_{\text{ran},1,j'} \xleftarrow{\text{U}} \text{span}\langle (\boldsymbol{b}^*_{0,1+u_0+1+1}, \ldots, \boldsymbol{b}^*_{0,1+u_0+1+w_0})^{\langle 0 \rangle},$$
$$\{(\boldsymbol{b}^*_{2+n+u+1}, \ldots, \boldsymbol{b}^*_{2+n+u+w})^{\langle t \rangle}\}_{t=1,\ldots,L+1} \rangle,$$

$$\boldsymbol{r}^*_{\text{del}(\tau,\iota)}, \boldsymbol{r}^*_{\text{ran},2,\tau} \xleftarrow{\text{U}} \text{span}\langle (\boldsymbol{b}^*_{0,1+u_0+1+1}, \ldots, \boldsymbol{b}^*_{0,1+u_0+1+w_0})^{\langle 0 \rangle},$$
$$\{(\boldsymbol{b}^*_{2+n+u+1}, \ldots, \boldsymbol{b}^*_{2+n+u+w})^{\langle t \rangle}\}_{t=1,\ldots,L+1,\tau} \rangle$$

(S1204: Paso de generación de elemento de clave de nivel más bajo)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de clave de nivel más bajo 432 genera un elemento de clave de nivel más bajo $k^*_{L+1,\text{dec}}$ que es un elemento de una clave de delegación sk_{L+1}, como se indica en la Fórmula 185.

[Fórmula 185]

$$\boldsymbol{k}^*_{L+1,\text{dec}} := \boldsymbol{k}^*_{L,\text{dec}} + \boldsymbol{p}^*_{\text{dec}} + \boldsymbol{r}^*_{\text{dec}}$$

(S1205: Paso de generación de primer elemento de aleatorización de nivel más bajo)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de aleatorización de nivel más bajo 433 genera un primer elemento de aleatorización de nivel más bajo $k^*_{L+1,\text{ran},1,j'}$ que es un elemento de la clave de delegación sk_{L+1}, para cada entero j' = 1, …, 2(L+1), como se indica en la Fórmula 186.

[Fórmula 186]

$$\boldsymbol{k}^{*}_{L+1,\mathrm{ran},1,j'} := \boldsymbol{p}^{*}_{\mathrm{ran},1,j'} + \boldsymbol{r}^{*}_{\mathrm{ran},1,j'}$$

(S1206: Paso de generación de segundo elemento de aleatorización de nivel más bajo)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de aleatorización de nivel más bajo 433 genera un segundo elemento de aleatorización de nivel más bajo $k^{*}_{L+1,\mathrm{ran},2,\tau}$ que es un elemento de la clave de delegación sk_{L+1}, para cada entero τ = L+2, …, d, como se indica en la Fórmula 187.

[Fórmula 187]

$$\boldsymbol{k}^{*}_{L+1,\mathrm{ran},2,\tau} := \boldsymbol{p}^{*}_{\mathrm{ran},2,\tau} + \mu'_{\mathrm{ran},2,\tau}(\tau \boldsymbol{b}^{*}_{1} - \boldsymbol{b}^{*}_{2})^{(\tau)} + \phi_{\mathrm{ran},2,\tau}\boldsymbol{k}^{*}_{L,\mathrm{ran},2,\tau} + \boldsymbol{r}^{*}_{\mathrm{ran},2,\tau}$$

(S1207: Paso de generación de elemento de delegación de nivel más bajo)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de delegación de nivel más bajo 434 genera un elemento de delegación de nivel más bajo $k^{*}_{L+1,\mathrm{del},(\tau,\iota)}$ que es un elemento de la clave de delegación sk_{L+1}, para cada entero τ = L+2, …, d y cada entero ι = 1, …, n con respecto a cada entero τ , como se indica en la Fórmula 188.

[Fórmula 188]

$$\boldsymbol{k}^{*}_{L+1,\mathrm{del}(\tau,\iota)} := \boldsymbol{p}^{*}_{\mathrm{del}(\tau,\iota)} + \mu'_{\mathrm{del}(\tau,\iota)}(\tau \boldsymbol{b}^{*}_{1} - \boldsymbol{b}^{*}_{2})^{(\tau)} + \phi_{\mathrm{del},(\tau,\iota)}\boldsymbol{k}^{*}_{L,\mathrm{ran},2,\tau} + \psi' \boldsymbol{k}^{*}_{L,\mathrm{del}(\tau,\iota)} + \boldsymbol{r}^{*}_{\mathrm{del}(\tau,\iota)}$$

(S1208: Paso de distribución de clave)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de distribución de clave 150 distribuye la clave de delegación sk_{L+1} (clave de descifrado de nivel más bajo) que tiene, como elementos, el elemento de clave de nivel más bajo $k^{*}_{L+1,\mathrm{dec}}$, el primer elemento de aleatorización de nivel más bajo $k^{*}_{L+1,\mathrm{ran},1,j'}$, el segundo elemento de aleatorización de nivel más bajo $k^{*}_{L+1,\mathrm{ran},2,\tau}$ y el elemento de delegación de nivel más bajo $k^{*}_{L+1,\mathrm{del},(\tau,\iota)}$ al dispositivo de descifrado de nivel más bajo 300 en secreto. Como una cuestión de rutina, la clave de delegación sk_{L+1} se puede distribuir al dispositivo de descifrado de nivel más bajo 300 mediante otro método.

En resumen, en (S1201) hasta (S1207), el dispositivo de delegación de clave 400 ejecuta el algoritmo $\mathrm{Delegate}_{L}$ indicado en la Fórmula 189 y de esta manera genera la clave de delegación sk_{L+1}. En (S1208), el dispositivo de delegación de clave 400 distribuye la clave de delegación generada sk_{L+1} al dispositivo de descifrado de nivel más bajo 300.

[Fórmula 189]

$$\mathsf{Delegate}_{L}(\mathsf{pk}, \mathsf{sk}_{L}, \vec{v}_{L+1}):$$

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

$$\mu'_{\mathrm{del},(\tau,\iota)},\ \mu'_{\mathrm{ran},2,\tau},\ \phi_{\mathrm{del},(\tau,\iota)},\ \phi_{\mathrm{ran},2,\tau},\ \psi' \xleftarrow{\mathrm{U}} \mathbb{F}_{q},$$

$$\boldsymbol{p}^{*}_{\mathrm{dec}}, \boldsymbol{p}^{*}_{\mathrm{del},(\tau,\iota)}, \boldsymbol{p}^{*}_{\mathrm{ran},1,j'}, \boldsymbol{p}^{*}_{\mathrm{ran},2,\tau} \xleftarrow{\mathrm{R}} \mathsf{CoreDel}_{L}(\mathsf{pk}, \mathsf{sk}_{L}, v_{L+1}),$$

donde $\mathsf{CoreDel}_{L}(\mathsf{pk}, \mathsf{sk}_{L}, v_{L+1}):$

$$\mu'_{t}, \xi, \alpha_{j} \xleftarrow{\mathrm{U}} \mathbb{F}_{q} \text{ para } t = 1,\ldots,L+1;\ j = 1,\ldots,2L+1,$$

devolver $$\boldsymbol{p}^{*} := \sum_{t=1}^{L+1} \mu'_{t}(t\boldsymbol{b}^{*}_{1} - \boldsymbol{b}^{*}_{2})^{\langle t \rangle} + \xi\left(\sum_{i=1}^{n} v_{L+1,i}\boldsymbol{k}^{*}_{L,\mathrm{del}(L+1,i)}\right) + \sum_{j=1}^{2L} \alpha_{j}\boldsymbol{k}^{*}_{L,\mathrm{ran},1,j} + \alpha_{2L+1}\boldsymbol{k}^{*}_{L,\mathrm{ran},2,L+1},$$

$$r^*_{\mathsf{dec}}, r^*_{\mathsf{ran},1,j'} \xleftarrow{\mathsf{U}} \mathsf{span}\langle (b^*_{0,1+u_0+1+1},\ldots,b^*_{0,1+u_0+1+w_0})^{\langle 0\rangle},$$
$$\{(b^*_{2+n+u+1},\ldots,b^*_{2+n+u+w})^{\langle t\rangle}\}_{t=1,\ldots,L+1}\rangle,$$
$$r^*_{\mathsf{del}(\tau,\iota)}, r^*_{\mathsf{ran},2,\tau} \xleftarrow{\mathsf{U}} \mathsf{span}\langle (b^*_{0,1+u_0+1+1},\ldots,b^*_{0,1+u_0+1+w_0})^{\langle 0\rangle},$$
$$\{(b^*_{2+n+u+1},\ldots,b^*_{2+n+u+w})^{\langle t\rangle}\}_{t=1,\ldots,L+1,\tau}\rangle,$$

$$k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + p^*_{\mathsf{dec}} + r^*_{\mathsf{dec}},$$
$$k^*_{L+1,\mathsf{del}(\tau,\iota)} := p^*_{\mathsf{del}(\tau,\iota)} + \mu'_{\mathsf{del}(\tau,\iota)}(\tau b^*_1 - b^*_2)^{(\tau)}$$
$$+ \phi_{\mathsf{del},(\tau,\iota)} k^*_{L,\mathsf{ran},2,\tau} + \psi' k^*_{L,\mathsf{del}(\tau,\iota)} + r^*_{\mathsf{del}(\tau,\iota)},$$
$$k^*_{L+1,\mathsf{ran},1,j'} := p^*_{\mathsf{ran},1,j'} + r^*_{\mathsf{ran},1,j'},$$
$$k^*_{L+1,\mathsf{ran},2,\tau} := p^*_{\mathsf{ran},2,\tau} + \mu'_{\mathsf{ran},2,\tau}(\tau b^*_1 - b^*_2)^{(\tau)} + \phi_{\mathsf{ran},2,\tau} k^*_{L,\mathsf{ran},2,\tau} + r^*_{\mathsf{ran},2,\tau},$$
$$\mathsf{sk}_{L+1} := (k^*_{L+1,\mathsf{dec}}, \{k^*_{L+1,\mathsf{del}(\tau,\iota)}\}_{\tau=L+2,\ldots,d;\iota=1,2},$$
$$\{k^*_{L,\mathsf{ran},1,j'}, k^*_{L,\mathsf{ran},2,\tau}\}_{j'=1,\ldots,2(L+1);\tau=L+2,\ldots,d}),$$
devolver sk_{L+1}.

Como se describió anteriormente, como en los sistemas criptográficos 10 según las Realizaciones 2 y 3, en el sistema criptográfico 10 según la Realización 4, se proporcionan las partes de índice, de modo que las bases que se usan para cada categoría de atributo se pueden construir como las bases comunes (base B y base B*). Como resultado, solamente la base B y la base B* necesitan ser incluidas en un parámetro público, eliminando la necesidad de reeditar el parámetro público cuando una categoría de atributo va a ser añadida en una etapa posterior.

Como en las Realizaciones 2 y 3, para las partes de índice, se requiere que 0 sea obtenido como resultado de una operación de producto interior de las partes de índice. Por lo tanto, aunque las partes de índice bidimensional, esto es los vectores de base b^*_1 y b^*_2 y los vectores de base b_1 y b_2, se emplean en la descripción anterior, las partes de índice no están limitadas a bidimensionales y pueden ser tridimensionales o de dimensión más alta. Los valores asignados a las partes de índice no están limitados a los descritos anteriormente y se puede emplear una disposición de asignación diferente.

El esquema HIPE basado en el esquema de cifrado funcional se ha descrito anteriormente. Como se indica en la Fórmula 190 hasta la Fórmula 195, no obstante, el esquema se puede modificar a un esquema HIPE basado en el esquema de cifrado basado en atributo. Señalar que N_0 es 1 + 1 + 1 + 1 + 1 = 5 y N_1 es 2 + 2 + 8 + 2 + 2 = 16 en la Fórmula 190 hasta la Fórmula 195. Es decir, $u_0 = 1$, $w_0 = 1$, $z_0 = 1$, n = 2, u = 8, w = 2 y z = 2. Incluso en este caso, se puede probar la seguridad.

[Fórmula 190]

$\mathsf{Setup}(1^\lambda)$:

$$(\mathsf{param}, (\mathbb{B}_0, \mathbb{B}^*_0), (\mathbb{B}, \mathbb{B}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda),$$
$$\hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,3}, b_{0,5}),\ \hat{\mathbb{B}} := (b_1,\ldots,b_4, b_{15}, b_{16}),$$
$$\hat{\mathbb{B}}^*_{0,\mathsf{pk}} := b^*_{0,4},\ \hat{\mathbb{B}}^*_{0,\mathsf{sk}} := (b^*_{0,1}, b^*_{0,3}),$$
$$\hat{\mathbb{B}}^*_{\mathsf{pk}} := (b^*_1, b^*_2, b^*_{13}, b^*_{14}),\ \hat{\mathbb{B}}^*_{\mathsf{sk}} := (b^*_3, b^*_4),$$
devolver $\mathsf{pk} := (1^\lambda, \mathsf{param}, \hat{\mathbb{B}}_0, \hat{\mathbb{B}}, \hat{\mathbb{B}}^*_{0,\mathsf{pk}}, \hat{\mathbb{B}}^*_{\mathsf{pk}})$, $\mathsf{sk} := (\hat{\mathbb{B}}^*_{0,\mathsf{sk}}, \hat{\mathbb{B}}^*_{\mathsf{sk}})$.

$\mathcal{G}_{\mathrm{ob}}(1^{\lambda})$:

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

$N_0 := 5,\ N_1 := 16,$

para $t = 0, 1,$ $\mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathrm{dpvs}}(1^{\lambda}, N_t, \mathsf{param}_{\mathbb{G}}),$

$X_t := (\chi_{t,i,j})_{i,j=1,..,N_t} \xleftarrow{U} GL(N_t, \mathbb{F}_q),$

$X_t^* := (\vartheta_{t,i,j})_{i,j=1,..,N_t} := \psi \cdot (X_t^T)^{-1},$ a partir de entonces, $\vec{\chi}_{t,i}$

y $\vec{\vartheta}_{t,i}$ indican las filas de orden i de X_t y X^*_t para $i = 1, \ldots, N_t$, respectivamente,

$\boldsymbol{b}_{t,i} := (\vec{\chi}_{t,i})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \chi_{t,i,j} \boldsymbol{a}_{t,j}$ para $i = 1, \ldots, N_t,$ $\mathbb{B}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,N_t}),$

$\boldsymbol{b}^*_{t,i} := (\vec{\vartheta}_{t,i})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \vartheta_{t,i,j} \boldsymbol{a}_{t,j}$ para $i = 1, \ldots, N_t,$ $\mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,N_t}),$

$g_T := e(g,g)^{\psi},\ \mathsf{param} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,1}, g_T),$

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

[Fórmula 191]

$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, (v_1, \ldots, v_L) \in \mathbb{F}_q^L)$:

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

$\psi, \mu_{\mathsf{dec},t}, \mu_{\mathsf{ran},1,j,t}, s_{\mathsf{dec},t}, s_{\mathsf{ran},1,j,t},$

$\theta_{\mathsf{dec},t}, \theta_{\mathsf{ran},1,j,t} \xleftarrow{U} \mathbb{F}_q$ para $t = 1, \ldots, L,$

$\mu_{\mathsf{del},(\tau,\iota),t}, \mu_{\mathsf{ran},2,\tau,t}, s_{\mathsf{del},(\tau,\iota),t}, s_{\mathsf{ran},2,\tau,t},$

$\theta_{\mathsf{del},(\tau,\iota),t}, \theta_{\mathsf{ran},2,\tau,t} \xleftarrow{U} \mathbb{F}_q$ para $t = 1, \ldots, L+1,$

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

$s_{\mathsf{ran},1,j,0} := \sum_{t=1}^{L} s_{\mathsf{ran},1,j,t},\ s_{\mathsf{ran},2,\tau,0} := \sum_{t=1}^{L+1} s_{\mathsf{ran},2,\tau,t},$

$\vec{\eta}_{\mathsf{dec},t}, \vec{\eta}_{\mathsf{ran},1,j,t} \xleftarrow{U} \mathbb{F}_q^2$ para $t = 0, \ldots, L,$

$\vec{\eta}_{\mathsf{del},(\tau,\iota),t}, \vec{\eta}_{\mathsf{ran},2,\tau,t} \xleftarrow{U} \mathbb{F}_q^2$ para $t = 0, \ldots, L+1,$

[Fórmula 192]

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

$(\mu_{\mathsf{dec},t}(t,-1),\ s_{\mathsf{dec},t} + \theta_{\mathsf{dec},t} v_t,\ -\theta_{\mathsf{dec},t},\ 0^8,\ \vec{\eta}_{\mathsf{dec},t},\ 0^2)_{\mathbb{B}^*} : t = 1, \ldots, L),$

$$\boldsymbol{k}^{*}_{L,\mathsf{del},(\tau,\iota)} := (\ (-s_{\mathsf{del},(\tau,\iota),0},\ 0,\ 0,\ \eta_{\mathsf{del},(\tau,\iota),0},\ 0)_{\mathbb{B}^{*}_{0}},$$
$$(\mu_{\mathsf{del},(\tau,\iota),t}(t,-1),\ s_{\mathsf{del},(\tau,\iota),t}+\theta_{\mathsf{del},(\tau,\iota),t}v_t,\ -\theta_{\mathsf{del},(\tau,\iota),t},\ 0^{8},$$
$$\vec{\eta}_{\mathsf{del},(\tau,\iota),t},\ 0^{2})_{\mathbb{B}^{*}}:\ t=1,\ldots,L,$$
$$(\mu_{\mathsf{del},(\tau,\iota),L+1}(\tau,-1),\ \pi_{\mathsf{del},(\tau,\iota),L+1,1},\ \pi_{\mathsf{del},(\tau,\iota),L+1,2},\ 0^{8},$$
$$\vec{\eta}_{\mathsf{del},(\tau,2),L+1},\ 0^{2})_{\mathbb{B}^{*}})$$

donde, $(\pi_{\mathsf{del},(\tau,1),L+1,\iota},\ \pi_{\mathsf{del},(\tau,\iota),L+1,2}) := \begin{cases} (s_{\mathsf{del},(\tau,1),L+1}+\psi,\ 0) \text{ si } \iota=1, \\ (\quad s_{\mathsf{del},(\tau,2),L+1},\ \psi) \text{ si } \iota=2, \end{cases}$

$$\boldsymbol{k}^{*}_{L,\mathsf{ran},1,j} := (\ (-s_{\mathsf{ran},1,j,0},\ 0,\ 0,\ \eta_{\mathsf{ran},1,j,0},\ 0)_{\mathbb{B}^{*}_{0}},$$
$$(\mu_{\mathsf{ran},1,j,t}(t,-1),\ s_{\mathsf{ran},1,j,t}+\theta_{\mathsf{ran},1,j,t}v_t,\ -\theta_{\mathsf{ran},1,j,t},\ 0^{8},$$
$$\vec{\eta}_{\mathsf{ran},1,j,t},\ 0^{2})_{\mathbb{B}^{*}}:\ t=1,\ldots,L),$$
$$\boldsymbol{k}^{*}_{L,\mathsf{ran},2,\tau} := (\ (-s_{\mathsf{ran},2,\tau,0},\ 0,\ 0,\ \eta_{\mathsf{ran},2,\tau,0},\ 0)_{\mathbb{B}^{*}_{0}},$$
$$(\mu_{\mathsf{ran},2,\tau,t}(t,-1),\ s_{\mathsf{ran},2,\tau,t}+\theta_{\mathsf{ran},2,\tau,t}v_t,\ -\theta_{\mathsf{ran},2,\tau,t},\ 0^{8},$$
$$\vec{\eta}_{\mathsf{ran},2,\tau,t},\ 0^{2})_{\mathbb{B}^{*}}:\ t=1,\ldots,L,$$
$$(\mu_{\mathsf{ran},2,\tau,L+1}(\tau,-1),\ s_{\mathsf{ran},2,\tau,L+1},\ 0,\ 0^{8},\ \vec{\eta}_{\mathsf{ran},2,\tau,L+1},\ 0^{2})_{\mathbb{B}^{*}}),$$
$$\mathsf{sk}_L := (\boldsymbol{k}^{*}_{L,\mathsf{dec}},\{\boldsymbol{k}^{*}_{L,\mathsf{del}(\tau,\iota)}\}_{\tau=L+1,\ldots,d;\ \iota=1,2},$$
$$\{\boldsymbol{k}^{*}_{L,\mathsf{ran},1,j},\boldsymbol{k}^{*}_{L,\mathsf{ran},2,\tau}\}_{j=1,\ldots,2L\ ;\tau=L+1,\ldots,d}),$$

devolver sk_L.

[Fórmula 193]

$$\mathsf{Enc}(\mathsf{pk},\ m\in\mathbb{G}_T,(x_1,\ldots,x_L)\in\mathbb{F}_q^{L}):$$
$$\omega,\zeta,\varphi_0,\varphi_{\mathsf{t},1},\varphi_{\mathsf{t},2},\sigma_{\mathsf{t}} \xleftarrow{\cup} \mathbb{F}_q \text{ para } t=1,\ldots,L,$$
$$\boldsymbol{c}_1 := ((\omega,0,\zeta,0,\varphi_0)_{\mathbb{B}_0},\ (\sigma_t(1,t),\ \omega(1,x_t),\ 0^{8},0^{2},\varphi_{\mathsf{t},1},\varphi_{\mathsf{t},2})_{\mathbb{B}}:t=1,\ldots,L),$$
$$c_2 := g_T^{\zeta}m,\quad \mathsf{ct} := (\boldsymbol{c}_1,c_2),\qquad \text{devolver } \mathsf{ct}.$$

[Fórmula 194]

$$\mathsf{Dec}(\mathsf{pk},\ \boldsymbol{k}^{*}_{L,\mathsf{dec}},\mathsf{ct}):$$
$$m' := c_2 / e(\boldsymbol{c}_1,\boldsymbol{k}^{*}_{L,\mathsf{dec}}),$$
devolver m'.

[Fórmula 195]

$\mathsf{Delegate}_L(\mathsf{pk},\ \mathsf{sk}_L, v_{L+1})$:

para $j'=1,\ldots,2(L+1);\ \tau=L+2,\ldots,d; t=1,2;$

$\mu'_{\mathsf{del},(\tau,t)},\ \mu'_{\mathsf{ran},2,\tau},\ \phi_{\mathsf{del},(\tau,t)},\ \phi_{\mathsf{ran},2,\tau},\ \psi' \xleftarrow{\mathsf{U}} \mathbb{F}_q,$

$\boldsymbol{p}^*_{\mathsf{dec}}, \boldsymbol{p}^*_{\mathsf{del},(\tau,t)}, \boldsymbol{p}^*_{\mathsf{ran},1,j'}, \boldsymbol{p}^*_{\mathsf{ran},2,\tau} \xleftarrow{\mathsf{R}} \mathsf{CoreDel}_L(\mathsf{pk},\ \mathsf{sk}_L, v_{L+1}),$

donde $\mathsf{CoreDel}_L(\mathsf{pk},\ \mathsf{sk}_L, v_{L+1}): \mu'_t, \xi, \alpha_j \xleftarrow{\mathsf{U}} \mathbb{F}_q$

para $t=1,\ldots,L+1\ ; j=1,\ldots,2L+1,$

devolver $\boldsymbol{p}^* := \sum_{t=1}^{L+1} \mu'_t (t\boldsymbol{b}^*_1 - \boldsymbol{b}^*_2)^{\langle t\rangle} + \xi\left(v_{L+1}\boldsymbol{k}^*_{L,\mathsf{del}(L+1,1)} - \boldsymbol{k}^*_{L,\mathsf{del},(L+1,2)}\right)$

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

$\boldsymbol{r}^*_{\mathsf{dec}}, \boldsymbol{r}^*_{\mathsf{ran},1,j'} \xleftarrow{\mathsf{U}} \mathsf{span}\langle (\boldsymbol{b}^*_{0,4})^{\langle 0\rangle}\ , \{(\boldsymbol{b}^*_{13})^{\langle t\rangle}, (\boldsymbol{b}^*_{14})^{\langle t\rangle}\}_{t=1,\ldots,L+1}\rangle,$

$\boldsymbol{r}^*_{\mathsf{del}(\tau,t)}, \boldsymbol{r}^*_{\mathsf{ran},2,\tau} \xleftarrow{\mathsf{U}} \mathsf{span}\langle (\boldsymbol{b}^*_{0,4})^{\langle 0\rangle}\ , \{(\boldsymbol{b}^*_{13})^{\langle t\rangle}, (\boldsymbol{b}^*_{14})^{\langle t\rangle}\}_{t=1,\ldots,L+1,\tau}\rangle,$

$\boldsymbol{k}^*_{L+1,\mathsf{dec}} := \boldsymbol{k}^*_{L,\mathsf{dec}} + \boldsymbol{p}^*_{\mathsf{dec}} + \boldsymbol{r}^*_{\mathsf{dec}},$

$\boldsymbol{k}^*_{L+1,\mathsf{del}(\tau,t)} := \boldsymbol{p}^*_{\mathsf{del}(\tau,t)} + \mu'_{\mathsf{del}(\tau,t)}(\tau\boldsymbol{b}^*_1 - \boldsymbol{b}^*_2)^{(\tau)}$

$+\ \phi_{\mathsf{del},(\tau,t)}\boldsymbol{k}^*_{L,\mathsf{ran},2,\tau} + \psi'\boldsymbol{k}^*_{L,\mathsf{del}(\tau,t)} + \boldsymbol{r}^*_{\mathsf{del}(\tau,t)},$

$\boldsymbol{k}^*_{L+1,\mathsf{ran},1,j'} := \boldsymbol{p}^*_{\mathsf{ran},1,j'} + \boldsymbol{r}^*_{\mathsf{ran},1,j'},$

$\boldsymbol{k}^*_{L+1,\mathsf{ran},2,\tau} := \boldsymbol{p}^*_{\mathsf{ran},2,\tau} + \mu'_{\mathsf{ran},2,\tau}(\tau\boldsymbol{b}^*_1 - \boldsymbol{b}^*_2)^{(\tau)} + \ \phi_{\mathsf{ran},2,\tau}\boldsymbol{k}^*_{L,\mathsf{ran},2,\tau} + \boldsymbol{r}^*_{\mathsf{ran},2,\tau}$

$\mathsf{sk}_{L+1} := (\boldsymbol{k}^*_{L+1,\mathsf{dec}}, \{\boldsymbol{k}^*_{L+1,\mathsf{del}(\tau,t)}\}_{\tau=L+2,\ldots,d;t=1,2},$

$\{\boldsymbol{k}^*_{L,\mathsf{ran},1,j'}, \boldsymbol{k}^*_{L,\mathsf{ran},2,\tau}\}_{j'=1,\ldots,2(L+1);\tau=L+2,\ldots,d}),$

devolver sk_{L+1}.

Realización 5

Esta realización describe un esquema de firma. En particular, esta realización describe un esquema de firma basado en el esquema CP-FE descrito en la Realización 3.

En primer lugar, se describirá la construcción del esquema de firma.

En segundo lugar, se describirá la configuración de un sistema criptográfico 10 que implementa el esquema de firma.

En tercer lugar, se describirá en detalle el esquema de firma.

<1. Construcción de esquema de firma>

El esquema de firma consta de cuatro algoritmos: Setup, KeyGen, Sig y Ver.

(Setup)

Un algoritmo Setup es un algoritmo probabilístico que toma como entrada un parámetro de seguridad λ y saca un parámetro público pk y una clave maestra sk.

(KeyGen)

Un algoritmo KeyGen es un algoritmo probabilístico que toma como entrada un conjunto de atributos $\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in F_q^n, 1 \leq t \leq d\}$, el parámetro público pk y la clave maestra sk y saca una clave de firma sk_Γ.

(Sig)

Un algoritmo Sig es un algoritmo probabilístico que toma como entrada un mensaje m, una clave de firma sk_Γ, una estructura de acceso S := (M, ρ) y el parámetro público pk y saca datos de firma sig.

(Ver)

Un algoritmo Ver es un algoritmo que toma como entrada el mensaje m, la estructura de acceso S := (M, ρ), los datos de firma sig y el parámetro público pk y saca un valor “1” que indica el éxito de verificación de la firma o un valor “0” que indica un fallo de verificación de la firma.

<2. Configuración de sistema criptográfico 10 que implementa un esquema de firma>

La Fig. 30 es un diagrama de configuración del sistema criptográfico 10 que implementa el esquema de firma según la Realización 5.

El sistema criptográfico 10 incluye un dispositivo de generación de clave 100, un dispositivo de firma 500 y un dispositivo de verificación 600.

El dispositivo de generación de clave 100 ejecuta el algoritmo Setup tomando como entrada un parámetro de seguridad λ y de esta manera genera un parámetro público pk y una clave maestra sk. Entonces, el dispositivo de generación de clave 100 publica el parámetro público pk generado. El dispositivo de generación de clave 100 también ejecuta el algoritmo KeyGen tomando como entrada un conjunto de atributos Γ y de esta manera genera una clave de firma sk_Γ y distribuye la clave de firma sk_Γ al dispositivo de firma 500 en secreto.

El dispositivo de firma 500 ejecuta el algoritmo Sig tomando como entrada un mensaje m, una estructura de acceso S, el parámetro público pk y la clave de firma sk_Γ y de esta manera genera información de firma $\vec{s}^*$. El dispositivo de firma 500 transmite la información de firma $\vec{s}^*$ generada, el mensaje m y la estructura de acceso S al dispositivo de verificación 600.

El dispositivo de verificación 600 ejecuta el algoritmo Ver tomando como entrada la información de firma $\vec{s}^*$, el mensaje m, la estructura de acceso S y el parámetro público pk y saca un valor “1” o un valor “0”.

<3. Esquema de firma en detalle>

Con referencia a las Fig. 31 a 37, se describirá el esquema de firma y se describirá la función y operación del sistema criptográfico 10 que implementa el esquema de firma.

La Fig. 31 es un diagrama de configuración del dispositivo de generación de clave 100 según la Realización 5. La Fig. 32 es un diagrama de configuración del dispositivo de firma 500 según la Realización 5. La Fig. 33 es un diagrama de configuración del dispositivo de verificación 600 según la Realización 5.

Las Fig. 34 y 35 muestran diagramas de flujo que ilustran la operación del dispositivo de generación de clave 100. La Fig. 34 es un diagrama de flujo que ilustra el proceso del algoritmo Setup. La Fig. 35 es un diagrama de flujo que ilustra el proceso del algoritmo KeyGen. La Fig. 36 es un diagrama de flujo que ilustra la operación del dispositivo de firma 500 y que ilustra el proceso del algoritmo Sig. La Fig. 37 es un diagrama de flujo que ilustra la operación del dispositivo de verificación 600 y que ilustra el proceso del algoritmo Ver.

En la siguiente descripción, $H := (KH_\lambda , H_{hk}^{\lambda,D})$ es una función de comprobación aleatoria resistente a colisión (ver la Literatura no de Patente 30). Una función de comprobación aleatoria resistente a colisión es una función de comprobación aleatoria para la que es difícil encontrar dos entradas que trocean a la misma salida.

Específicamente, una familia H de función de comprobación aleatoria resistente a colisión asociada con el algoritmo G_{bpg} y un polinomio poli(λ) especifican dos ítems:

1. Una familia de espacios de clave se indexa por λ. Cada espacio de clave tal es un espacio de probabilidad en cadenas de bits indicadas por KH_λ. Debe existir un algoritmo de polinomio-tiempo probabilístico cuya distribución de salida en la entrada 1^λ es igual a KH_λ.

2. Una familia de funciones de comprobación aleatoria se indexa por λ, hk seleccionada aleatoriamente a partir de KH_λ y $D := \{0, 1\}^{poli(\lambda)}$, donde cada función $H_{hk}^{\lambda,D}$ tal correlaciona un elemento de D a un elemento de F_q^x con q que es el primer elemento de salida $param_G$ de algoritmo $G_{bpg}(1^\lambda)$. Debe existir un algoritmo polinomio-tiempo determinístico que saca $H_{hk}^{\lambda,D}(d)$ en la entrada 1^λ, hk y $d \in D$.

Se describirán la función y operación del dispositivo de generación de clave 100.

El dispositivo de generación de clave 100 incluye una unidad de generación de clave maestra 110, una unidad de almacenamiento de clave maestra 120, una unidad de entrada de información 130, una unidad de generación de clave de descifrado 140 y una unidad de distribución de clave 150. La unidad de generación de clave de descifrado 140 incluye una unidad de generación de número aleatorio 143 y una unidad de generación de elemento de clave 144.

Con referencia a la Fig. 34, se describirá el proceso del algoritmo Setup.

(S1301) es básicamente el mismo que (S101) en la Realización 2 mostrada en la Fig. 9. Hay diferencias, no obstante, en que el proceso de (4) hasta (8) se ejecuta para t = 0, 1 y d+1 y que N_0 es $1 + u_0 + w_0 + z_0$. Señalar que N_{d+1} es $2 + u_{d+1} + w_{d+1} + z_{d+1}$ y que u_{d+1}, w_{d+1} y z_{d+1} son enteros de 1 o más.

(S1302: Paso de generación de clave de comprobación aleatoria)

Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 calcula la Fórmula 196 y de esta manera genera una clave de comprobación aleatoria hk aleatoriamente.

[Fórmula 196]

$$hk \xleftarrow{R} KH_{\lambda}$$

(S1303: Paso de generación de parámetro público)

Usando el dispositivo de procesamiento, la unidad de generación de clave maestra 110 genera una subbase $B\hat{}_0$ de la base B_0, una subbase $B\hat{}$ de la base B, una subbase $B\hat{}_{d+1}$ de la base B_{d+1}, una subbase $B\hat{}^*_0$ de la base B^*_0, una subbase $B\hat{}^*$ de la base B^* y una subbase $B\hat{}^*_{d+1}$ de la base B^*_{d+1}, como se indica en la Fórmula 197, las bases B_0, B, B_{d+1}, B^*_0, $B\hat{}^*$ y B^*_{d+1} que se han generado en (S1301).

[Fórmula 197]

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

$$\hat{\mathbb{B}} := (b_1, \ldots, b_{2+n}, b_{2+n+u+w+1}, \ldots, b_{2+n+u+w+z}),$$

$$\hat{\mathbb{B}}_{d+1} := (b_{d+1,1}, b_{d+1,2}, b_{d+1,2+u_{d+1}+w_{d+1}+1}, \ldots, b_{d+1,2+u_{d+1}+w_{d+1}+z_{d+1}}),$$

$$\hat{\mathbb{B}}_0^* := (b^*_{0,1+u_0+1}, \ldots, b_{0,1+u_0+w_0}),$$

$$\hat{\mathbb{B}}^* := (b_1^*, \ldots, b_{2+n}^*, b_{2+n+u+1}^*, \ldots, b_{2+n+u+w}^*),$$

$$\hat{\mathbb{B}}_{d+1}^* := (b^*_{d+1,1}, b^*_{d+1,2}, b^*_{d+1,2+u_{d+1}+1}, \ldots, b^*_{d+1,2+u_{d+1}+w_{d+1}})$$

La unidad de generación de clave maestra 110 genera un parámetro público pk poniendo juntos la subbase $B\hat{}_0$, la subbase $B\hat{}$, la subbase $B\hat{}_{d+1}$, la subbase $B\hat{}^*_0$, la subbase $B\hat{}^*$ y la subbase $B\hat{}^*_{d+1}$ generadas, el parámetro de seguridad λ (1^{λ}) introducido en (S1301), el param generado en (S1301) y la clave de comprobación aleatoria hk generada en (S1302).

(S1304: Paso de generación de clave maestra)

La unidad de generación de clave maestra 110 genera una clave maestra sk que se constituye por un vector de base $b^*_{0,1}$ de la base $B\hat{}^*_0$.

(S1305: Paso de almacenamiento de clave maestra)

La unidad de almacenamiento de clave maestra 120 almacena el parámetro público pk generado en (S1303) en el dispositivo de almacenamiento. La unidad de almacenamiento de clave maestra 120 también almacena la clave maestra sk generada en (S1304) en el dispositivo de almacenamiento.

En resumen, en (S1301) hasta (S1304), el dispositivo de generación de clave 100 ejecuta el algoritmo Setup indicado en la Fórmula 198 y de esta manera genera el parámetro público pk y la clave maestra sk. En (S1305), el

dispositivo de generación de clave 100 almacena el parámetro público pk y la clave maestra sk generados en el dispositivo de almacenamiento.

El parámetro público se publica a través de la red, por ejemplo y se pone a disposición del dispositivo de firma 500 y del dispositivo de verificación 600.

[Fórmula 198]

$$\begin{aligned}
&\mathsf{Setup}(1^{\lambda})\\
&\quad \mathsf{hk} \xleftarrow{R} \mathrm{KH}_{\lambda},\\
&\quad (\mathsf{param},(\mathbb{B}_0,\mathbb{B}_0^*),(\mathbb{B},\mathbb{B}^*),(\mathbb{B}_{d+1},\mathbb{B}_{d+1}^*)) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}(1^{\lambda}),\\
&\quad \hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,1+u_0+w_0+1}, \ldots, b_{0,1+u_0+w_0+z_0}),\\
&\quad \hat{\mathbb{B}} := (b_1, \ldots, b_{2+n}, b_{2+n+u+w+1}, \ldots, b_{2+n+u+w+z}),\\
&\quad \hat{\mathbb{B}}_{d+1} := (b_{d+1,1}, b_{d+1,2}, b_{d+1,2+u_{d+1}+w_{d+1}+1}, \ldots, b_{d+1,2+u_{d+1}+w_{d+1}+z_{d+1}}),\\
&\quad \hat{\mathbb{B}}_0^* := (b_{0,1+u_0+1}^*, \ldots, b_{0,1+u_0+w_0}),\\
&\quad \hat{\mathbb{B}}^* := (b_1^*, \ldots, b_{2+n}^*, b_{2+n+u+1}^*, \ldots, b_{2+n+u+w}^*),\\
&\quad \hat{\mathbb{B}}_{d+1}^* := (b_{d+1,1}^*, b_{d+1,2}^*, b_{d+1,2+u_{d+1}+1}^*, \ldots, b_{d+1,2+u_{d+1}+w_{d+1}}^*),\\
&\quad \mathsf{sk} := b_{0,1}^*,\\
&\quad \mathsf{pk} := (1^{\lambda}, \mathsf{hk}, \mathsf{param}, \hat{\mathbb{B}}_0, \hat{\mathbb{B}}, \hat{\mathbb{B}}_{d+1}, \hat{\mathbb{B}}_0^*, \hat{\mathbb{B}}^*, \hat{\mathbb{B}}_{d+1}^*).\\
&\quad \text{devolver } \mathsf{sk}, \mathsf{pk}.
\end{aligned}$$

Con referencia a la Fig. 35, se describirá el proceso del algoritmo KeyGen.

(S1401: Paso de entrada de información)

Usando el dispositivo de entrada, la unidad de entrada de información 130 toma como entrada un conjunto de atributos $\Gamma := \{(t, \vec{x}_t := (x_{t,1}, \ldots, x_{t,n} \in F_q^n)) \mid 1 \leq t \leq d\}$. Señalar que la información de atributo del usuario de una clave de firma sk_Γ se fija en el conjunto de atributos Γ, por ejemplo.

(S1402: Paso de generación de número aleatorio)

Usando el dispositivo de procesamiento, la unidad de generación de número aleatorio 143 genera números aleatorios, como se indica en la Fórmula 199.

[Fórmula 199]

$$\begin{aligned}
&\delta \xleftarrow{U} \mathbb{F}_q^{\times},\\
&\vec{\varphi}_0 := \varphi_{0,1}, \ldots, \varphi_{0,w_0} \xleftarrow{U} \mathbb{F}_q^{w_0},\\
&\vec{\varphi}_t := \varphi_{t,1}, \ldots, \varphi_{t,w} \xleftarrow{U} \mathbb{F}_q^{w} \text{ para } t = 1, \ldots, d,\\
&\vec{\varphi}_{d+1,1} := \varphi_{d+1,1,1}, \ldots, \varphi_{d+1,1,w_{d+1}} \xleftarrow{U} \mathbb{F}_q^{w_{d+1}},\\
&\vec{\varphi}_{d+1,2} := \varphi_{d+1,2,1}, \ldots, \varphi_{d+1,2,w_{d+1}} \xleftarrow{U} \mathbb{F}_q^{w_{d+1}}
\end{aligned}$$

(S1403: Paso de generación de elemento de clave)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de clave 144 genera un elemento k^*_0 de la clave de firma sk_Γ, como se indica en la Fórmula 200.

[Fórmula 200]

$$k_0^* := (\delta, \overbrace{0^{u_0}}^{u_0}, \overbrace{\vec{\varphi}_0}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*}$$

Usando el dispositivo de procesamiento, la unidad de generación de elemento de clave 144 también genera un elemento k^*_t de la clave de firma sk_Γ para cada entero t incluido en el conjunto de atributos Γ, como se indica en la Fórmula 201.

[Fórmula 201]

$$k_t^* := (\overbrace{\delta(1, t), \delta\vec{x}_t}^{2+n}, \overbrace{0^u}^{u}, \overbrace{\vec{\varphi}_t}^{w}, \overbrace{0^z}^{z})_{\mathbb{B}^*} \text{ para } (t, \vec{x}_t) \in \Gamma$$

Usando el dispositivo de procesamiento, la unidad de generación de elemento de clave 144 también genera los elementos k^*_{d+1}, k^*_{d+2} de la clave de firma sk_Γ, como se indica en la Fórmula 202.

[Fórmula 202]

$$k_{d+1,1}^* := (\overbrace{\delta(1, 0)}^{2}, \overbrace{0^{u_{d+1}}}^{u_{d+1}}, \overbrace{\vec{\varphi}_{d+1,1}}^{w_{d+1}}, \overbrace{0^{z_{d+1}}}^{z_{d+1}})_{\mathbb{B}_{d+1}^*},$$

$$k_{d+1,2}^* := (\overbrace{\delta(0, 1)}^{2}, \overbrace{0^{u_{d+1}}}^{u_{d+1}}, \overbrace{\vec{\varphi}_{d+1,2}}^{w_{d+1}}, \overbrace{0^{z_{d+1}}}^{z_{d+1}})_{\mathbb{B}_{d+1}^*}$$

(S1404: Paso de distribución de clave)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de distribución de clave 150 distribuye la clave de firma sk_Γ que tiene, como elementos, el conjunto de atributos Γ introducido en (S1401) y k^*_0, k^*_t, k^*_{d+1} y k^*_{d+2} generados en (S1403) al dispositivo de firma 500 en secreto. Como una cuestión de rutina, la clave de firma sk_Γ se puede distribuir al dispositivo de firma 500 mediante otro método.

En resumen, en (S1401) hasta (S1403), el dispositivo de generación de clave 100 ejecuta el algoritmo KeyGen indicado en la Fórmula 203 y de esta manera genera la clave de firma sk_Γ. En (S1404), el dispositivo de generación de clave 100 distribuye la clave de firma sk_Γ generada al dispositivo de firma 500.

[Fórmula 203]

$$\text{KeyGen}(\text{pk}, \text{sk}, \Gamma := \{(t, \vec{x}_t := (x_{t,1}, ..., x_{t,n}) \in \mathbb{F}_q^n \setminus \{\vec{0}\}) \mid 1 \le t \le d\})$$

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

$$\vec{\varphi}_0 \xleftarrow{U} \mathbb{F}_q^{w_0},$$

$$\vec{\varphi}_t \xleftarrow{U} \mathbb{F}_q^w \text{ para } t = 1, ..., d,$$

$$\vec{\varphi}_{d+1,1}, \vec{\varphi}_{d+1,2} \xleftarrow{U} \mathbb{F}_q^{w_{d+1}},$$

$$k_0^* := (\delta, \overbrace{0^{u_0}}^{u_0}, \overbrace{\vec{\varphi}_0}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*},$$

$$k_t^* := (\overbrace{\delta(1, t), \delta\vec{x}_t}^{2+n}, \overbrace{0^u}^{u}, \overbrace{\vec{\varphi}_t}^{w}, \overbrace{0^z}^{z})_{\mathbb{B}^*}$$

$$\text{para } (t, \vec{x}_t) \in \Gamma,$$

$$k^*_{d+1,1} := (\overbrace{\delta(1,0)}^{2}, \overbrace{0^{u_{d+1}}}^{u_{d+1}}, \overbrace{\vec{\varphi}_{d+1,1}}^{w_{d+1}}, \overbrace{0^{z_{d+1}}}^{z_{d+1}})_{\mathbb{B}^*_{d+1}},$$

$$k^*_{d+1,2} := (\overbrace{\delta(0,1)}^{2}, \overbrace{0^{u_{d+1}}}^{u_{d+1}}, \overbrace{\vec{\varphi}_{d+1,2}}^{w_{d+1}}, \overbrace{0^{z_{d+1}}}^{z_{d+1}})_{\mathbb{B}^*_{d+1}},$$

$$T := \{0,(d+1,1),(d+1,2)\} \cup \{t \,|\, 1 \le t \le d, (t,\vec{x}_t) \in \Gamma\},$$

devolver $\mathsf{sk}_\Gamma := (\Gamma, \{k^*_t\}_{t\in T})$.

Se describirá la función y operación del dispositivo de firma 500.

El dispositivo de firma 500 incluye una unidad de adquisición de clave de firma 510, una unidad de entrada de información 520, una unidad de cálculo de coeficiente complementario 530, una unidad de generación de datos de firma 540 y una unidad de transmisión de datos 550. La unidad de generación de datos de firma 540 incluye una unidad de generación de número aleatorio 541 y una unidad de generación de elemento de firma 542.

Con referencia a la Fig. 36, se describirá el proceso del algoritmo Sig.

(S1501: Paso de adquisición de clave de firma)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de adquisición de clave de firma 510 obtiene la clave de firma sk_Γ generada por el dispositivo de generación de clave 100. La unidad de adquisición de clave de firma 510 también obtiene el parámetro público pk generado por el dispositivo de generación de clave 100.

(S1502: Paso de entrada de información)

Usando el dispositivo de entrada, la unidad de entrada de información 520 toma como entrada una estructura de acceso S := (M, ρ). Señalar que una matriz M de la estructura de acceso S va a ser fijada según las condiciones de un sistema que se implementa.

Usando el dispositivo de entrada, la unidad de entrada de información 520 también toma como entrada un mensaje m al que va a ser unido una firma.

(S1503: Paso de cálculo de programa de tramo)

Usando el dispositivo de procesamiento, la unidad de cálculo de coeficiente complementario 530 comprueba si la estructura de acceso S introducida en (S1502) acepta o no el conjunto de atributos Γ incluido en la clave de firma sk_Γ obtenida en (S1501).

El método para comprobar si la estructura de acceso acepta o no el conjunto de atributos es el mismo que el descrito en “5. Concepto para implementar cifrado funcional en la Realización 1”.

Si la estructura de acceso S acepta el conjunto de atributos Γ (aceptar en S1503), la unidad de cálculo de coeficiente complementario 530 avanza el proceso a (S1504). Si la estructura de acceso S rechaza el conjunto de atributos Γ (rechazar en S1503), la unidad de cálculo de coeficiente complementario 530 finaliza el proceso.

(S1504: Paso de cálculo de coeficiente complementario)

Usando el dispositivo de procesamiento, la unidad de cálculo de coeficiente complementario 530 calcula 1 y una constante (coeficiente complementario) α_i para cada entero i incluido en I de manera que se satisface la Fórmula 204.

[Fórmula 204]

$$\sum_{i\in I} \alpha_i M_i := \vec{1}$$

$$\text{e } I \subseteq \{i \in \{1,\ldots,L\} \,|\, [\rho(i) = (t,\vec{v}_i) \wedge (t,\vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t = 0] \vee [\rho(i) = \neg(t,\vec{v}_i) \wedge (t,\vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t \neq 0]\}$$

(S1505: Paso de generación de número aleatorio)

Usando el dispositivo de procesamiento, la unidad de generación de número aleatorio 541 genera números aleatorios, como se indica en la Fórmula 205.

[Fórmula 205]

$$\xi \xleftarrow{U} \mathbb{F}_q^{\times},$$
$$(\beta_i) \xleftarrow{U} \{(\beta_1,\ldots,\beta_L) \mid \textstyle\sum_{i=1}^{L} \beta_i M_i = \vec{0}\}$$

(S1506: Paso de generación de elemento de firma)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de firma 542 genera un elemento de firma s^*_0 que es un elemento de datos de firma sig, como se indica en la Fórmula 206.

[Fórmula 206]

$$s_0^* := \xi k_0^* + r_0^*$$

Señalar que r^*_0 se define por la Fórmula 207 (ver la Fórmula 110 hasta la Fórmula 112 y explicaciones de las mismas).

[Fórmula 207]

$$r_0^* \xleftarrow{U} \mathrm{span}\left\langle b^*_{0,1+u_0+1},\ldots,b^*_{0,1+u_0+w_0}\right\rangle$$

Usando el dispositivo de procesamiento, la unidad de generación de elemento de firma 542 también genera un elemento de firma s^*_i que es un elemento de datos de firma sig para cada entero i = 1, …, L, como se indica en la Fórmula 208.

[Fórmula 208]

$$s_i^* := \gamma_i \cdot \xi k_t^* + \textstyle\sum_{t=1}^{n} y_{i,t} \cdot b^*_{t,t} + r_i^*$$, para $1 \leq i \leq L$

Señalar que r^*_i se define por la Fórmula 209.

[Fórmula 209]

$$r_i^* \xleftarrow{U} \mathrm{span}\left\langle b^*_{t,2+n+u+1},\ldots,b^*_{t,2+n+u+w}\right\rangle$$

Señalar que γ_i e $\vec{y}_i := (y_{i,i'}$ (i' = 1, …, n) se definen por la Fórmula 210.

[Fórmula 210]

$\gamma_i, \vec{y}_i := (y_{i,1},\ldots,y_{i,n})$ se definen como

si $i \in I \wedge \rho(i) = (t, \vec{v}_i)$,

$$\gamma_i := \alpha_i,$$
$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \mid \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},$$

si $i \in I \wedge \rho(i) = \neg(t, \vec{v}_i)$,

$$\gamma_i := \frac{\alpha_i}{\vec{v}_i \cdot \vec{x}_t},$$
$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \mid \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

si $i \notin I \wedge \rho(i) = (t, \vec{v}_i)$,

$\gamma_i := 0$,

$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\}$,

si $i \notin I \wedge \rho(i) = \neg(t, \vec{v}_i)$,

$\gamma_i := 0$,

$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\}$

Usando el dispositivo de procesamiento, la unidad de generación de elemento de firma 542 también genera un elemento de firma s^*_{L+1} que es un elemento de los datos de firma sig, como se indica en la Fórmula 211.

[Fórmula 211]

$$s^*_{L+1} := \xi(k^*_{d+1,1} + \mathsf{H}^{\lambda,D}_{hk}(m \| \mathbb{S}) \cdot k^*_{d+1,2}) + r^*_{L+1}$$

Señalar que r^*_{L+1} se define por la Fórmula 212.

$$r^*_{L+1} \xleftarrow{U} \mathrm{span}\left\langle b^*_{d+1,2+u_{d+1}+1}, \ldots, b^*_{d+1,2+u_{d+1}+w_{d+1}} \right\rangle$$

(S1507: Paso de transmisión de datos)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de transmisión de datos 550 transmite los datos de firma sig que incluyen el elemento de firma s^*_0, el elemento de firma s^*_i (i = 1, …, L), el elemento de firma s^*_{L+1}, el mensaje m y la estructura de acceso S := (M, ρ) al dispositivo de verificación 600. Como una cuestión de rutina, los datos de firma sig se pueden transmitir al dispositivo de verificación 600 mediante otro método.

En resumen, en (S1501) hasta (S1506), el dispositivo de firma 500 ejecuta el algoritmo Sig indicado en la Fórmula 213 y de esta manera genera los datos de firma sig. En (S1507), el dispositivo de firma 500 transmite los datos de firma sig generados al dispositivo de verificación 600.

[Fórmula 213]

$\mathsf{Sig}(\mathsf{pk}, \mathsf{sk}_\Gamma, m, \mathbb{S} := (M, \rho))$:

Si $\mathbb{S} := (M, \rho)$ acepta $\Gamma := \{(t, \vec{x}_t)\}$,

entonces calcular I y $\{\alpha_i\}_{i \in I}$ de manera que

$$\sum_{i \in I} \alpha_i M_i := \vec{1}$$

e $I \subseteq \{i \in \{1, \ldots, L\} \,|\, [\rho(i) = (t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t = 0]$
$\vee [\rho(i) = \neg(t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t \neq 0]\}$,

$$\xi \xleftarrow{U} \mathbb{F}_q^\times, \quad (\beta_i) \xleftarrow{U} \left\{(\beta_1, \ldots, \beta_L) \,\middle|\, \sum_{i=1}^{L} \beta_i M_i = \vec{0}\right\},$$

$$s^*_0 := \xi k^*_0 + r^*_0, \quad \text{donde } r^*_0 \xleftarrow{U} \mathrm{span}\left\langle b^*_{0,1+u_0+1}, \ldots, b^*_{0,1+u_0+w_0} \right\rangle,$$

$$s^*_i := \gamma_i \cdot \xi k^*_t + \sum_{\iota=1}^{n} y_{i,\iota} \cdot b^*_{t,\iota} + r^*_i, \text{ para } 1 \le i \le L,$$

donde $r^*_i \xleftarrow{U} \mathrm{span}\left\langle b^*_{t,2+n+u+1}, \ldots, b^*_{t,2+n+u+w} \right\rangle$,

y $\gamma_i, \vec{y}_i := (y_{i,1}, \ldots, y_{i,n})$ se define como

$$\text{si } i \in I \wedge \rho(i) = (t, \vec{v}_i),\ \ \gamma_i := \alpha_i,\ \ \ \vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},$$

$$\text{si } i \in I \wedge \rho(i) = \neg(t, \vec{v}_i),\ \ \gamma_i := \frac{\alpha_i}{\vec{v}_i \cdot \vec{x}_t},$$

$$\vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

$$\text{si } i \notin I \wedge \rho(i) = (t, \vec{v}_i),\ \ \gamma_i := 0,\ \ \vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},$$

$$\text{si } i \notin I \wedge \rho(i) = \neg(t, \vec{v}_i),\ \ \gamma_i := 0,$$

$$\vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

$$s^*_{L+1} := \xi(k^*_{d+1,1} + \mathsf{H}^{\lambda,D}_{hk}(m \| \mathbb{S}) \cdot k^*_{d+1,2}) + r^*_{L+1},$$

$$\text{donde } r^*_{L+1} \xleftarrow{\cup} \text{span}\left\langle b^*_{d+1,2+u_{d+1}+1}, \ldots, b^*_{d+1,2+u_{d+1}+w_{d+1}} \right\rangle,$$

$$\text{devolver } \vec{s}^* := (s^*_0, \ldots, s^*_{L+1}).$$

Se describirá la función y operación del dispositivo de verificación 600.

El dispositivo de verificación 600 incluye una unidad de adquisición de parámetro público 610, una unidad de recepción de datos 620, una unidad de generación de datos de verificación 630 y una unidad de operación de emparejamiento 640. La unidad de generación de datos de verificación 630 incluye una unidad de generación de vector f 631, una unidad de generación de vector s 632, una unidad de generación de número aleatorio 633 y una unidad de generación de elemento de verificación 634.

Con referencia a la Fig. 37, se describirá el proceso del algoritmo Ver.

(S1601: Paso de adquisición de parámetro público)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de adquisición de parámetro público 610 obtiene el parámetro público pk generado por el dispositivo de generación de clave 100.

(S1602: Paso de recepción de datos de firma)

Usando el dispositivo de comunicación y a través de la red, por ejemplo, la unidad de recepción de datos 620 recibe los datos de firma sig transmitidos por el dispositivo de firma 500.

(S1603: Paso de generación de vector f)

Usando el dispositivo de procesamiento, la unidad de generación de vector f 631 genera aleatoriamente un vector $\vec{f}$ que tiene r piezas de elementos, como se indica en la Fórmula 214.

[Fórmula 214]

$$\vec{f} \xleftarrow{\cup} \mathbb{F}_q^r$$

(S1604: Paso de generación de vector s)

Usando el dispositivo de procesamiento y en base a la matriz M (L filas x r columnas) de la estructura de acceso S incluida en los datos de firma sig recibidos en (S1602) y el vector $\vec{f}$ que tiene r piezas de elementos generados en (S1603), la unidad de generación de vector s 632 genera un vector $\vec{s}^{\mathrm{T}}$, como se indica en la Fórmula 215.

[Fórmula 215]

$$\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$$

Usando el dispositivo de procesamiento y en base al vector $\vec{f}$ generado en (S1603), la unidad de generación de vector s 632 también genera un valor s_0, como se indica en la Fórmula 216. Señalar que $\vec{1}$ es un vector que tiene un valor de 1 en todos sus elementos.

[Fórmula 216]

$$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$$

(S1605: Paso de generación de número aleatorio)

Usando el dispositivo de procesamiento, la unidad de generación de número aleatorio 633 genera números aleatorios, como se indica en la Fórmula 217.

[Fórmula 217]

$$\vec{\eta}_0 := \eta_{0,1},\ldots,\eta_{0,z_0} \xleftarrow{\mathrm{U}} \mathbb{F}_q^{z_0},$$

$$\vec{\eta}_{L+1} := \eta_{L+1,1},\ldots,\eta_{L+1,z_{d+1}} \xleftarrow{\mathrm{U}} \mathbb{F}_q^{z_{d+1}},$$

$$\theta_{L+1}, s_{L+1} \xleftarrow{\mathrm{U}} \mathbb{F}_q,$$

para $1 \leq i \leq L$,

si $\rho(i) = (t, \vec{v}_i)$ $\mu_i,\ \theta_i \xleftarrow{\mathrm{U}} \mathbb{F}_q, \vec{\eta}_i \xleftarrow{\mathrm{U}} \mathbb{F}_q^z,$

si $\rho(i) = \neg(t, \vec{v}_i)$ $\mu_i \xleftarrow{\mathrm{U}} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\mathrm{U}} \mathbb{F}_q^z$

(S1606: Paso de generación de elemento de verificación)

Usando el dispositivo de procesamiento, la unidad de generación de elemento de verificación 634 genera un elemento de verificación c_0 que es un elemento de una clave de verificación, como se indica en la Fórmula 218.

[Fórmula 218]

$$c_0 := (-s_0 - s_{L+1}, \overbrace{0^{u_0}}^{u_0}, \overbrace{0^{w_0}}^{w_0}, \overbrace{\vec{\eta}_0}^{z_0})_{\mathbb{B}_0}$$

Usando el dispositivo de procesamiento, la unidad de generación de elemento de verificación 634 también genera un elemento de verificación c_i que es un elemento de la clave de verificación para cada entero i = 1, …, L, como se indica en la Fórmula 219.

[Fórmula 219]

para $1 \leq i \leq L$,

si $\rho(i) = (t, \vec{v}_i)$

si $s_i^* \notin \mathbb{V}_t$, devolver 0

de otro modo $c_i := (\overbrace{\mu_i(t, -1),\ s_i e_1 + \theta_i \vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\eta}}^{z})_{\mathbb{B}},$

si $\rho(i) = \neg(t, \vec{v}_i)$

si $s_i^* \notin \mathbb{V}_t$, devolver 0,

de otro modo $c_i := (\overbrace{\mu_i(t, -1), s_i \vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\eta}_i}^{z})_{\mathbb{B}}$

Usando el dispositivo de procesamiento, la unidad de generación de elemento de verificación 634 también genera un elemento de verificación c_{L+1} que es un elemento de la clave de verificación, como se indica en la Fórmula 220.

[Fórmula 220]

$$c_{L+1} := (\overbrace{s_{L+1} - \theta_{L+1} \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m \| \mathbb{S}), \theta_{L+1}}^{2}, \overbrace{0^{u_{d+1}}}^{u_{d+1}},$$
$$\overbrace{0^{w_{d+1}}}^{w_{d+1}}, \overbrace{\vec{\eta}_{L+1}}^{z_{d+1}})_{\mathbb{B}_{d+1}}$$

(S1607: Paso de primera operación de emparejamiento)

Usando el dispositivo de procesamiento, la unidad de operación de emparejamiento 640 calcula una operación de emparejamiento e ($b_{0,1}$, s^*_0).

Si el resultado de calcular la operación de emparejamiento e ($b_{0,1}$, s^*_0) es un valor 1, la unidad de operación de emparejamiento 640 saca un valor 0 que indica un fallo de verificación de la firma y finaliza el proceso. Si el resultado de calcular la operación de emparejamiento e ($b_{0,1}$, s^*_0) es distinto de un valor 1, la unidad de operación de emparejamiento 640 avanza el proceso a S1608.

(S1608: Paso de segunda operación de emparejamiento)

Usando el dispositivo de procesamiento, la unidad de operación de emparejamiento 640 calcula una operación de emparejamiento indicada en la Fórmula 221.

[Fórmula 221]

$$\prod_{i=0}^{L+1} e(c_i, s_i^*)$$

Si el resultado de calcular la operación de emparejamiento en la Fórmula 221 es un valor 1, la unidad de operación de emparejamiento 640 saca un valor 1 que indica el éxito de la verificación de la firma. Si el resultado es cualquier otro valor, la unidad de operación de emparejamiento 640 saca un valor 0 que indica un fallo de verificación de la firma.

En resumen, en (S1601) hasta (S1608), el dispositivo de verificación 600 ejecuta el algoritmo Ver indicado en la Fórmula 222 y de esta manera verifica los datos de firma sig.

[Fórmula 222]

$$\mathsf{Ver}(\mathsf{pk}, m, \mathbb{S} := (M, \rho), \vec{s}^*)$$
$$\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, \quad \vec{s}^{\mathrm{T}} := (s_1, \ldots, s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, \quad s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}},$$
$$\vec{\eta}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0}, \ \vec{\eta}_{L+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_{d+1}}, \ \theta_{L+1}, s_{L+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$
$$c_0 := (-s_0 - s_{L+1}, \overbrace{0^{u_0}}^{u_0}, \overbrace{0^{w_0}}^{w_0}, \overbrace{\vec{\eta}_0}^{z_0})_{\mathbb{B}_0},$$
$$\text{para } 1 \le i \le L,$$
$$\text{si } \rho(i) = (t, \vec{v}_i),$$
$$\text{si } s_i^* \notin \mathbb{V}_t, \text{ devolver } 0,$$
$$\text{de otro modo } \mu_i, \ \theta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\eta}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^z,$$
$$c_i := (\overbrace{\mu_i(t, -1), s_i e_1 + \theta_i \vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\eta}}^{z})_{\mathbb{B}},$$
$$\text{si } \rho(i) = \neg(t, \vec{v}_i),$$
$$\text{si } s_i^* \notin \mathbb{V}_t, \text{ devolver } 0,$$

de otro modo $\mu_i \xleftarrow{U} \mathbb{F}_q$, $\vec{\eta}_i \xleftarrow{U} \mathbb{F}_q^z$,

$$c_i := (\overbrace{\mu_i(t, -1), s_i \vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\eta}_i}^{z})_{\mathbb{B}},$$

$$c_{L+1} := (\overbrace{s_{L+1} - \theta_{L+1} \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m \| \mathbb{S}), \theta_{L+1}}^{2}, \overbrace{0^{u_{d+1}}}^{u_{d+1}},$$

$$\overbrace{0^{w_{d+1}}}^{w_{d+1}}, \overbrace{\vec{\eta}_{L+1}}^{z_{d+1}})_{\mathbb{B}_{d+1}}$$

devolver 0 si $e(b_{0,1}, s_0^*) = 1$,

devolver 1 si $\prod_{i=0}^{L+1} e(c_i, s_i^*) = 1$, devolver 0 de otra manera.

Como se ha descrito anteriormente, como en los sistemas criptográficos 10 según las Realizaciones 2 a 4, en el sistema criptográfico 10 según la Realización 5, se proporcionan partes de índice, de modo que las bases que se usan para cada categoría de atributo se pueden construir como las bases comunes (base B y base B*). Como resultado, solamente la base B y la base B* necesitan ser incluidas en un parámetro público, eliminando la necesidad de reeditar el parámetro público cuando va a ser añadida una categoría de atributo en una etapa posterior.

Como en las Realizaciones 2 a 4, para las partes de índice, se requiere que 0 sea obtenido como resultado de una operación de producto interior de las partes de índice. Por lo tanto, aunque las partes de índice bidimensional, esto es los vectores de base b^*_1 y b^*_2 y los vectores de base b_1 y b_2, se emplean en la descripción anterior, las partes de índice no están limitadas a bidimensionales y pueden ser tridimensionales o de dimensión más alta. Los valores asignados a las partes de índice no están limitados a los descritos anteriormente y se puede emplear una disposición de asignación diferente.

El esquema de firma basado en el esquema de cifrado funcional se ha descrito anteriormente. No obstante, como se explica en la Realización 3 el esquema de cifrado funcional se puede modificar en un esquema de cifrado basado en atributo, así el esquema de firma basado en el esquema de cifrado funcional se puede modificar a un esquema de firma basado en el esquema de cifrado basado en atributo.

Realización 6

Esta realización describe un esquema de cifrado funcional de autoridad múltiple y un esquema de firma de autoridad múltiple.

Autoridad múltiple significa la presencia de una pluralidad de autoridades que generan la clave de descifrado del usuario (o clave de firma).

En un cifrado funcional ordinario, la seguridad del sistema entero depende de una cierta parte (autoridad). Por ejemplo, en el sistema criptográfico 10 descrito en la Realización 2 o 3, la seguridad del sistema entero depende del dispositivo de generación de clave 100. Si la clave secreta maestra sk que es la clave secreta del dispositivo de generación de clave 100 se compromete, se romperá la seguridad del sistema entero.

Con el esquema de autoridad múltiple, no obstante, incluso si se rompe la seguridad de alguna autoridad o se compromete la clave secreta (clave maestra) de alguna autoridad, solamente parte del sistema deja de funcionar y la parte restante del sistema puede funcionar adecuadamente.

La Fig. 38, es un dibujo explicativo de la autoridad múltiple. En la Fig. 38, se usa como ejemplo un proceso criptográfico definido estrechamente.

En la Fig. 38, una oficina gubernamental gestiona atributos tales como dirección, número de teléfono y edad. La policía gestiona atributos tales como el tipo de carnet de conducir. La Empresa A gestiona atributos tales como la posición en la Empresa A y el departamento de pertenencia en la Empresa A. Una clave de descifrado 1 asociada con los atributos gestionados por la oficina gubernamental se emite por la oficina gubernamental. Una clave de descifrado 2 asociada con los atributos gestionados por la policía se emite por la policía. Una clave de descifrado 3 asociada con los atributos gestionados por la Empresa A se emite por la Empresa A.

Un descifrador que descifra un texto cifrado descifra el texto cifrado usando una clave de descifrado formada poniendo juntas las claves de descifrado 1, 2 y 3 emitidas por las autoridades respectivas tales como la oficina gubernamental, la policía y la Empresa A. Es decir, cuando se ve desde el descifrador, una clave de descifrado formada poniendo juntas las claves de descifrado emitidas por las autoridades respectivas es la clave de descifrado única emitida a él o ella.

Por ejemplo, en un caso en el que la clave maestra de la Empresa A está comprometida, aunque el sistema de procesamiento criptográfico no funcione con respecto a los atributos de la Empresa A, funciona con respecto a los atributos gestionados por las otras autoridades. Es decir, concerniente a los atributos gestionados por la Empresa A hay un riesgo de descifrado por un usuario que tiene atributos distintos de los atributos especificados. No obstante, concerniente a atributos distintos de los gestionados por la Empresa A, el descifrado solamente es posible por un usuario que tenga los atributos especificados.

Como se ve a partir del ejemplo de la Fig. 38, según el cifrado funcional, es normal que estén presentes una pluralidad de autoridades y que cada autoridad gestione una cierta categoría (subespacio) o rango de definición en los atributos y emita (una parte de) una clave de descifrado con respecto al atributo del usuario en esta categoría.

Cuando cualquier parte puede servir como una autoridad y emite (una parte de) una clave de descifrado sin interactuar con las otras partes y cada usuario puede obtener (una parte de) la clave de descifrado sin interactuar con las otras partes, este esquema se llama un esquema de autoridad múltiple descentralizada.

Por ejemplo, si existe una autoridad central, el esquema no está descentralizado. Una autoridad central es una autoridad superior a las otras autoridades. Si se rompe la seguridad de la autoridad central, se romperá la seguridad de cada autoridad.

La Literatura no de Patente 31 describe un esquema de cifrado funcional de autoridad múltiple descentralizada y la Literatura no de Patente 30 describe un esquema de firma de autoridad múltiple no descentralizada. Como en el caso del esquema de cifrado y del esquema de firma descritos en las realizaciones anteriores, los esquemas descritos en la Literatura no de Patente 30 y Literatura no de Patente 31 se pueden construir de manera que no hay necesidad de reeditar un parámetro público cuando va a ser añadida una categoría de atributos.

La Fig. 39 es un dibujo explicativo de un esquema de cifrado funcional que permite la adición de una categoría de atributo en un caso de autoridad múltiple.

En la Fig. 39, como en la Fig. 38, una oficina gubernamental gestiona atributos tales como dirección, número de teléfono y edad. La policía gestiona atributos tales como el tipo de carnet de conducir. La Empresa A gestiona atributos tales como la posición en la Empresa A y el departamento de pertenencia en la Empresa A. Una clave de descifrado 1 asociada con los atributos gestionados por la oficina gubernamental se emite por la oficina gubernamental. Una clave de descifrado 2 asociada con los atributos gestionados por la policía se emite por la policía. Una clave de descifrado 3 asociada con los atributos gestionados por la Empresa A se emite por la Empresa A.

Señalar aquí que la oficina gubernamental genera una base $B\hat{}_1$ y una base $B\hat{}^*_1$ como un parámetro público pk y una clave secreta maestra sk, respectivamente. Usando la base $B\hat{}^*_1$, la oficina gubernamental genera la clave de descifrado 1 que concierne a los atributos tales como dirección, número de teléfono y edad. Del mismo modo, la policía genera una base $B\hat{}_2$ y una base $B\hat{}^*_2$ como un parámetro público pk y una clave secreta maestra sk, respectivamente. Usando la base $B\hat{}^*_2$, la policía genera la clave de descifrado 2 que concierne a los atributos tales como el tipo de carnet de conducir. Del mismo modo, la Empresa A genera una base $B\hat{}_3$ y una $B\hat{}^*_3$ como un parámetro público pk y una clave secreta maestra sk, respectivamente. Usando la base $B\hat{}^*_3$, la Empresa A genera la clave de descifrado 3 que concierne a los atributos tales como la posición en la Empresa A y el departamento de pertenencia en la Empresa A.

Un remitente genera un texto cifrado fijando los atributos tales como dirección, número de teléfono y edad usando la base $B\hat{}_1$, fijando los atributos tales como el tipo de carnet de conducir usando la base $B\hat{}_2$ y fijando los atributos tales como la posición en la Empresa A y el departamento de pertenencia en la Empresa A usando la base $B\hat{}_3$. Un descifrador descifra el texto cifrado usando las claves de descifrado 1 a 3.

Por ejemplo, cuando va a ser añadida una categoría de atributo gestionada por la oficina gubernamental, se puede añadir la categoría de atributo sin reeditar el parámetro público pk de la oficina gubernamental.

El esquema de cifrado funcional que permite la adición de una categoría de atributo ha sido descrito en la presente memoria. No obstante, el mismo concepto se puede aplicar básicamente al esquema de firma adaptado a partir del esquema de cifrado funcional.

Realización 7

En las realizaciones anteriores, se ha descrito el método para implementar los procesos de las primitivas criptográficas en los espacios de vector dual. En la Realización 7, se describirá un método para implementar los procesos de las primitivas criptográficas en grupos aditivos duales.

Más específicamente, en las realizaciones anteriores, los procesos de las primitivas criptográficas se implementan en el grupo cíclico del orden primo q. Cuando un anillo R se expresa usando una M compuesta como se indica en la Fórmula 223, los procesos de las primitivas criptográficas descritas en las realizaciones anteriores también se pueden aplicar a un grupo aditivo que tiene el anillo R como coeficiente.

[Fórmula 223]

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

donde

$\mathbb{Z}$: un entero y

M : un número compuesto

Cambiando F_q a R en los algoritmos descritos en las realizaciones anteriores, se pueden implementar los procesos de las primitivas criptográficas en grupos aditivos duales.

Desde el punto de vista de prueba de seguridad, en las realizaciones anteriores, ρ(i) para cada entero i = 1, ..., L se puede limitar a una tupla positiva (t, v→) o tupla negativa ¬(t, v→) para información de identificación t diferente respectivamente.

En otras palabras, cuando ρ(i) = (t, $\vec{v}$) o ρ(i) = ¬(t, $\vec{v}$), permitamos que una función $\tilde{\rho}$ sea una correlación de {1, ..., L} $\vec{}$ {1, ..., d} de manera que $\tilde{\rho}$(i) = t. En este caso, $\tilde{\rho}$ se puede limitar a inyección. Señalar que ρ(i) es ρ(i) en la estructura de acceso S: = (M, ρ(i)) descrita anteriormente.

Una configuración hardware del sistema criptográfico 10 (el dispositivo de generación de clave 100, el dispositivo de cifrado 200, el dispositivo de descifrado 300, el dispositivo de delegación de clave 400, el dispositivo de firma 500 y el dispositivo de verificación 600) se describirá según las realizaciones.

La fig. 40 es un diagrama que muestra un ejemplo de una configuración hardware del dispositivo de generación de clave 100, el dispositivo de cifrado 200, el dispositivo de descifrado 300, el dispositivo de delegación de clave 400, el dispositivo de firma 500 y el dispositivo de verificación 600.

Como se muestra en la Fig. 40, cada uno del dispositivo de generación de claves 100, el dispositivo de cifrado 200, el dispositivo de descifrado 300, el dispositivo de delegación de clave 400, el dispositivo de firma 500 y el dispositivo de verificación 600 incluye la CPU 911 (también denominada Unidad Central de Proceso, dispositivo de procesamiento central, dispositivo de procesamiento, dispositivo aritmético, microprocesador, microordenador o procesador) que ejecuta programas. La CPU 911 se conecta a través de un bus 912 a la ROM 913, la RAM 914, un LCD 901 (visualizador de cristal líquido), el teclado 902 (K/B), la placa de comunicación 915 y el dispositivo de disco magnético 920 y controla estos dispositivos hardware. En lugar del dispositivo de disco magnético 920 (dispositivo de disco fijo), se puede emplear un dispositivo de almacenamiento tal como un dispositivo de disco óptico o un dispositivo de lectura/escritura de tarjeta de memoria. El dispositivo de disco magnético 920 se conecta a través de una interfaz de disco fijo predeterminada.

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

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

Los programas 923 almacenan software y programas que ejecutan las funciones descritas en la descripción anterior como la “unidad de generación de clave maestra 110”, la “unidad de almacenamiento de clave maestra 120”, la “unidad de entrada de información 130”, la “unidad de generación de clave de descifrado 140”, la “unidad de distribución de clave 150”, la “unidad de adquisición de parámetro público 210”, la “unidad de entrada de información 220”, la “unidad de generación de datos de cifrado 230”, la “unidad de transmisión de datos 240”, la “unidad de adquisición de clave de descifrado 310”, la “unidad de recepción de datos 320”, la “unidad de cálculo de programa de tramo 330”, la “unidad de cálculo de coeficiente complementario 340”, la “unidad de operación de emparejamiento

350", la "unidad de cálculo de mensaje 360", la "unidad de adquisición de clave de descifrado 410", la "unidad de entrada de información 420", la "unidad de generación de clave de delegación 430", la "unidad de distribución de clave 440", la "unidad de adquisición de clave de firma 510" la "unidad de entrada de información 520", la "unidad de cálculo de coeficiente complementario 530", la "unidad de generación de datos de firma 540", la "unidad de transmisión de datos 550", la "unidad de adquisición de parámetro público 610", la "unidad de recepción de datos 620", la "unidad de generación de datos de verificación 630", la "unidad de operación de emparejamiento 640" y similares. Los programas 923 almacenan otros programas también. Los programas se leen y ejecutan por la CPU 911.

Los archivos 924 almacenan información, datos, valores de señal, valores de variable y parámetros tales como el "parámetro público pk", la "clave secreta maestra sk", las "claves de descifrado sk_S y sk_Γ", los "textos cifrados ct_Γ y ct_S", la "estructura de acceso S", la "información de atributo" y el "mensaje m", como los ítems de un "archivo" y "base de datos". El "archivo" y la "base de datos" se almacenan en un medio de grabación tal como un disco o memoria. La información, datos, valores de señal, valores de variables y parámetros almacenados en el medio de grabación tal como el disco o la memoria se leen de la memoria principal o memoria caché por la CPU 911 a través de un circuito de lectura/escritura y se usan para operaciones de la CPU 911 tales como extracción, búsqueda, revisión, comparación, cálculo, computación, procesamiento, salida, impresión y visualización. La información, datos, valores de señal, valores de variable y parámetros se almacenan temporalmente en la memoria principal, memoria caché o memoria de almacenamiento temporal durante las operaciones de la CPU 911 que incluyen extracción, búsqueda, revisión, comparación, cálculo, computación, procesamiento, salida, impresión y visualización.

Las flechas en los diagramas de flujo en la descripción anterior indican principalmente la entrada/salida de datos y señales. Los datos y valores de señal se almacenan en la memoria de la RAM 914, el medio de grabación tal como un disco óptico o en un chip IC. Los datos y señales se transmiten en línea a través de un medio de transmisión tal como el bus 912, líneas de señal o cables o a través de ondas eléctricas.

Lo que se describe como "unidad" en la descripción anterior puede ser "circuito", "dispositivo", "equipo", "medios" o "función" y también puede ser "paso", "procedimiento" o "proceso". Lo que se describe como "dispositivo" puede ser "circuito", "equipo", "medios" o "función" y también puede ser "paso", "procedimiento" o "proceso". Lo que se describe como "proceso" puede ser "paso". En otras palabras, lo que se describe como "unidad" se puede realizar mediante un microprograma almacenado en la ROM 913. Alternativamente, lo que se describe como "unidad" se puede implementar únicamente por software o únicamente por hardware tal como un elemento, un dispositivo, un sustrato o una línea de cableado o por una combinación de software y microprograma o por una combinación que incluye microprograma. El microprograma y software se almacenan como programas en el medio de grabación tal como la ROM 913. Los programas se leen por la CPU 911 y se ejecutan por la CPU 911. Es decir, cada programa hace al ordenador o similar funcionar como cada "unidad" descrita anteriormente. Alternativamente, cada programa hace al ordenador o similar ejecutar un procedimiento o un método de cada "unidad" descrita anteriormente.

Lista de signos de referencia

10: sistema criptográfico; 100: dispositivo de generación de clave; 110: unidad de generación de clave maestra; 120: unidad de almacenamiento de clave maestra; 130: unidad de entrada de información; 140: unidad de generación de clave de descifrado; 141: unidad de generación de vector f; 142: unidad de generación de vector s; 143: unidad de generación de número aleatorio; 144: unidad de generación de elemento de clave; 145: unidad de generación de elemento de aleatorización; 146: unidad de generación de elemento de delegación; 150: unidad de distribución de clave; 200: dispositivo de cifrado; 210: unidad de adquisición de parámetro público; 220: unidad de entrada de información; 230: unidad de generación de datos de cifrado; 231: unidad de generación de número aleatorio; 232: unidad de generación de elemento de cifrado; 240: unidad de transmisión de datos; 300: dispositivo de descifrado; 310: unidad de adquisición de clave de descifrado; 320: unidad de recepción de datos; 330: unidad de cálculo de programa de tramo; 340: unidad de cálculo de coeficiente complementario; 350: unidad de operación de emparejamiento; 360: unidad de cálculo de mensaje; 400: dispositivo de delegación de clave; 410: unidad de adquisición de clave de descifrado; 420: unidad de entrada de información; 430: unidad de generación de clave de delegación; 431: unidad de generación de número aleatorio; 432: unidad de generación de elemento de clave de nivel más bajo; 433: unidad de generación de elemento de aleatorización de nivel más bajo; 434: unidad de generación de elemento de delegación de nivel más bajo; 440: unidad de distribución de clave; 500: dispositivo de firma; 510: unidad de adquisición de clave de firma; 520: unidad de entrada de información; 530: unidad de cálculo del coeficiente complementario; 540: unidad de generación de datos de firma; 541: unidad de generación de número aleatorio; 542: unidad de generación de elemento de firma; 550: unidad de transmisión de datos; 600: dispositivo de verificación; 610: unidad de adquisición de parámetro público; 620: unidad de recepción de datos; 630: unidad de generación de datos de verificación; 631: unidad de generación de vector f; 632: unidad de generación de vector s; 633: unidad de generación de número aleatorio; 634: unidad de generación de elemento de verificación; 640: unidad de operación de emparejamiento.

REIVINDICACIONES

1. Un sistema criptográfico (10) configurado para realizar un proceso usando una base B predeterminada y una base B* predeterminada, el sistema criptográfico que comprende:

un dispositivo de transmisión (200, 500) configurado para generar un vector de lado de transmisión t_j para al menos un índice j de entre una pluralidad de índices j, el vector de lado de transmisión t_j que es un vector en el cual información J asignada por adelantado al índice j se fija como un coeficiente de un vector de base predeterminado $b_{índice}$ de la base B y un parámetro Φ_j para el índice j se fija como un coeficiente de otro vector de base b_{att} de la base B; y

un dispositivo de recepción (300, 600) configurado para usar un vector de lado de recepción $r_{j'}$ para al menos un índice j' de entre una pluralidad de índices j', el vector de lado de recepción $r_{j'}$ que es un vector en el cual información J' que tiene un producto interior de 0 con información J asignada por adelantado al índice j que corresponde al índice j' se fija como un coeficiente de un vector de base $b^*_{índice}$ de la base B* que corresponde al vector de base $b_{índice}$ y un parámetro $\psi_{j'}$ para el índice j' se fija como un coeficiente de un vector de base b^*_{att} de la base B* que corresponde al vector de base b_{att} y calcular un producto de operaciones de emparejamiento sobre pares correspondientes de los vectores de base del vector de lado de transmisión t_j para el índice j y el vector de lado de recepción $r_{j'}$ para el índice j' que corresponde al índice j.

2. El sistema criptográfico según la reivindicación 1,

en el que el dispositivo de transmisión es un dispositivo de cifrado (200) que genera un texto cifrado ct y se configura para usar un entero t de t = 1, …, d (d que es un entero de 1 o más) como el índice j, usar información de atributo x_t para el entero t como el parámetro Φ_j para el índice j y generar el texto cifrado ct que incluye como el vector de lado de transmisión t_j un vector de cifrado c_t en el que información J asignada al entero t se fija como el coeficiente del vector de base $b_{índice}$ y la información de atributo x_t para el entero t se fija como el coeficiente del vector de base b_{att}, para al menos un entero t y

en el que el dispositivo de recepción es un dispositivo de descifrado (300) que descifra el texto cifrado ct y se configura para usar un entero i de i = 1, …, L (L que es un entero de 1 o más) como el índice j', usar información de predicado v_i para el entero i como el parámetro $\psi_{j'}$ para el índice j', usar como el vector de lado de recepción $r_{j'}$ un vector de clave k^*_i en el cual información J' que tiene un producto interior de 0 con la información J asignada al entero t que corresponde al entero i se fija como un coeficiente de vector de base $b^*_{índice}$ y la información de predicado v_i para el entero i se fija como el coeficiente del vector de base b^*_{att}, para cada entero i y calcular un producto de operaciones de emparejamiento sobre pares correspondientes de los vectores de base del vector de clave k^*_i para cada entero i y el vector de cifrado c_t para el entero t que corresponde a cada entero i.

3. El sistema criptográfico según la reivindicación 2,

en el que el sistema criptográfico se configura para realizar el proceso usando una base B_0 predeterminada y una base B^*_0 predeterminada y una base B predeterminada y una base B* predeterminada,

en el que el dispositivo de transmisión se configura para generar el texto cifrado ct incluyendo un vector de cifrado c_0 y un vector de cifrado c_t para al menos un entero t de t = 1, …, d, como se indica en la Fórmula 1 y

en el que el dispositivo de recepción se configura para calcular la Fórmula 3 para un vector de clave k^*_i para cada entero i de i = 0, …, L, como se indica en la Fórmula 2 y el vector de cifrado c_t

[Fórmula 1]

$$c_0 := (\omega, \overbrace{0^{u_0}}^{u_0}, \zeta, \overbrace{0^{w_0}}^{w_0}, \overbrace{\vec{\varphi}_0}^{z_0})_{\mathbb{B}_0},$$

$$c_t = (\overbrace{\sigma_t(1, t), \omega\vec{x}_t}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\varphi}_t}^{z})_{\mathbb{B}}$$

donde

$$\vec{x}_t := (x_{t,1}, \ldots, x_{t,n}),$$

$\omega, \zeta, \vec{\varphi}_0 = \varphi_{0,1}, \ldots, \varphi_{0,z_0}, \sigma_t, \vec{\varphi}_t = \varphi_{t,1}, \ldots, \varphi_{t,z}$ son números aleatorios,

n es un entero de 1 o más y

u_0, w_0, z_0, u, w, z son cada uno un entero de 0 o más,

[Fórmula 2]

$$\boldsymbol{k}_0^* := (-s_0, \overbrace{0^{u_0}}^{u_0}, 1, \overbrace{\vec{\eta}_0}^{w_0}, \overbrace{0^{z_0}}^{z_0},)_{\mathbb{B}_0^*},$$

si $\rho(i) = (t, \vec{v}_i)$,

$$\boldsymbol{k}_i^* := (\overbrace{\mu_i(t, -1,), s_i\vec{e}_1 + \theta_i\vec{v}_i}^{2+n}, \overbrace{0^u,}^{u}, \overbrace{\vec{\eta}_i,}^{w}, \overbrace{0^z}^{z},)_{\mathbb{B}^*},$$

si $\rho(i) = \neg(t, \vec{v}_i)$,

$$\boldsymbol{k}_i^* := (\overbrace{\mu_i(t, -1,), s_i\vec{v}_i,}^{2+n}, \overbrace{0^u,}^{u}, \overbrace{\vec{\eta}_i,}^{w}, \overbrace{0^z}^{z},)_{\mathbb{B}^*}$$

donde

$\vec{v}_i := (v_{i,1}, \ldots, v_{i,n})$,

$\vec{\eta}_0 = \eta_{0,1}, \ldots, \eta_{0,w_0}$, μ_i, θ_i, $\vec{\eta}_i = \eta_{i,1}, \ldots, \eta_{i,w}$ son números aleatorios,

$$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}},$$
$$\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}},$$

$\vec{f}$ es un vector que tiene r piezas de elementos,

M es una matriz de L filas y r columnas,

ρ(i) es una variable a la que se asigna por adelantado $(t, \vec{v}_i)$ o $\neg(t, \vec{v}_i)$,

n es un entero de 1 o más y

u_0, w_0, z_0, u, w, z son cada uno un entero de 0 o más,

[Fórmula 3]

$$K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \prod_{i \in I \wedge \rho(i) = (t, \vec{v}_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i} \prod_{i \in I \wedge \rho(i) = \neg(t, \vec{v}_i)} e(\boldsymbol{c}_t, \boldsymbol{k}_i^*)^{\alpha_i / (\vec{v}_i \cdot \vec{x}_t)}$$

donde

$\vec{1} = \sum_{i \in I} \alpha_i M_i$, donde M_i es la fila de orden i de M,

$$I \subseteq \{i \in \{1, \ldots L\} \mid [\rho(i) = (t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t = 0]$$
$$\vee [\rho(i) = \neg(t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t \neq 0]$$

4. El sistema criptográfico según la reivindicación 1,

en el que el dispositivo de transmisión es un dispositivo de cifrado (200) que genera un texto cifrado ct y se configura para usar un entero i de i = 1, …, L (L que es un entero de 1 o más) como el índice j, usar información de predicado v_i para el entero i como el parámetro Φ_j para el índice j y generar el texto cifrado ct que incluye como el vector de lado de transmisión t_j un vector de cifrado c_i en el que información J asignada al entero i se fija

como el coeficiente del vector de base $b_{índice}$ y la información de predicado v_i para el entero i se fija como el coeficiente del vector de base b_{att}, para cada entero i y

en el que el dispositivo de recepción es un dispositivo de descifrado (300) que descifra el texto cifrado ct y se configura para usar un entero t de t = 1, …, d (d que es un entero de 1 o más) como el índice j', usar información de atributo x_t para el entero t como el parámetro $\psi_{j'}$ para el índice j', usar como el vector de lado de recepción $r_{j'}$ un vector de clave k^*_t en el cual información J' que tiene un producto interior de 0 con la información J asignada al entero i que corresponde al entero t se fija como el coeficiente del vector de base $b^*_{índice}$ e información de atributo x_t para el entero t se fija como el coeficiente del vector de base b^*_{att}, para al menos un entero t y calcular un producto de operaciones de emparejamiento sobre pares correspondientes de los vectores de base del vector de cifrado c_i para cada entero i y el vector de clave k^*_t para el entero t que corresponde a cada entero i.

5. El sistema criptográfico según la reivindicación 4,

en el que el sistema criptográfico se configura para realizar el proceso usando una base B_0 predeterminada y una base B^*_0 predeterminada y una base B predeterminada y una base B* predeterminada,

en el que el dispositivo de transmisión se configura para generar el texto cifrado ct incluyendo un vector de cifrado c_i para cada entero i de i = 0, …, L, como se indica en la Fórmula 4 y

en el que el dispositivo de recepción se configura para calcular la Fórmula 6 para un vector de clave k^*_0 y un vector de clave k^*_t para al menos un entero t de t = 1, …, d, como se indica en la Fórmula 5 y el vector de cifrado c_i

[Fórmula 4]

$$c_0 := (-s_0, \overbrace{0^{u_0}}^{u_0}, \zeta, \overbrace{0^{w_0}}^{w_0}, \overbrace{\vec{\eta}_0}^{z_0})_{\mathbb{B}_0},$$

si $\rho(i) = (t, \vec{v}_i)$,

$$c_i := (\overbrace{\mu_i(t, -1), s_i\vec{e}_1 + \theta_i\vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\eta}_i}^{z})_{\mathbb{B}},$$

si $\rho(i) = \neg(t, \vec{v}_i)$,

$$c_i := (\overbrace{\mu_i(t, -1), s_i\vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\eta}_i}^{z})_{\mathbb{B}}$$

donde

$\vec{v}_i := (v_{i,1}, \ldots, v_{i,n})$,

$\zeta, \vec{\eta}_0 = \eta_{0,1}, \ldots, \eta_{0,z_0}, \mu_i, \theta_i, \vec{\eta}_i = \eta_{i,1}, \ldots, \eta_{i,z}$ son números aleatorios,

$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$,

$\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$,

$\vec{f}$ es un vector que tiene r piezas de elementos,

M es una matriz de L filas y r columnas,

ρ(i) es una variable a la que se asigna por adelantado $(t, \vec{v}_i)$ o $\neg(t, \vec{v}_i)$,

n es un entero de 1 o más y

u_0, w_0, z_0, *u*, *w*, *z* son cada uno un entero de 0 o más,

[Fórmula 5]

$$\boldsymbol{k}_0^* := (\omega, \overbrace{0^{u_0},}^{u_0} 1, \overbrace{\vec{\varphi}_0,}^{w_0} \overbrace{0^{z_0},}^{z_0})_{\mathbb{B}_0^*},$$

$$\boldsymbol{k}_t^* := (\overbrace{\sigma_t(1,\ t),}^{2+n} \overbrace{\omega\vec{x}_t,}^{u} \overbrace{0^u,}^{w} \overbrace{\vec{\varphi}_t,}^{z} \overbrace{0^z}^{})_{\mathbb{B}^*}$$

donde

$\vec{x}_t := (x_{t,1},\ldots,x_{t,n})$,

$\omega,\ \vec{\varphi}_0 = \varphi_{0,1},\ldots,\varphi_{0,w_0},\ \sigma_t,\ \vec{\varphi}_t = \varphi_{t,1},\ldots,\varphi_{t,w}$ son números aleatorios,

n es un entero de 1 o más y

u_0, w_0, z_0, *u*, *w*, *z* son cada uno un entero de 0 o más,

[Fórmula 6]

$$K := e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \prod_{i\in I \wedge \rho(i)=(t,\vec{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}_t^*)^{\alpha_i} \prod_{i\in I \wedge \rho(i)=\neg(t,\vec{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}_t^*)^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)}$$

donde

$\vec{1}=\sum_{i\in I}\alpha_i M_i$, donde M_i es la fila de orden i de *M*,

$$I \subseteq \{i \in \{1,\ldots L\} \mid [\rho(i) = (t,\vec{v}_i) \wedge (t,\vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t = 0]$$
$$\vee [\rho(i) = \neg(t,\vec{v}_i) \wedge (t,\vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t \neq 0]\}.$$

6. El sistema criptográfico según la reivindicación 1,

en el que el dispositivo de transmisión es un dispositivo de cifrado (200) que genera un texto cifrado ct y se configura para usar un entero i de i = 1, …, L (L que es un entero de 1 o más) como el índice j, usar información de atributo x_i para el entero i como el parámetro Φ_j para el índice j y generar el texto cifrado ct que incluye como el vector de lado de transmisión t_j un vector de cifrado c_i en el que información J asignada al entero i se fija como el coeficiente del vector de base $b_{índice}$ e información de atributo x_i para el entero i se fija como el coeficiente del vector de base b_{att}, para cada entero i y

en el que el dispositivo de recepción es un dispositivo de descifrado (300) que descifra el texto cifrado ct y se configura para usar el entero i como el índice j' y usar información de predicado v_i para el entero i como el parámetro $\psi_{j'}$ para el índice j', usar como el vector de lado de recepción $r_{j'}$ un vector de clave k^*_i en el cual información J' que tiene un producto interior de 0 con la información J asignada al entero i se fija como el coeficiente del vector de base $b^*_{índice}$ e información de predicado v_i para el entero i se fija como el coeficiente del vector de base b^*_{att}, para cada entero i y calcular un producto de operaciones de emparejamiento sobre pares correspondientes de los vectores de base del vector de clave k^*_i y el vector de cifrado c_i para cada entero i.

7. El sistema criptográfico según la reivindicación 6,

en el que el sistema criptográfico se configura para realizar el proceso usando una base B_0 predeterminada y una base B^*_0 predeterminada y una base B predeterminada y una base B* predeterminada,

en el que el dispositivo de transmisión se configura para generar el texto cifrado ct incluyendo un vector de cifrado c_l que es una suma de los vectores de cifrado c_i para cada entero i de i = 0, …, L, como se indica en la Fórmula 7 y

en el que el dispositivo de recepción se configura para calcular un producto de operaciones de emparejamiento sobre los pares correspondientes de los vectores de base del vector de cifrado c_l y un vector de clave $k^*_{L,dec}$ que es una suma de vectores de clave k^*_i para cada entero i, como se indica en la Fórmula 8

[Fórmula 7]

$$\boldsymbol{c}_1 := ((\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0},\ (\sigma_t(1,t),\ \omega\vec{x}_t),\ 0^u, 0^w, \vec{\varphi}_t)_{\mathbb{B}} : t = 1,...,L)$$

donde

$$\vec{x}_t := (x_{t,1},\ldots,x_{t,n})$$,

$$\omega,\ \zeta,\ \vec{\varphi}_0 := \varphi_{0,1},\ldots,\varphi_{0,z_0},\ \sigma_i,\ \vec{\varphi}_t := \varphi_{t,1},\ldots,\varphi_{t,z}$$ son números aleatorios,

y

u_0, w_0, z_0, u, w, z son cada uno un entero de 0,

[Fórmula 8]

$$\boldsymbol{k}^*_{L,\mathrm{dec}} := (\ (-s_{\mathrm{dec},0},\ 0^{u_0},\ 1,\ \vec{\eta}_{\mathrm{dec},0},\ 0^{z_0})_{\mathbb{B}^*_0},\ (\mu_{\mathrm{dec},t}(t,-1),\ s_{\mathrm{dec},t}\vec{e}_1 + \theta_{\mathrm{dec},t}\vec{v}_t,\ 0^{\mathrm{u}},\ \vec{\eta}_{\mathrm{dec},t},\ 0^{\mathrm{z}})_{\mathbb{B}^*} : t = 1,...,L),$$

donde

$$\vec{v}_i := (v_{i,1},\ldots,v_{i,n})$$,

$$\vec{\eta}_{\mathrm{dec},0} = \eta_{\mathrm{dec},0,1},\ldots,\eta_{\mathrm{dec},0,w_0},\ \mu_{\mathrm{dec},t},\ \theta_{\mathrm{dec},t},$$

$$\vec{\eta}_{\mathrm{dec},t} = \eta_{\mathrm{dec},t,1},\ldots,\eta_{\mathrm{dec},t,w}$$ son números aleatorios,

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

n es un entero de 1 o más y

u_0, w_0, z_0, u, w, z son cada uno un entero de 0 o más.

8. El sistema criptográfico según la reivindicación 1,

en el que el dispositivo de transmisión es un dispositivo de firma (500) que genera datos de firma sig y se configura para usar un entero t de t = 1, …, d (d que es un entero de 1 o más) como el índice j, usar información de atributo x_i para el entero t como el parámetro Φ_j para el índice j, usar un vector de clave k^*_t en el que información J asignada al entero t se fija como el coeficiente del vector de base $b_{\text{índice}}$ e información de atributo x_t para el entero t se fija como el coeficiente del vector de base b_{att} para al menos un entero t y generar los datos de firma sig incluyendo como el vector de lado de transmisión t_j un elemento de firma s_i, para cada entero i de i = 1, …, L (L que es un entero de 1 o más), incluyendo el vector de clave k^*_t para el entero t que corresponde a cada entero i y

en el que el dispositivo de recepción es un dispositivo de verificación (600) que verifica los datos de firma sig y se configura para usar el entero i como el índice j', usar información de predicado v_i para el entero i como el parámetro $\psi_{j'}$ para el índice j', usar como el vector de lado de recepción $r_{j'}$ un elemento de verificación c_i en el cual, para cada entero i, información J' que tiene un producto interior de 0 con la información J asignada a cada entero t que corresponde a cada entero i se fija como el coeficiente del vector de base $b^*_{\text{índice}}$ e información de predicado v_i para cada entero i se fija como el coeficiente del vector de base b^*_{att} y calcular un producto de operaciones de emparejamiento sobre pares correspondientes de los vectores de base del elemento de firma s_i y el elemento de verificación c_i para cada entero i.

9. El sistema criptográfico según la reivindicación 8,

en el que el sistema criptográfico se configura para realizar el proceso usando una base B_0 predeterminada y una base B^*_0 predeterminada, una base B predeterminada y una base B* predeterminada y una base B_{d+1} predeterminada y una base B^*_{d+1} predeterminada,

en el que el dispositivo de transmisión se configura para generar los datos de firma sig incluyendo un elemento de firma s_i, como se indica en la Fórmula 10, usando un vector de clave k^*_0, un vector de clave k^*_t para al menos un entero t de t = 1, …, d, un vector de clave $_{d+1,1}$ y un vector de clave $_{d+1,2}$, como se indica en la Fórmula 9 y

en el que el dispositivo de recepción calcula la Fórmula 12 para un elemento de verificación c_i para cada entero i, como se indica en la Fórmula 11 y el elemento de firma s_i

[Fórmula 9]

$$k_0^* := (\delta, \overbrace{0^{u_0}}^{u_0}, \overbrace{\vec{\varphi}_0}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0},$$

$$k_t^* := (\overbrace{\sigma_t(1, t), \delta\vec{x}_t}^{2+n}, \overbrace{0^u}^{u}, \overbrace{\vec{\varphi}_t}^{w}, \overbrace{0^z}^{z})_{\mathbb{B}},$$

$$k_{d+1,1}^* := (\overbrace{\delta(1, 0)}^{2}, \overbrace{0^{u_{d+1}}}^{u_{d+1}}, \overbrace{\vec{\varphi}_{d+1,1}}^{w_{d+1}}, \overbrace{0^{z_{d+1}}}^{z_{d+1}})_{\mathbb{B}_{d+1}},$$

$$k_{d+1,2}^* := (\overbrace{\delta(0, 1)}^{2}, \overbrace{0^{u_{d+1}}}^{u_{d+1}}, \overbrace{\vec{\varphi}_{d+1,2}}^{w_{d+1}}, \overbrace{0^{z_{d+1}}}^{z_{d+1}})_{\mathbb{B}_{d+1}}$$

donde

$\vec{x}_t := (x_{t,1},\ldots,x_{t,n})$,

$\delta, \vec{\varphi}_0 = \varphi_{0,1},\ldots,\varphi_{0,w_0}, \sigma_t, \vec{\varphi}_t = \varphi_{t,1},\ldots,\varphi_{t,w}$,

$\vec{\varphi}_{d+1,1} = \varphi_{d+1,,11},\ldots,\varphi_{d+1,1,w_{d+1}}$, son números aleatorios

$\vec{\varphi}_{d+2} = \varphi_{d+1,2,1},\ldots,\varphi_{d+1,2,w_{d+1}}$

n es un entero de 1 o más y

u_0, w_0, z_0, u, w, z son cada uno un entero de 0 o más,

[Fórmula 10]

$$s_0^* := \xi k_0^* + r_0^*,$$

$$s_i^* := \gamma_i \cdot \xi k_t^* + \sum_{l=1}^{n} y_{i,l} \cdot b_{t,l}^* + r_i^*, \text{ para } 1 \le i \le L,$$

$$s_{L+1}^* := \xi(k_{d+1,1}^* + \mathrm{H} \cdot k_{d+1,2}^*) + r_{L+1}^*$$

donde

$\xi, r_0^*, r_i^*, r_{L+1}^*$ son números aleatorios,

$\gamma_i, \vec{y}_i := (y_{i,1},...,y_{i,n})$ se definen como

$$\text{si } i \in I \wedge \rho(i) = (t, \vec{v}_i),\ \gamma_i := \alpha_i,\ \vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},$$

$$\text{si } i \in I \wedge \rho(i) = \neg(t, \vec{v}_i),\ \gamma_i := \frac{\alpha_i}{\vec{v}_i \cdot \vec{x}_t},\ \vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

$$\text{si } i \notin I \wedge \rho(i) = (t, \vec{v}_i),\ \gamma_i := 0,\ \vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},$$

$$\text{si } i \notin I \wedge \rho(i) = \neg(t, \vec{v}_i),\ \gamma_i := 0,\ \vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

$$(\beta_i) \xleftarrow{\cup} \{(\beta_1,...,\beta_L) \,|\, \textstyle\sum_{i=1}^{L} \beta_i M_i = \vec{0}\},$$

M es una matriz de L filas y r columnas,

ρ(i) es una variable a la cual se asigna por adelantado $(t, \vec{v}_i)$ o $\neg(t, \vec{v}_i)$ y H es un valor de comprobación aleatoria,

[Fórmula 11]

$$c_0 := (-s_0 - s_{L+1}, \overbrace{0^{u_0}}^{u_0}, \overbrace{0^{w_0}}^{w_0}, \overbrace{\vec{\eta}_0}^{z_0})_{\mathbb{B}_0^*},$$

$$\text{si } \rho(i) = (t, \vec{v}_i)$$

$$c_i := (\overbrace{\mu_i(t, -1), s_i e_1 + \theta_i \vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\eta}}^{z})_{\mathbb{B}^*},$$

$$\text{si } \rho(i) = \neg(t, \vec{v}_i)$$

$$c_i := (\overbrace{\mu_i(t, -1), s_i \vec{v}_i}^{2+n}, \overbrace{0^u}^{u}, \overbrace{0^w}^{w}, \overbrace{\vec{\eta}_i}^{z})_{\mathbb{B}^*},$$

$$c_{L+1} := (\overbrace{s_{L+1} - \theta_{L+1}\mathsf{H}, \theta_{L+1}}^{2}, \overbrace{0^{u_{d+1}}}^{u_{d+1}}, \overbrace{0^{w_{d+1}}}^{w_{d+1}}, \overbrace{\vec{\eta}_{L+1}}^{z_{d+1}})_{\mathbb{B}_{d+1}^*}$$

donde

$\vec{v}_i := (v_{i,1},\ldots,v_{i,n})$,

$\vec{\eta}_0 = \eta_{0,1},...,\eta_{0,z_0}$, μ_i, θ_i, $\vec{\eta}_i = \eta_{i,1},...,\eta_{i,z}$,

$\vec{\eta}_{L+1} = \eta_{L+1,1},...,\eta_{L+1,z}$ son números aleatorios,

$s_0 \coloneqq \vec{1} \cdot \vec{f}^{\mathrm{T}},\ \vec{s}^{\mathrm{T}} \coloneqq (s_1,...,s_L)^{\mathrm{T}} \coloneqq M \cdot \vec{f}^{\mathrm{T}}$,

$\vec{f}$ es un vector que tiene r piezas de elementos, *M* es una matriz de L filas y r columnas,

ρ(i) es una variable a la que se asigna por adelantado $(t,\vec{v}_i)$ o $\neg(t,\vec{v}_i)$,

n es un entero de 1 o más y u_0, w_0, z_0, *u*, *w*, *z* son cada uno un entero de 0 o más,

[Fórmula 12]

$\prod_{i=0}^{L+1} e(c_i, s_i^*)$.

10. Un método criptográfico para realizar un proceso usando una base B predeterminada y una base B* predeterminada, el método criptográfico que comprende:

generar un vector de lado de transmisión t_j para al menos un índice j de entre una pluralidad de índices j, el vector de lado de transmisión t_j que es un vector en el cual información J asignada por adelantado al índice j se fija como un coeficiente de un vector de base predeterminado $b_{índice}$ de la base B y un parámetro Φ_j para el índice j se fija como un coeficiente de otro vector de base b_{att} de la base B, por un dispositivo de transmisión (200, 500); y

usar un vector de lado de recepción $r_{j'}$ para al menos un índice j' de entre una pluralidad de índices j', el vector de lado de recepción $r_{j'}$ que es un vector en el cual información J' que tiene un producto interior de 0 con la información J asignada por adelantado al índice j que corresponde al índice j' se fija como un coeficiente de un vector de base $b^*_{índice}$ de la base B* que corresponde al vector de base $b_{índice}$ y un parámetro $\psi_{j'}$ para el índice j' se fija como un coeficiente de un vector de base b^*_{att} de la base B* que corresponde al vector de base b_{att} y calcular un producto de operaciones de emparejamiento sobre pares correspondientes de los vectores de base del vector de lado de transmisión t_j para el índice j y el vector de lado de recepción $r_{j'}$ para el índice j' que corresponde al índice j, por un dispositivo de recepción (300, 600).

11. Un programa criptográfico para realizar procesos usando una base B predeterminada y una base B* predeterminada, el programa criptográfico que hace a un ordenador ejecutar:

un proceso de transmisión de generación de un vector de lado de transmisión t_j para al menos un índice j de entre una pluralidad de índices j, el vector de lado de transmisión t_j que es un vector en el cual información J asignada por adelantado al índice j se fija como un coeficiente de un vector de base predeterminado $b_{índice}$ de la base B y un parámetro Φ_j para el índice j se fija como un coeficiente de otro vector de base b_{att} de la base B; y

un proceso de recepción de uso de un vector de lado de recepción $r_{j'}$ para al menos un índice j' de entre una pluralidad de índices j', el vector de lado de recepción $r_{j'}$ que es un vector en el cual información J' que tiene un producto interior de 0 con la información J asignada por adelantado al índice j que corresponde al índice j' se fija como un coeficiente de un vector de base $b^*_{índice}$ de la base B* que corresponde al vector de base $b_{índice}$ y un parámetro $\psi_{j'}$ para el índice j' se fija como un coeficiente de un vector de base b^*_{att} de la base B* que corresponde al vector de base b_{att} y calcular un producto de operaciones de emparejamiento sobre pares correspondientes de los vectores de base del vector de lado de transmisión t_j para el índice j y el vector de lado de recepción $r_{j'}$ para el índice j' que corresponde al índice j.

Fig. 1

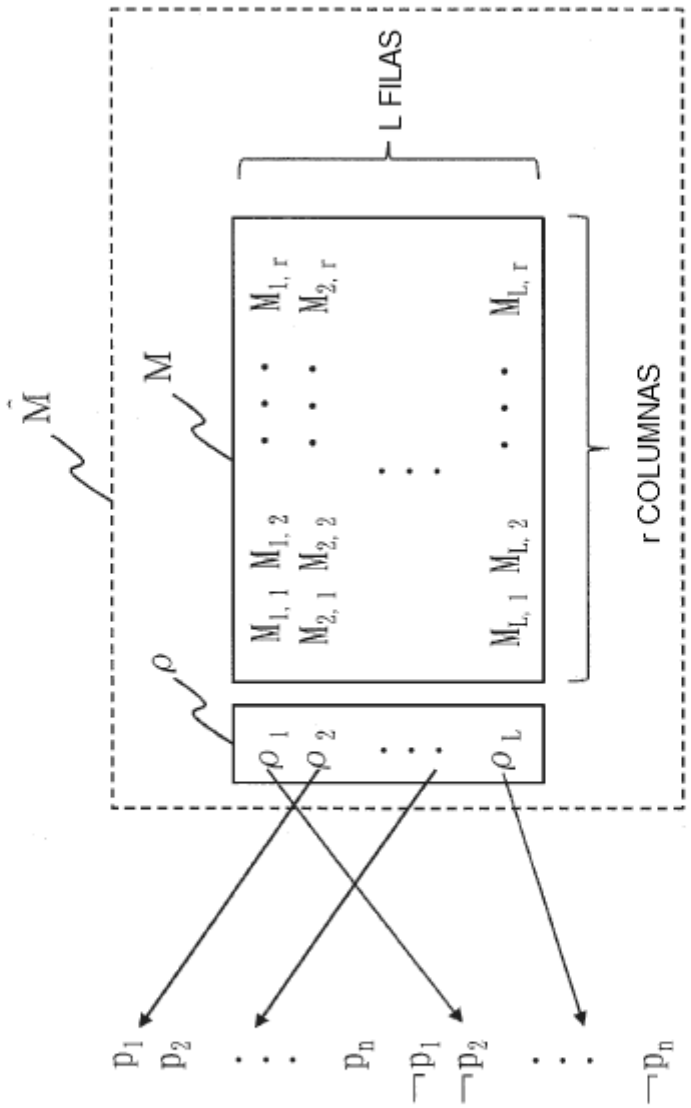

M̃
M
ρ
L FILAS
r COLUMNAS
ρ 1
ρ 2
ρ L
M1, 1 M1, 2 M1, r
M2, 1 M2, 2 M2, r
ML, 1 ML, 2 ML, r
p1
p2
pn
¬p1
¬p2
¬pn

Fig. 2

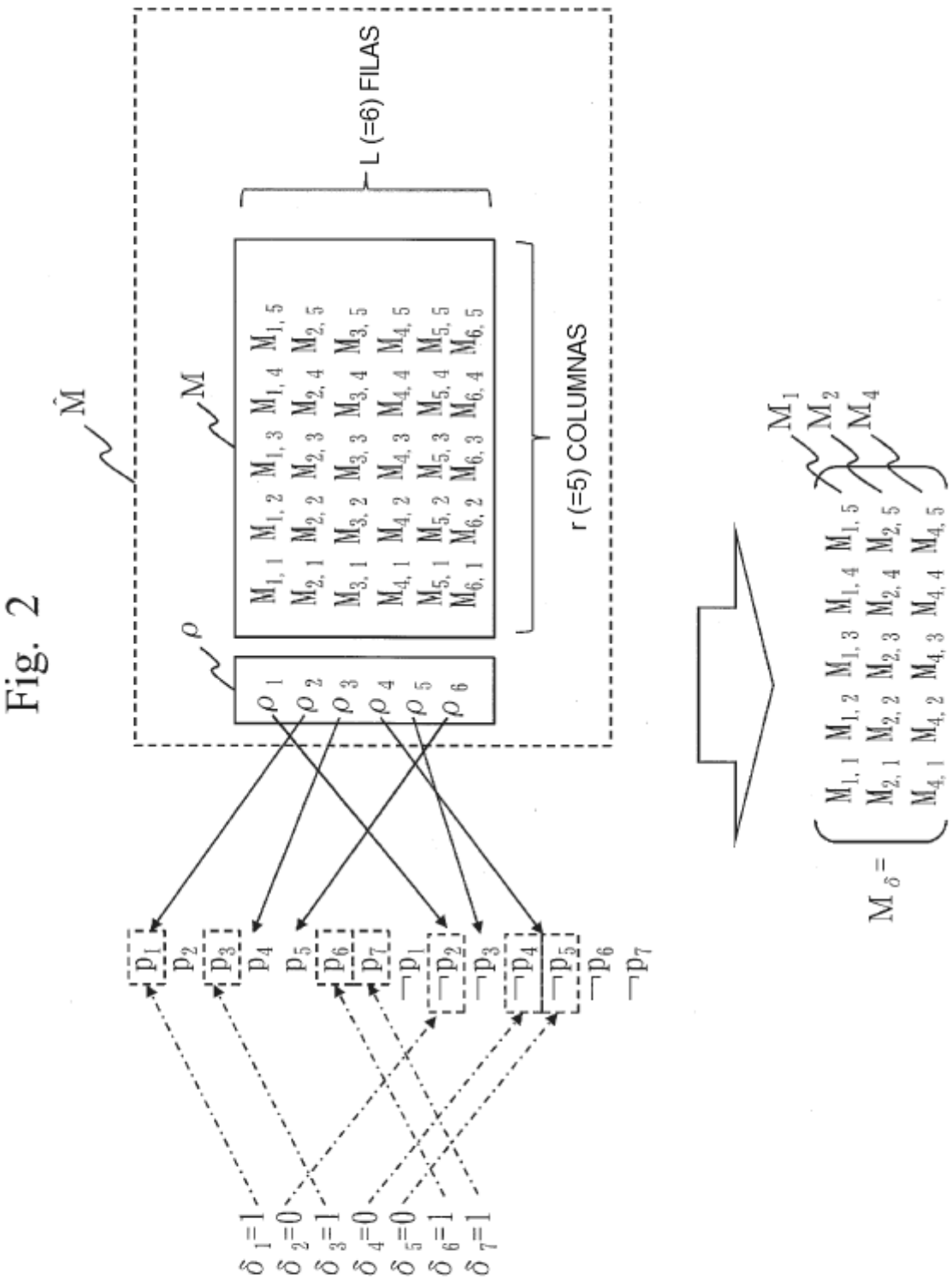

M̃
M
L (=6) FILAS
r (=5) COLUMNAS
ρ
ρ 1 ρ 2 ρ 3 ρ 4 ρ 5 ρ 6
p1 p2 p3 p4 p5 p6 p7 ¬p1 ¬p2 ¬p3 ¬p4 ¬p5 ¬p6 ¬p7
δ 1=1 δ 2=0 δ 3=1 δ 4=0 δ 5=0 δ 6=1 δ 7=1
M1 M2 M4
M δ=

Fig. 3

$$s_0 = \begin{pmatrix} \overbrace{1, \ldots, 1}^{r \text{ COLUMNAS}} \end{pmatrix} \begin{pmatrix} f_1 \\ \cdot \\ \cdot \\ \cdot \\ f_r \end{pmatrix} = \sum_{k=1}^{r} f_k$$

Fig. 4

$$\vec{s} = \vec{T} \begin{pmatrix} M_{1,1} & M_{1,2} & \cdots & M_{1,r} \\ M_{2,1} & M_{2,2} & \cdots & M_{2,r} \\ & & \vdots & \\ M_{L,1} & M_{L,2} & \cdots & M_{L,r} \end{pmatrix} \begin{pmatrix} f_1 \\ \cdot \\ \cdot \\ \cdot \\ f_r \end{pmatrix} = \begin{pmatrix} s_1 \\ \cdot \\ \cdot \\ \cdot \\ s_L \end{pmatrix}$$

Fig. 5

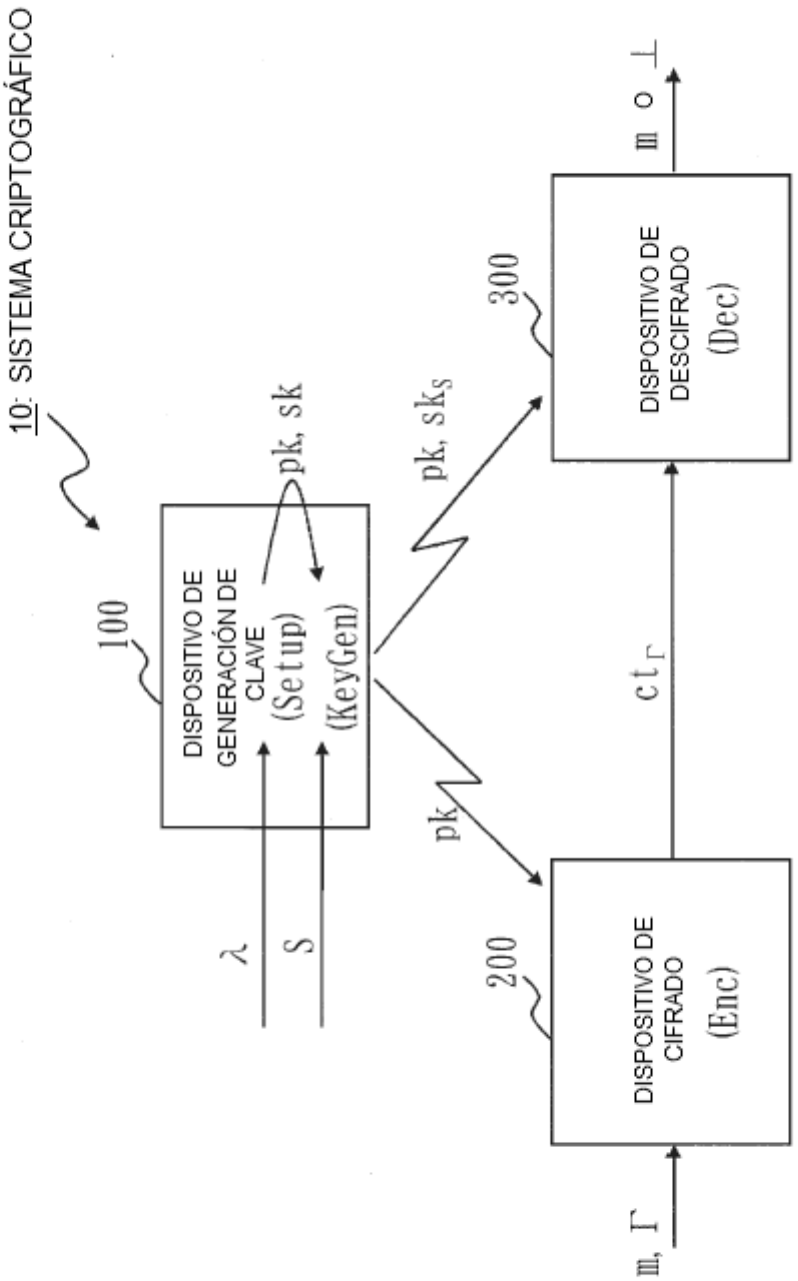

10: SISTEMA CRIPTOGRÁFICO
100
DISPOSITIVO DE GENERACIÓN DE CLAVE
(Setup)
(KeyGen)
pk, sk
pk, sk$_S$
pk
λ
S
200
DISPOSITIVO DE CIFRADO
(Enc)
m, Γ
ct$_\Gamma$
300
DISPOSITIVO DE DESCIFRADO
(Dec)
m o ⊥

Fig. 6

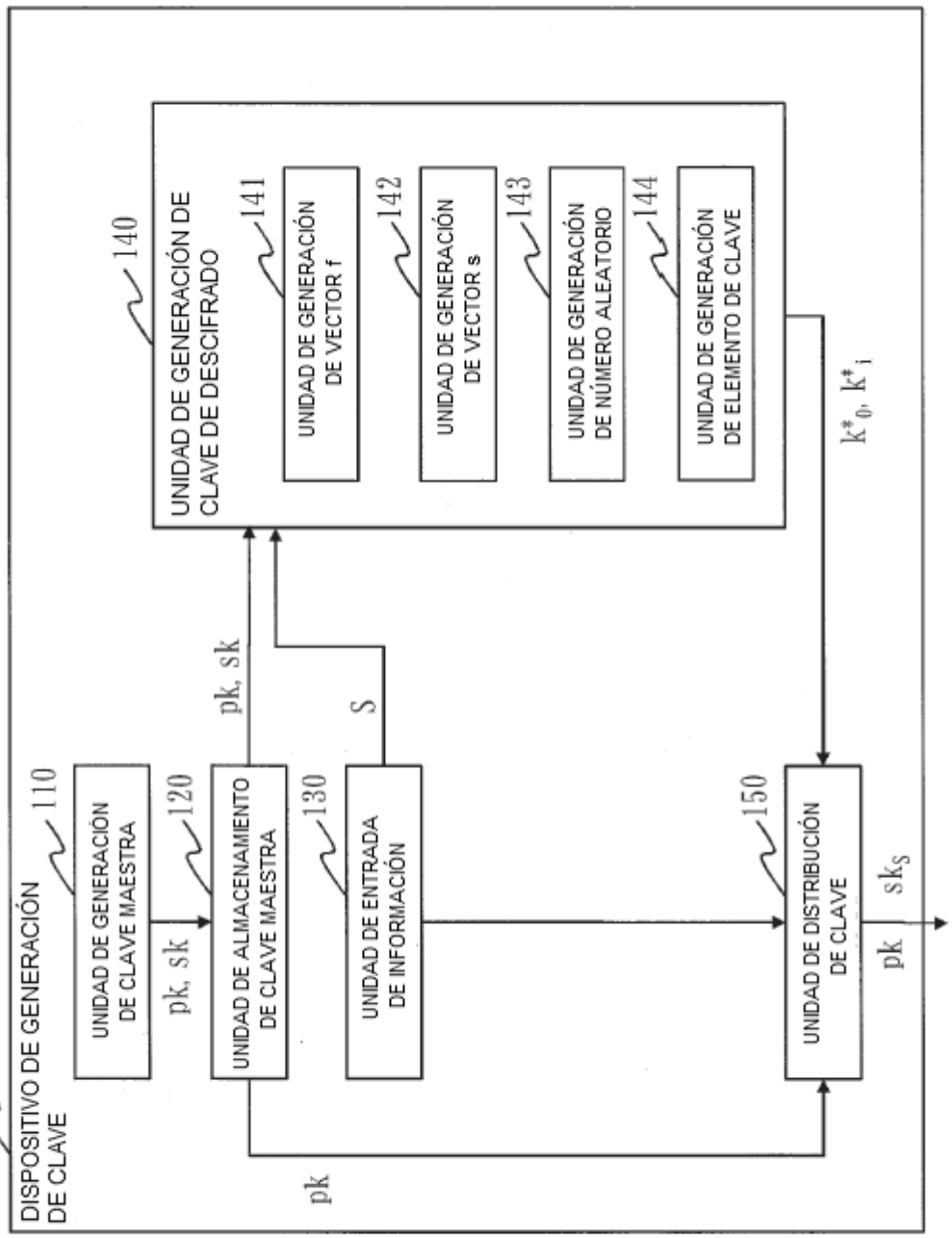

100
DISPOSITIVO DE GENERACIÓN DE CLAVE
110
UNIDAD DE GENERACIÓN DE CLAVE MAESTRA
120
UNIDAD DE ALMACENAMIENTO DE CLAVE MAESTRA
130
UNIDAD DE ENTRADA DE INFORMACIÓN
140
UNIDAD DE GENERACIÓN DE CLAVE DE DESCIFRADO
141
UNIDAD DE GENERACIÓN DE VECTOR f
142
UNIDAD DE GENERACIÓN DE VECTOR s
143
UNIDAD DE GENERACIÓN DE NÚMERO ALEATORIO
144
UNIDAD DE GENERACIÓN DE ELEMENTO DE CLAVE
150
UNIDAD DE DISTRIBUCIÓN DE CLAVE
pk, sk
pk, sk
S
pk
pk
sk_S
k*_0, k*_i

Fig. 7

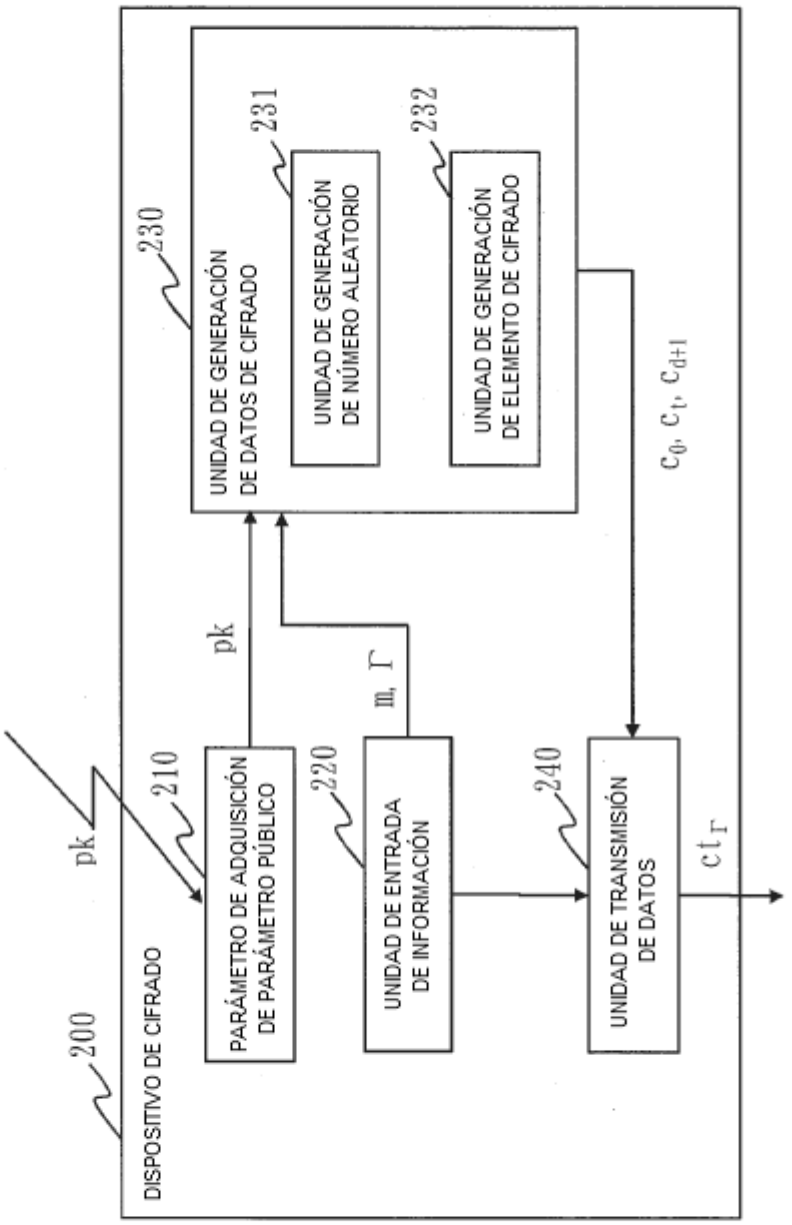

DISPOSITIVO DE CIFRADO
200
pk
PARÁMETRO DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
210
pk
UNIDAD DE ENTRADA DE INFORMACIÓN
220
m, r
UNIDAD DE GENERACIÓN DE DATOS DE CIFRADO
230
UNIDAD DE GENERACIÓN DE NÚMERO ALEATORIO
231
UNIDAD DE GENERACIÓN DE ELEMENTO DE CIFRADO
232
c_0, c_t, c_{d+1}
UNIDAD DE TRANSMISIÓN DE DATOS
240
ct_r

Fig. 8

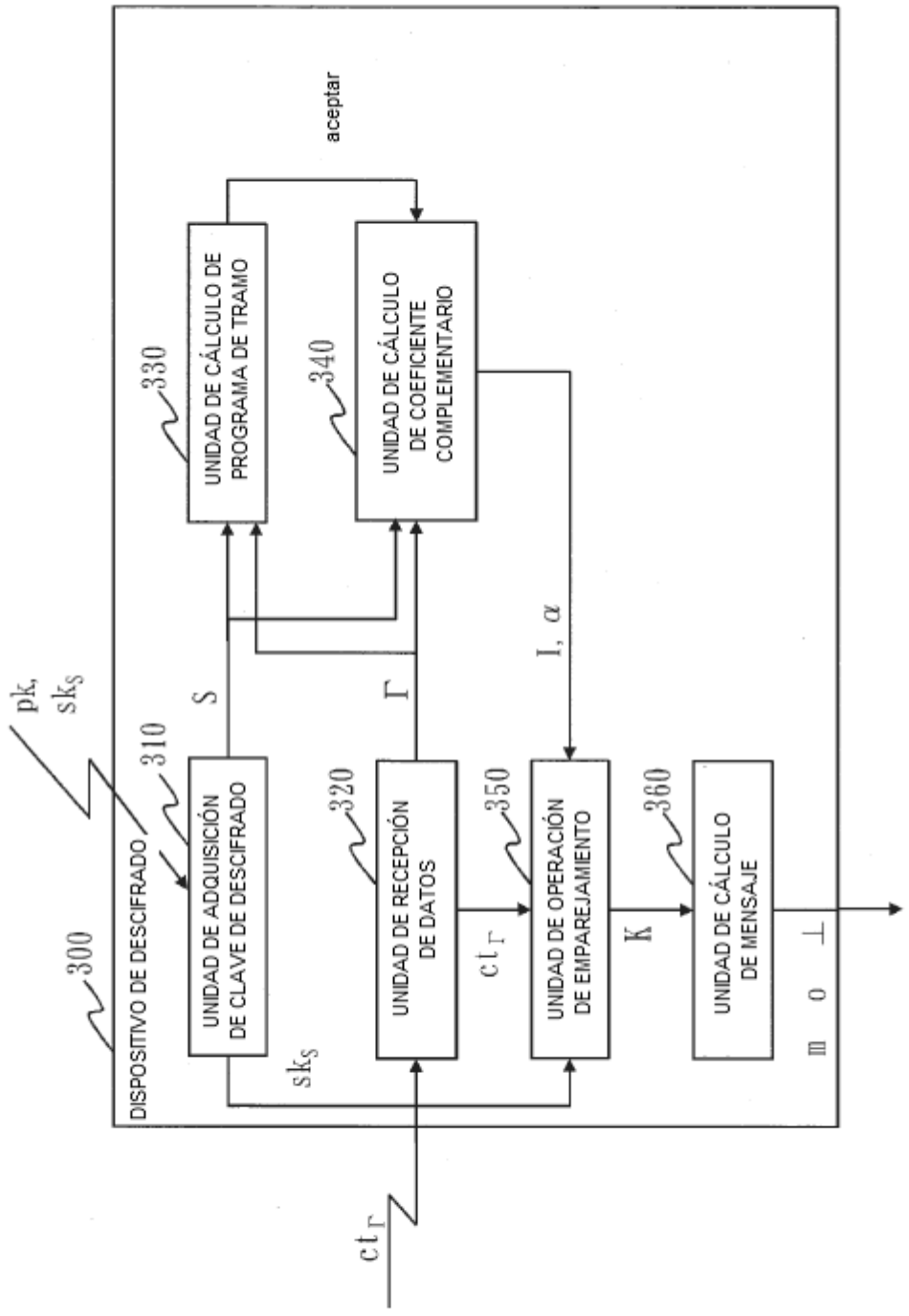

DISPOSITIVO DE DESCIFRADO
300
UNIDAD DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
310
UNIDAD DE RECEPCIÓN DE DATOS
320
UNIDAD DE CÁLCULO DE PROGRAMA DE TRAMO
330
UNIDAD DE CÁLCULO DE COEFICIENTE COMPLEMENTARIO
340
UNIDAD DE OPERACIÓN DE EMPAREJAMIENTO
350
UNIDAD DE CÁLCULO DE MENSAJE
360
pk, sk_S
S
Γ
l, α
aceptar
sk_S
ct_Γ
K
m o ⊥

Fig. 9

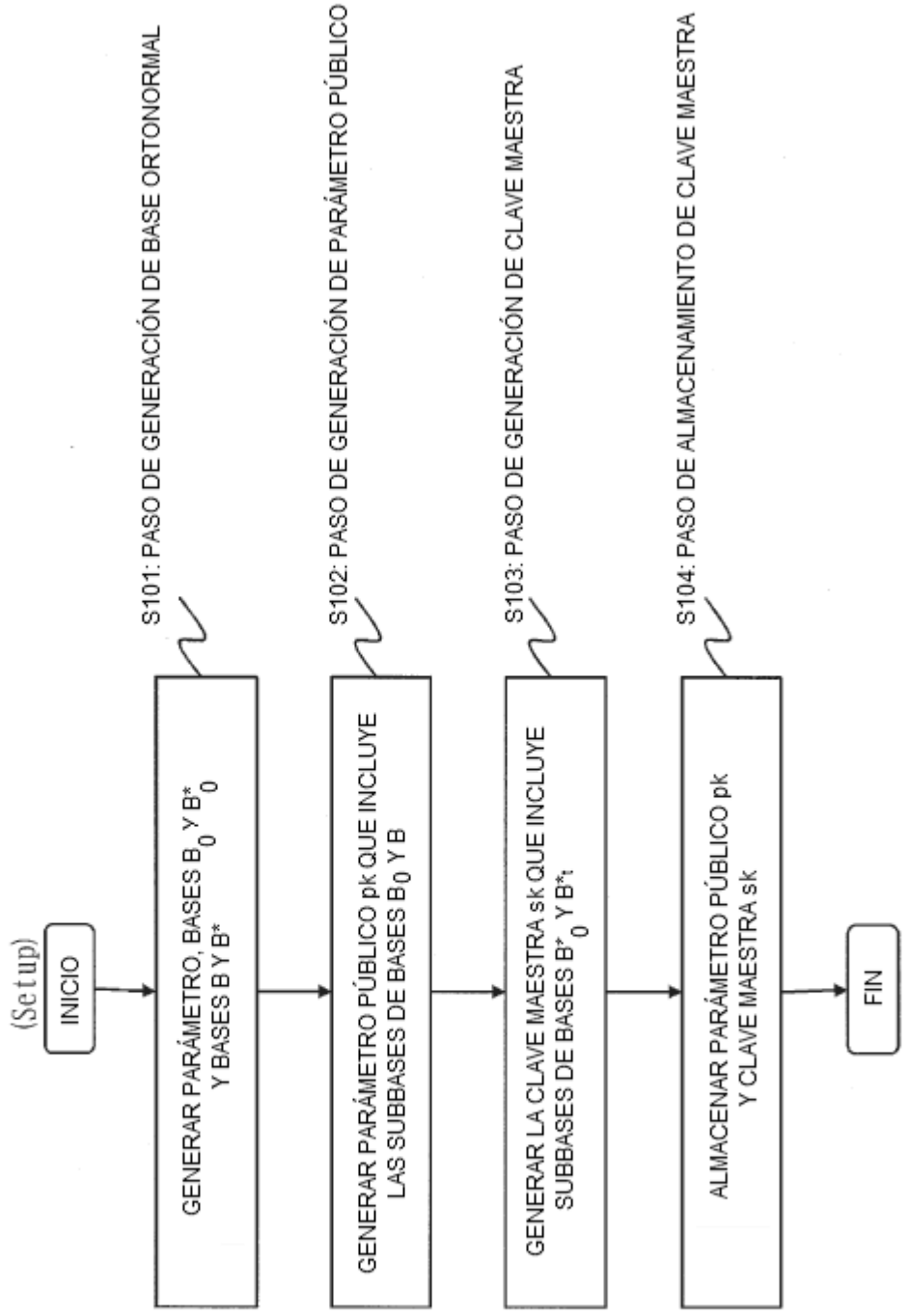

(Setup)
INICIO
S101: PASO DE GENERACIÓN DE BASE ORTONORMAL
GENERAR PARÁMETRO, BASES B_0 Y B^*_0 Y BASES B Y B*
S102: PASO DE GENERACIÓN DE PARÁMETRO PÚBLICO
GENERAR PARÁMETRO PÚBLICO pk QUE INCLUYE LAS SUBBASES DE BASES B_0 Y B
S103: PASO DE GENERACIÓN DE CLAVE MAESTRA
GENERAR LA CLAVE MAESTRA sk QUE INCLUYE SUBBASES DE BASES B^*_0 Y B^*_1
S104: PASO DE ALMACENAMIENTO DE CLAVE MAESTRA
ALMACENAR PARÁMETRO PÚBLICO pk Y CLAVE MAESTRA sk
FIN

Fig. 10

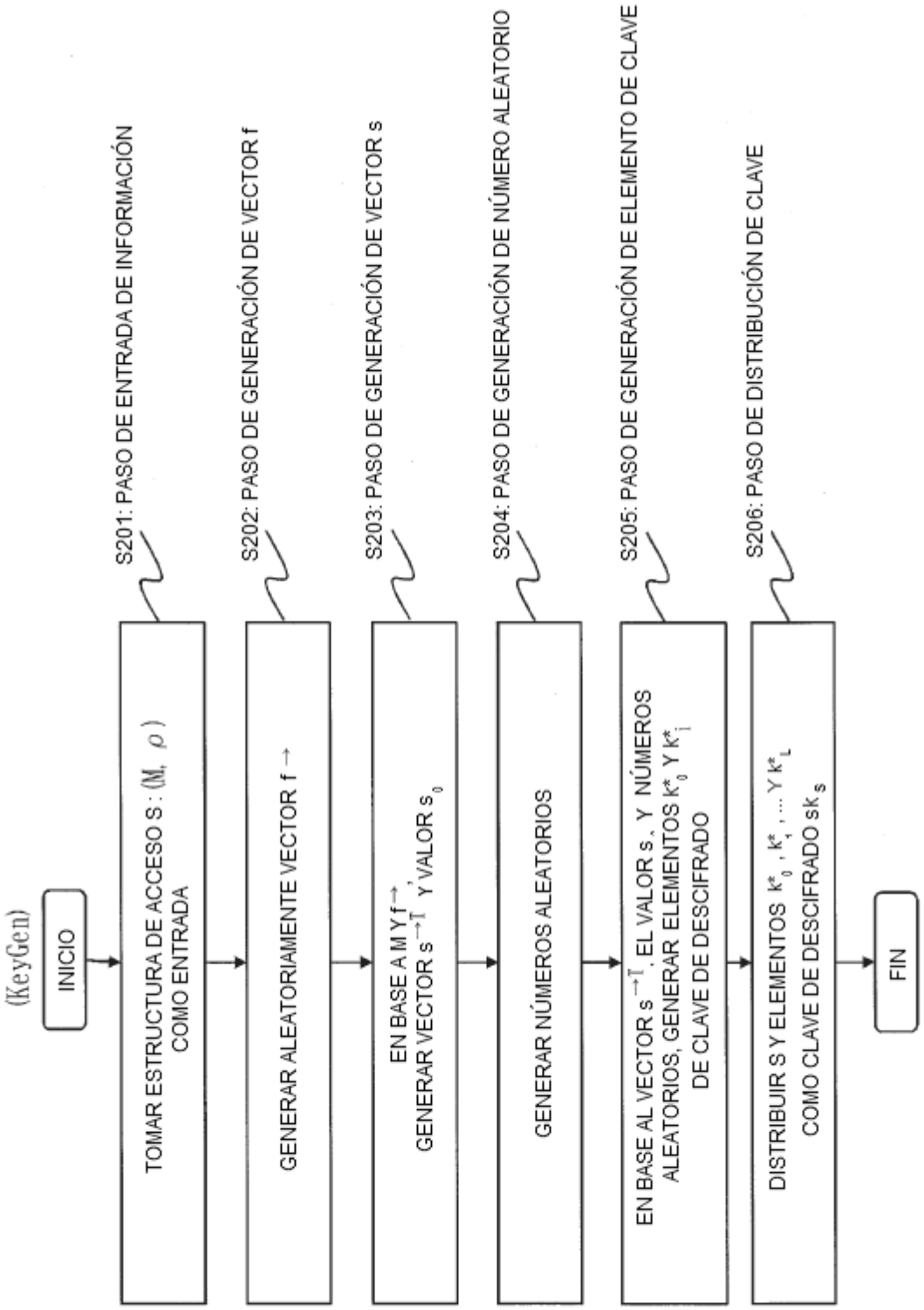

(KeyGen)
INICIO
S201: PASO DE ENTRADA DE INFORMACIÓN
TOMAR ESTRUCTURA DE ACCESO S : (M, ρ)
COMO ENTRADA
S202: PASO DE GENERACIÓN DE VECTOR f
GENERAR ALEATORIAMENTE VECTOR f →
S203: PASO DE GENERACIÓN DE VECTOR s
EN BASE A M Y f →,
GENERAR VECTOR s →T Y VALOR s0
S204: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S205: PASO DE GENERACIÓN DE ELEMENTO DE CLAVE
EN BASE AL VECTOR s →T, EL VALOR s , Y NÚMEROS
ALEATORIOS, GENERAR ELEMENTOS k*0 Y k*i
DE CLAVE DE DESCIFRADO
S206: PASO DE DISTRIBUCIÓN DE CLAVE
DISTRIBUIR S Y ELEMENTOS k*0 , k*1 , ... Y k*L
COMO CLAVE DE DESCIFRADO sk s
FIN

Fig. 11

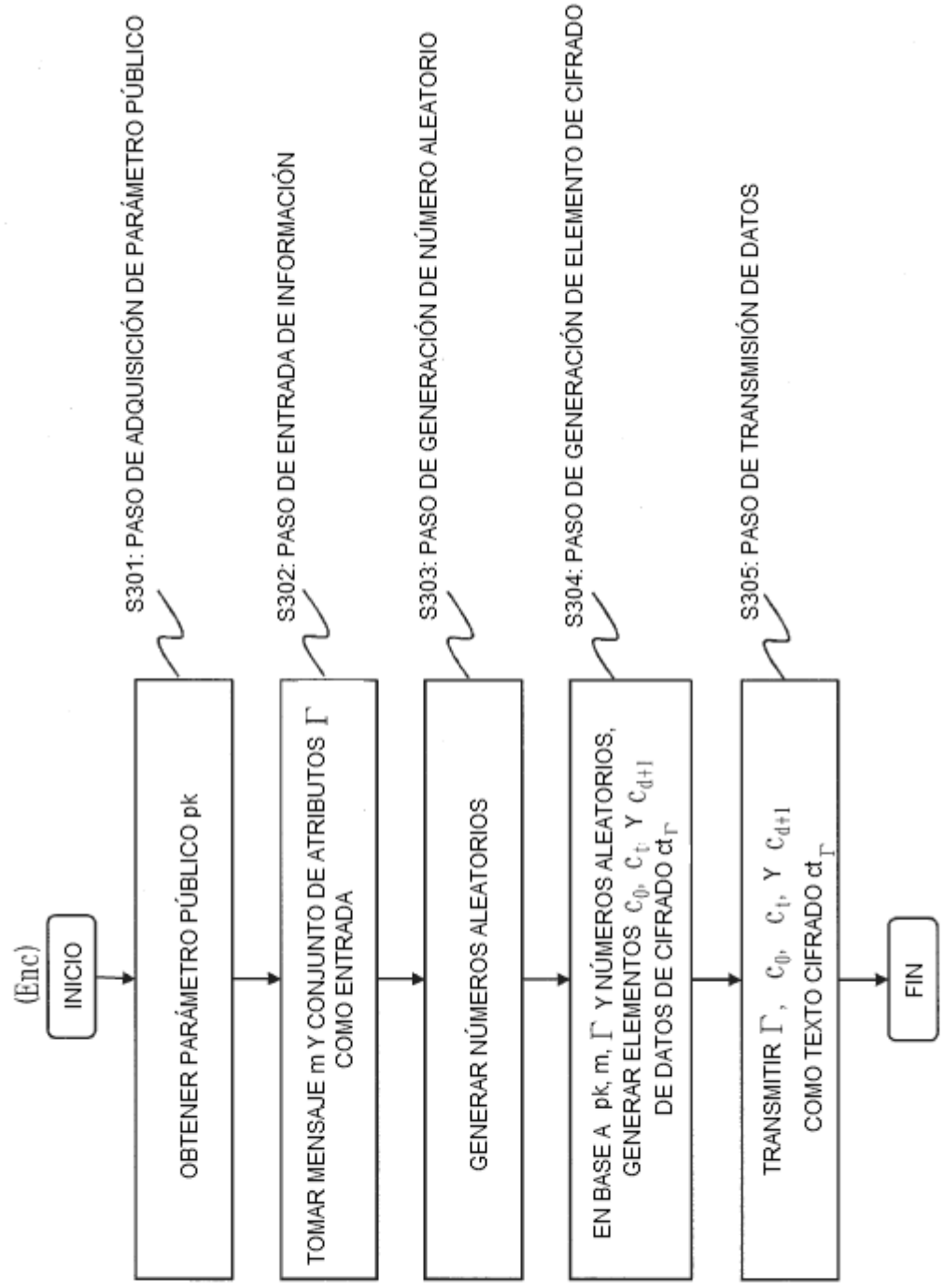

(Enc)
INICIO
S301: PASO DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
OBTENER PARÁMETRO PÚBLICO pk
S302: PASO DE ENTRADA DE INFORMACIÓN
TOMAR MENSAJE m Y CONJUNTO DE ATRIBUTOS Γ COMO ENTRADA
S303: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S304: PASO DE GENERACIÓN DE ELEMENTO DE CIFRADO
EN BASE A pk, m, Γ Y NÚMEROS ALEATORIOS, GENERAR ELEMENTOS c_0, c_1, Y c_{d+1} DE DATOS DE CIFRADO ct_Γ
S305: PASO DE TRANSMISIÓN DE DATOS
TRANSMITIR Γ, c_0, c_1, Y c_{d+1} COMO TEXTO CIFRADO ct_Γ
FIN

Fig. 12

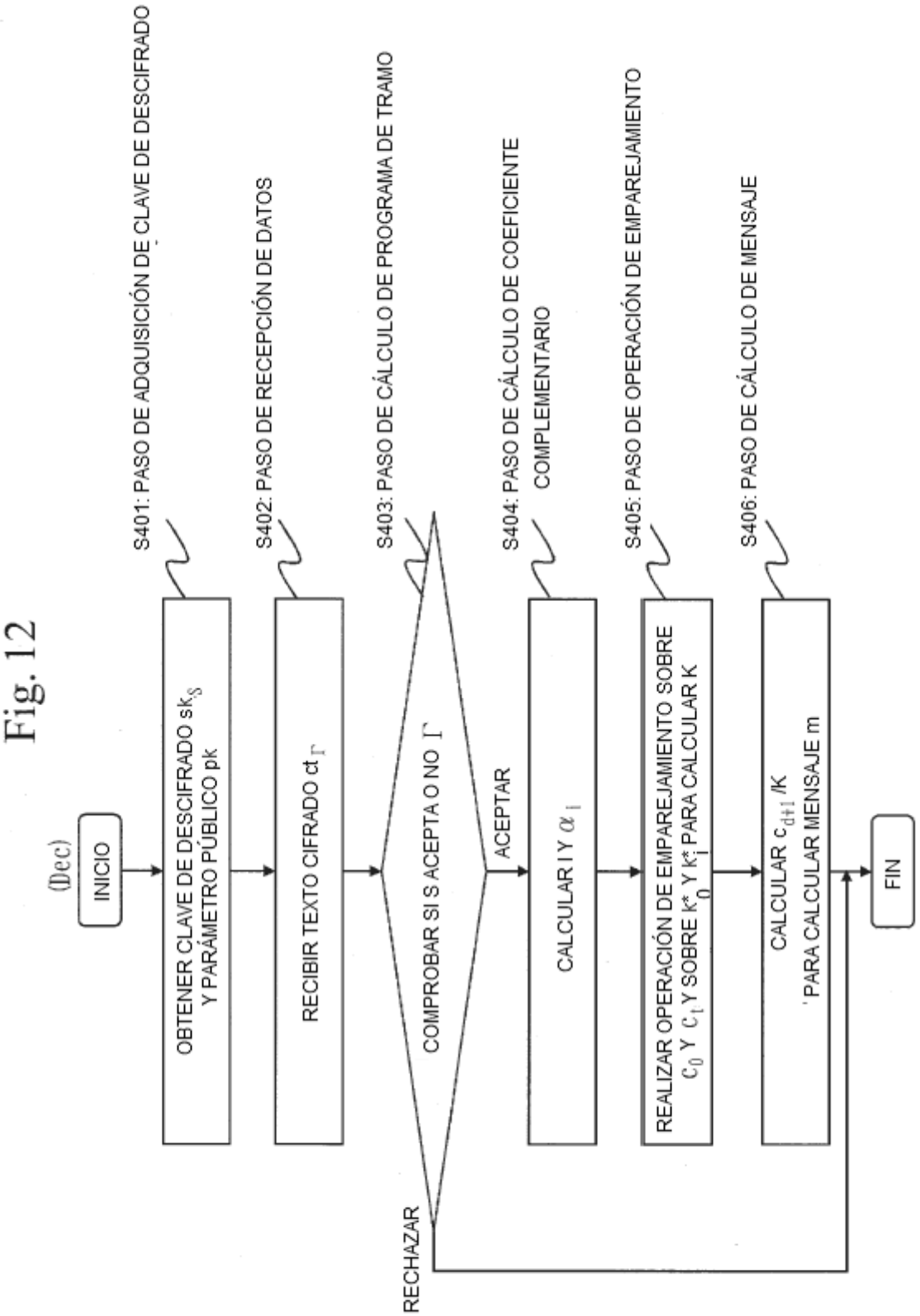

(Dec)
INICIO
S401: PASO DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
OBTENER CLAVE DE DESCIFRADO sk_S Y PARÁMETRO PÚBLICO pk
S402: PASO DE RECEPCIÓN DE DATOS
RECIBIR TEXTO CIFRADO ct_Γ
S403: PASO DE CÁLCULO DE PROGRAMA DE TRAMO
COMPROBAR SI S ACEPTA O NO Γ
ACEPTAR
RECHAZAR
S404: PASO DE CÁLCULO DE COEFICIENTE COMPLEMENTARIO
CALCULAR I Y α_I
S405: PASO DE OPERACIÓN DE EMPAREJAMIENTO
REALIZAR OPERACIÓN DE EMPAREJAMIENTO SOBRE c_0 Y c_1 Y SOBRE k_0^* Y k_1^* PARA CALCULAR K
S406: PASO DE CÁLCULO DE MENSAJE
CALCULAR c_{d+1} /K
' PARA CALCULAR MENSAJE m
FIN

Fig. 13

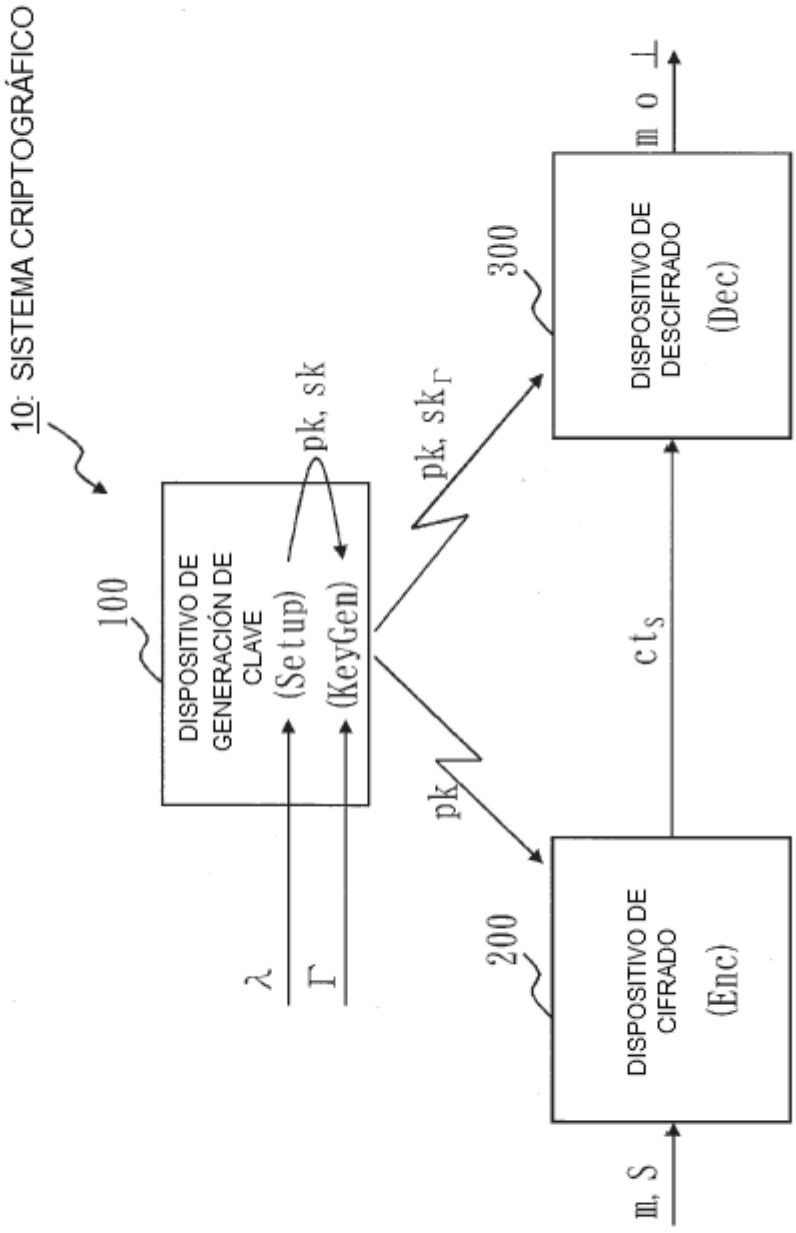

10: SISTEMA CRIPTOGRÁFICO
100
DISPOSITIVO DE GENERACIÓN DE CLAVE
(Setup)
(KeyGen)
pk, sk
pk, sk_Γ
pk
λ
Γ
200
DISPOSITIVO DE CIFRADO
(Enc)
m, S
ct_S
300
DISPOSITIVO DE DESCIFRADO
(Dec)
m o ⊥

Fig.14

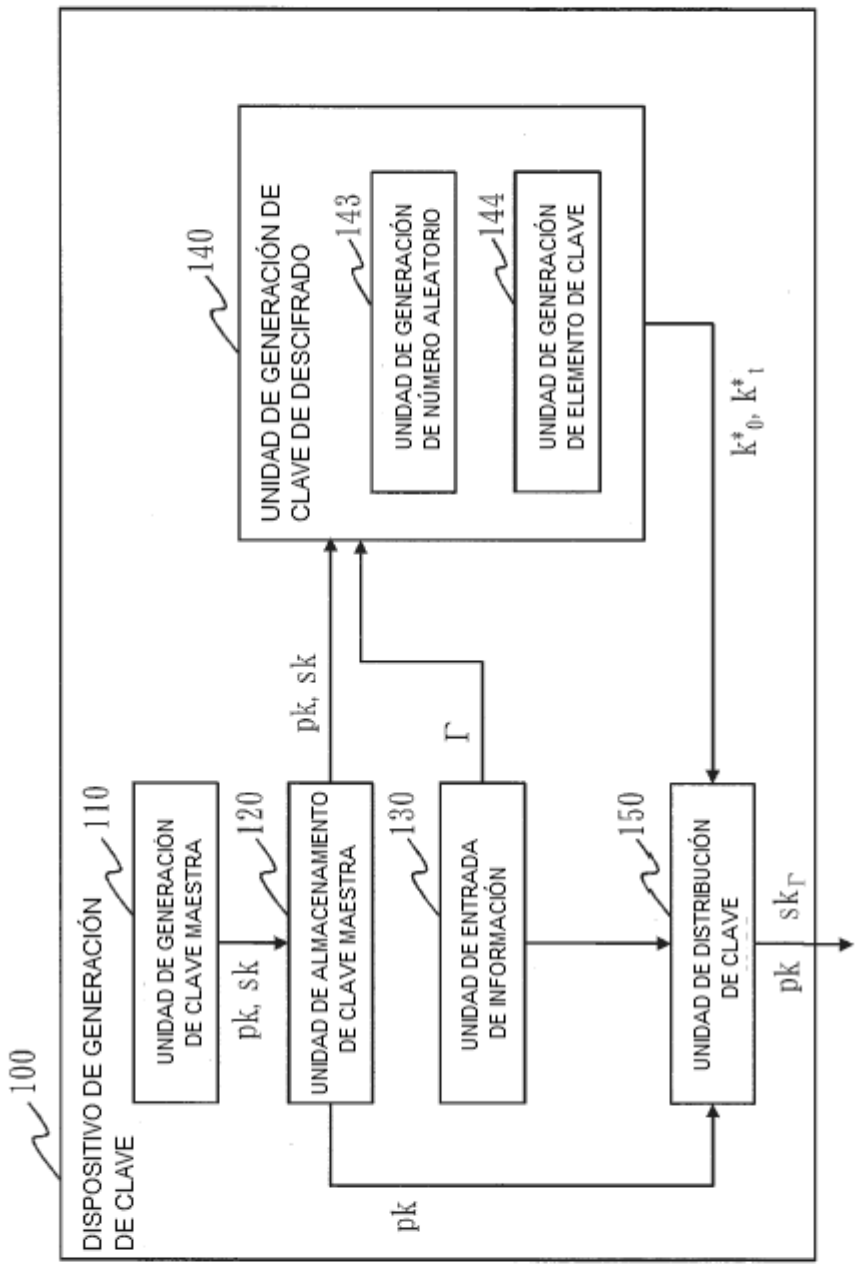

100
DISPOSITIVO DE GENERACIÓN DE CLAVE
110
UNIDAD DE GENERACIÓN DE CLAVE MAESTRA
120
UNIDAD DE ALMACENAMIENTO DE CLAVE MAESTRA
130
UNIDAD DE ENTRADA DE INFORMACIÓN
140
UNIDAD DE GENERACIÓN DE CLAVE DE DESCIFRADO
143
UNIDAD DE GENERACIÓN DE NÚMERO ALEATORIO
144
UNIDAD DE GENERACIÓN DE ELEMENTO DE CLAVE
150
UNIDAD DE DISTRIBUCIÓN DE CLAVE
pk, sk
pk, sk
Γ
pk
k^*_0, k^*_1
pk
sk_Γ

Fig. 15

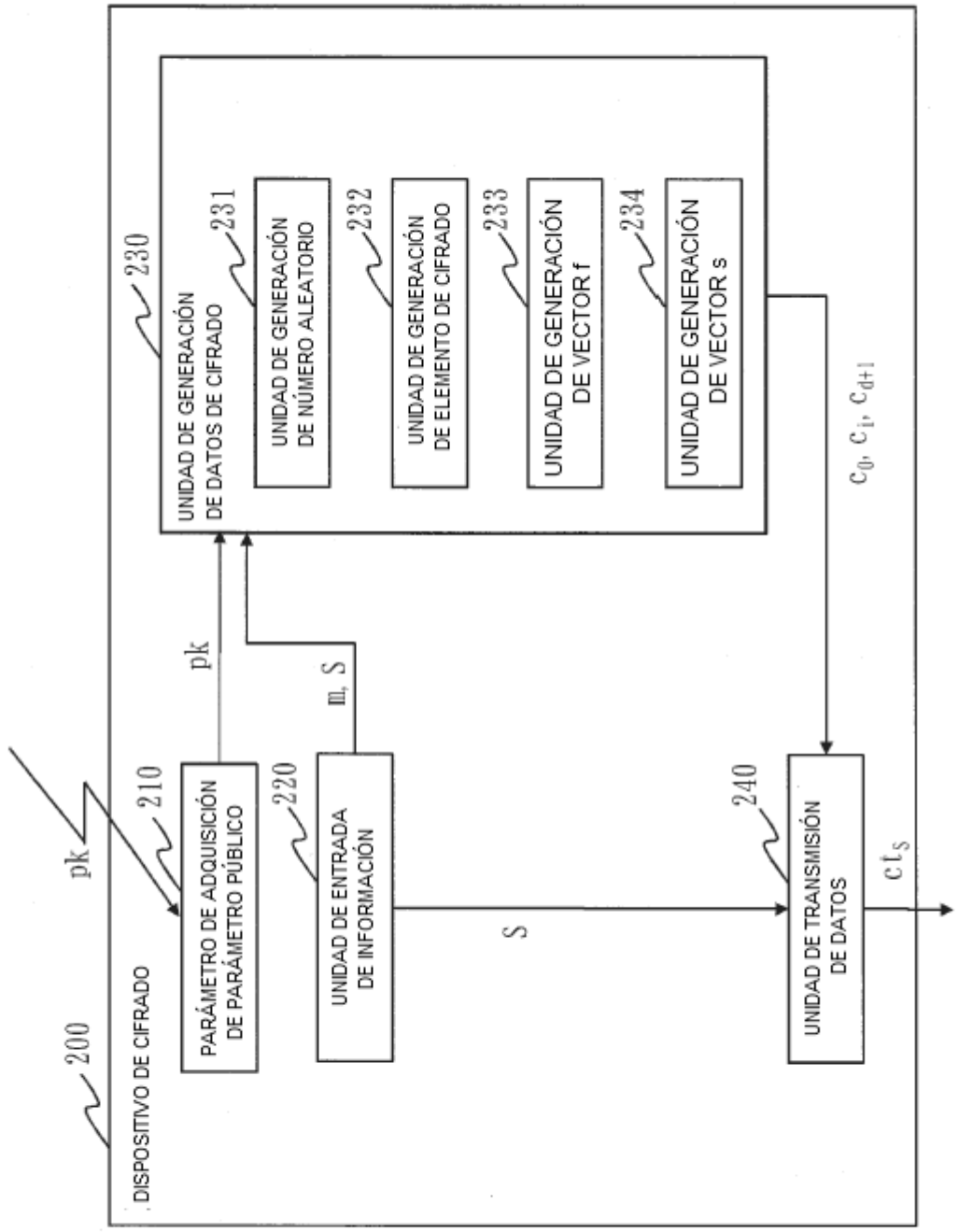

200
DISPOSITIVO DE CIFRADO
pk
210
PARÁMETRO DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
pk
220
UNIDAD DE ENTRADA DE INFORMACIÓN
m, S
S
230
UNIDAD DE GENERACIÓN DE DATOS DE CIFRADO
231
UNIDAD DE GENERACIÓN DE NÚMERO ALEATORIO
232
UNIDAD DE GENERACIÓN DE ELEMENTO DE CIFRADO
233
UNIDAD DE GENERACIÓN DE VECTOR f
234
UNIDAD DE GENERACIÓN DE VECTOR s
c_0, c_1, c_{d+1}
240
UNIDAD DE TRANSMISIÓN DE DATOS
ct_S

Fig. 16

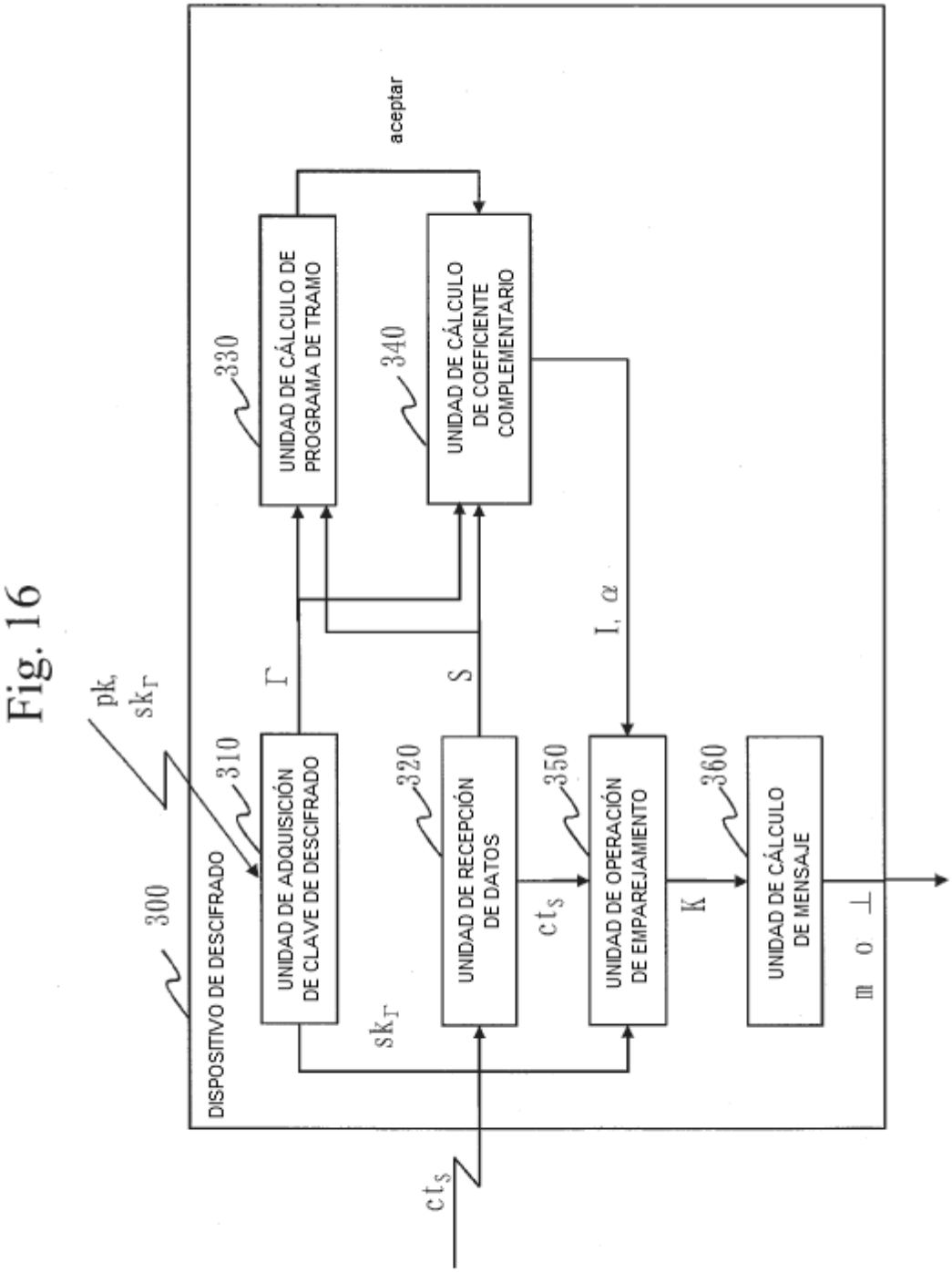

pk,
sk$_\Gamma$
300
DISPOSITIVO DE DESCIFRADO
310
UNIDAD DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
320
UNIDAD DE RECEPCIÓN DE DATOS
350
UNIDAD DE OPERACIÓN DE EMPAREJAMIENTO
360
UNIDAD DE CÁLCULO DE MENSAJE
330
UNIDAD DE CÁLCULO DE PROGRAMA DE TRAMO
340
UNIDAD DE CÁLCULO DE COEFICIENTE COMPLEMENTARIO
aceptar
Γ
S
I, α
sk$_\Gamma$
ct$_S$
K
m o ⊥
ct$_S$

Fig. 17

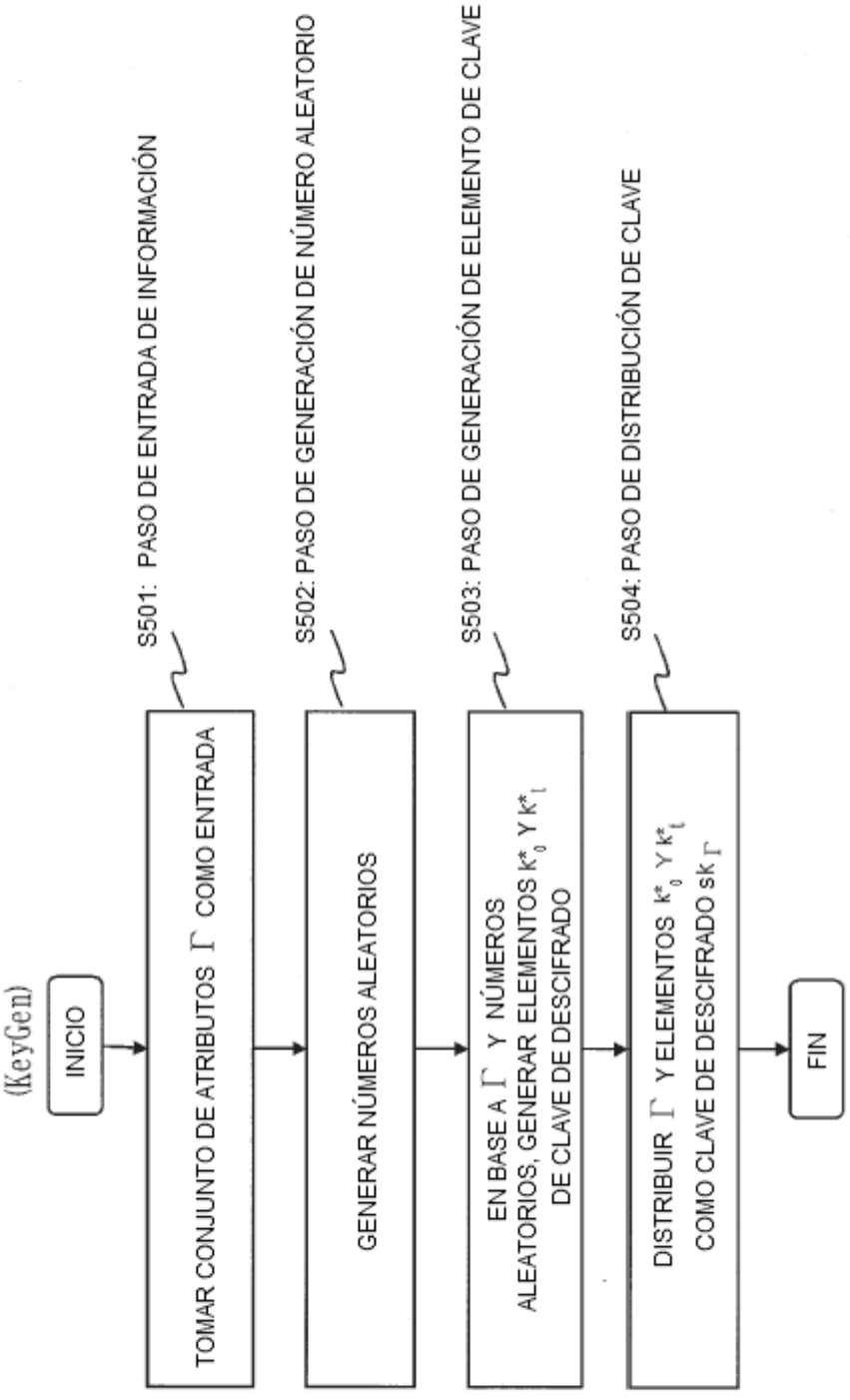

(KeyGen)
INICIO
S501: PASO DE ENTRADA DE INFORMACIÓN
TOMAR CONJUNTO DE ATRIBUTOS Γ COMO ENTRADA
S502: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S503: PASO DE GENERACIÓN DE ELEMENTO DE CLAVE
EN BASE A Γ Y NÚMEROS ALEATORIOS, GENERAR ELEMENTOS k*0 Y k*1 DE CLAVE DE DESCIFRADO
S504: PASO DE DISTRIBUCIÓN DE CLAVE
DISTRIBUIR Γ Y ELEMENTOS k*0 Y k*1 COMO CLAVE DE DESCIFRADO skΓ
FIN

Fig. 18

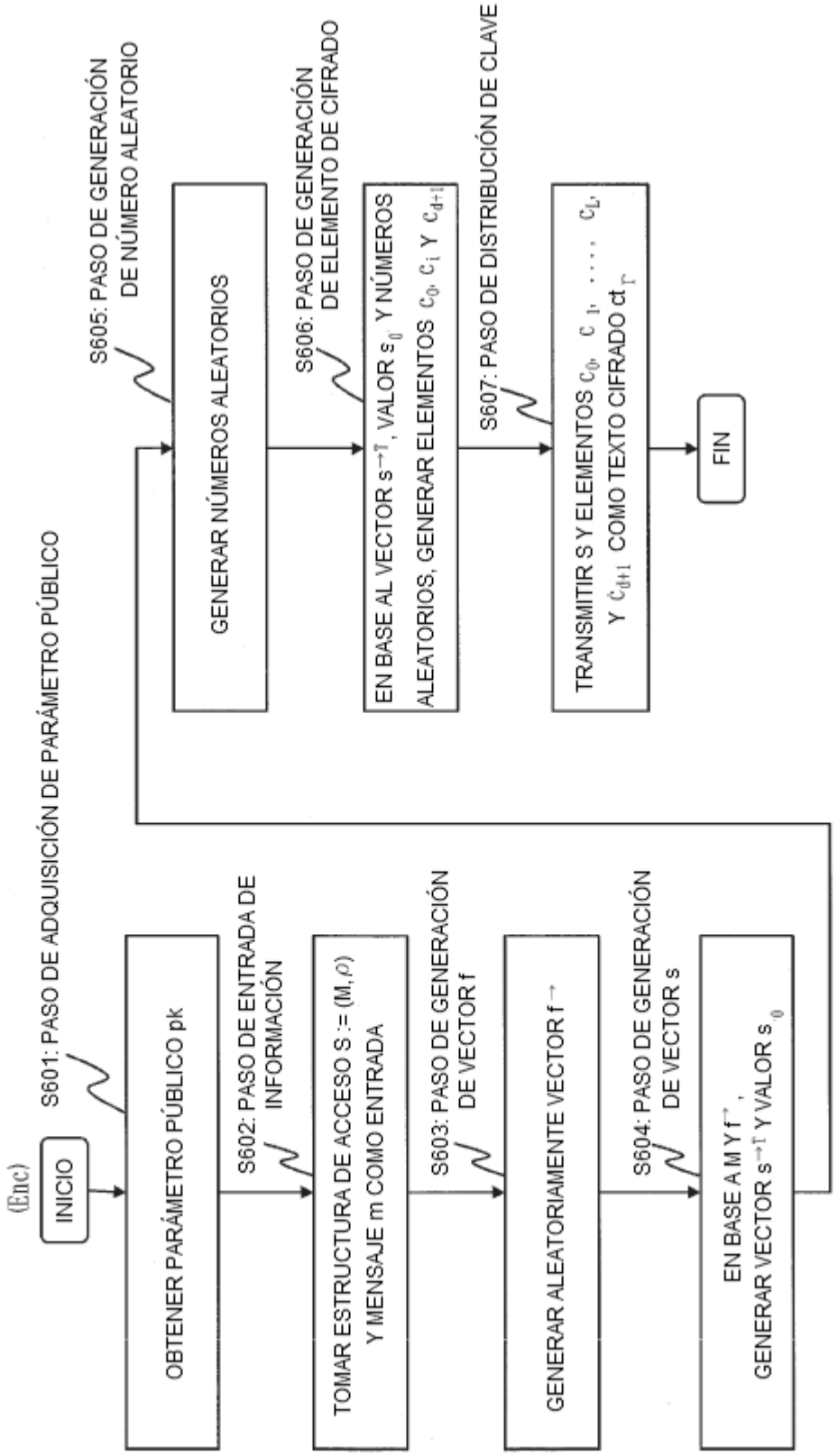

(Enc)
INICIO
S601: PASO DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
OBTENER PARÁMETRO PÚBLICO pk
S602: PASO DE ENTRADA DE INFORMACIÓN
TOMAR ESTRUCTURA DE ACCESO S := (M, ρ) Y MENSAJE m COMO ENTRADA
S603: PASO DE GENERACIÓN DE VECTOR f
GENERAR ALEATORIAMENTE VECTOR f→
S604: PASO DE GENERACIÓN DE VECTOR s
EN BASE A M Y f→, GENERAR VECTOR s→T Y VALOR s0
S605: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S606: PASO DE GENERACIÓN DE ELEMENTO DE CIFRADO
EN BASE AL VECTOR s→T, VALOR s0 Y NÚMEROS ALEATORIOS, GENERAR ELEMENTOS c0, ci Y cd+1
S607: PASO DE DISTRIBUCIÓN DE CLAVE
TRANSMITIR S Y ELEMENTOS c0, c1, ..., cL, Y cd+1 COMO TEXTO CIFRADO ctΓ
FIN

Fig. 19

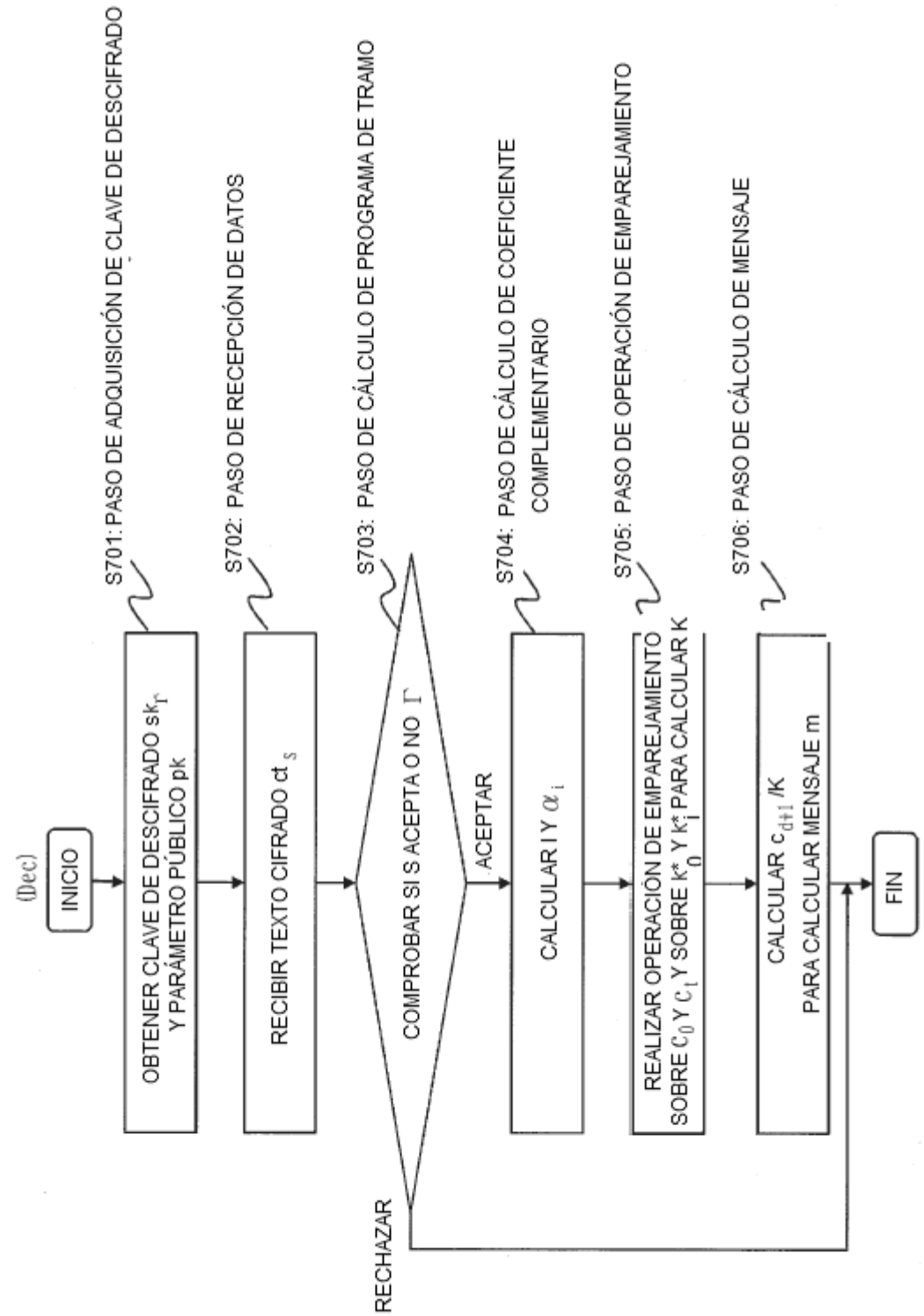

(Dec)
INICIO
S701: PASO DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
OBTENER CLAVE DE DESCIFRADO sk_Γ Y PARÁMETRO PÚBLICO pk
S702: PASO DE RECEPCIÓN DE DATOS
RECIBIR TEXTO CIFRADO ct_s
S703: PASO DE CÁLCULO DE PROGRAMA DE TRAMO
COMPROBAR SI S ACEPTA O NO Γ
RECHAZAR
ACEPTAR
S704: PASO DE CÁLCULO DE COEFICIENTE COMPLEMENTARIO
CALCULAR I Y α_i
S705: PASO DE OPERACIÓN DE EMPAREJAMIENTO
REALIZAR OPERACIÓN DE EMPAREJAMIENTO SOBRE c_0 Y c_t Y SOBRE k_0^* Y k_i^* PARA CALCULAR K
S706: PASO DE CÁLCULO DE MENSAJE
CALCULAR c_{d+1} /K PARA CALCULAR MENSAJE m
FIN

Fig. 20

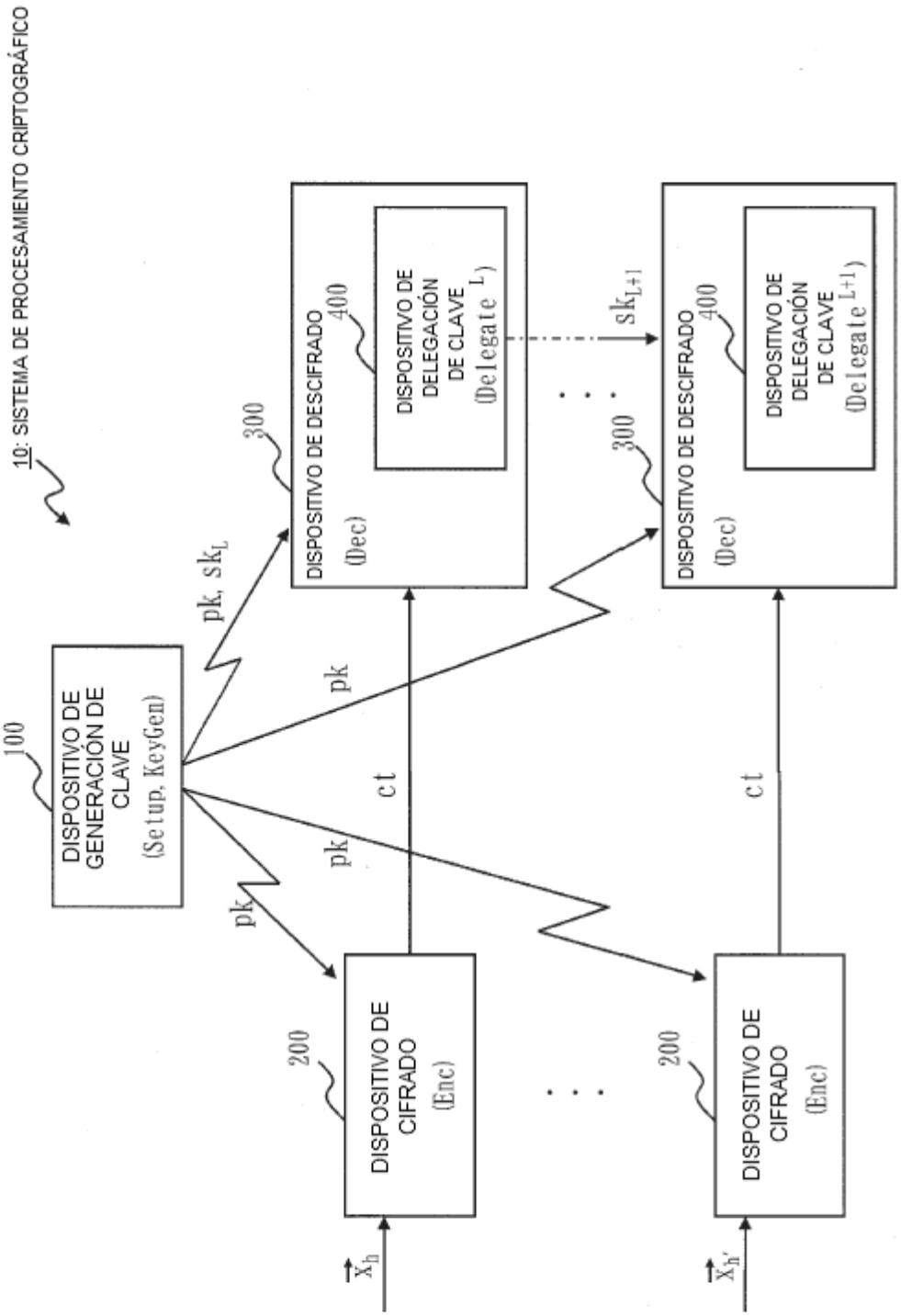

10: SISTEMA DE PROCESAMIENTO CRIPTOGRÁFICO
100
DISPOSITIVO DE GENERACIÓN DE CLAVE
(Setup, KeyGen)
pk, sk_L
300
DISPOSITIVO DE DESCIFRADO
(Dec)
400
DISPOSITIVO DE DELEGACIÓN DE CLAVE
(Delegate^L)
sk_{L+1}
300
DISPOSITIVO DE DESCIFRADO
(Dec)
400
DISPOSITIVO DE DELEGACIÓN DE CLAVE
(Delegate^{L+1})
pk
pk
pk
ct
ct
200
DISPOSITIVO DE CIFRADO
(Enc)
200
DISPOSITIVO DE CIFRADO
(Enc)
x_h
x_h'

Fig. 21

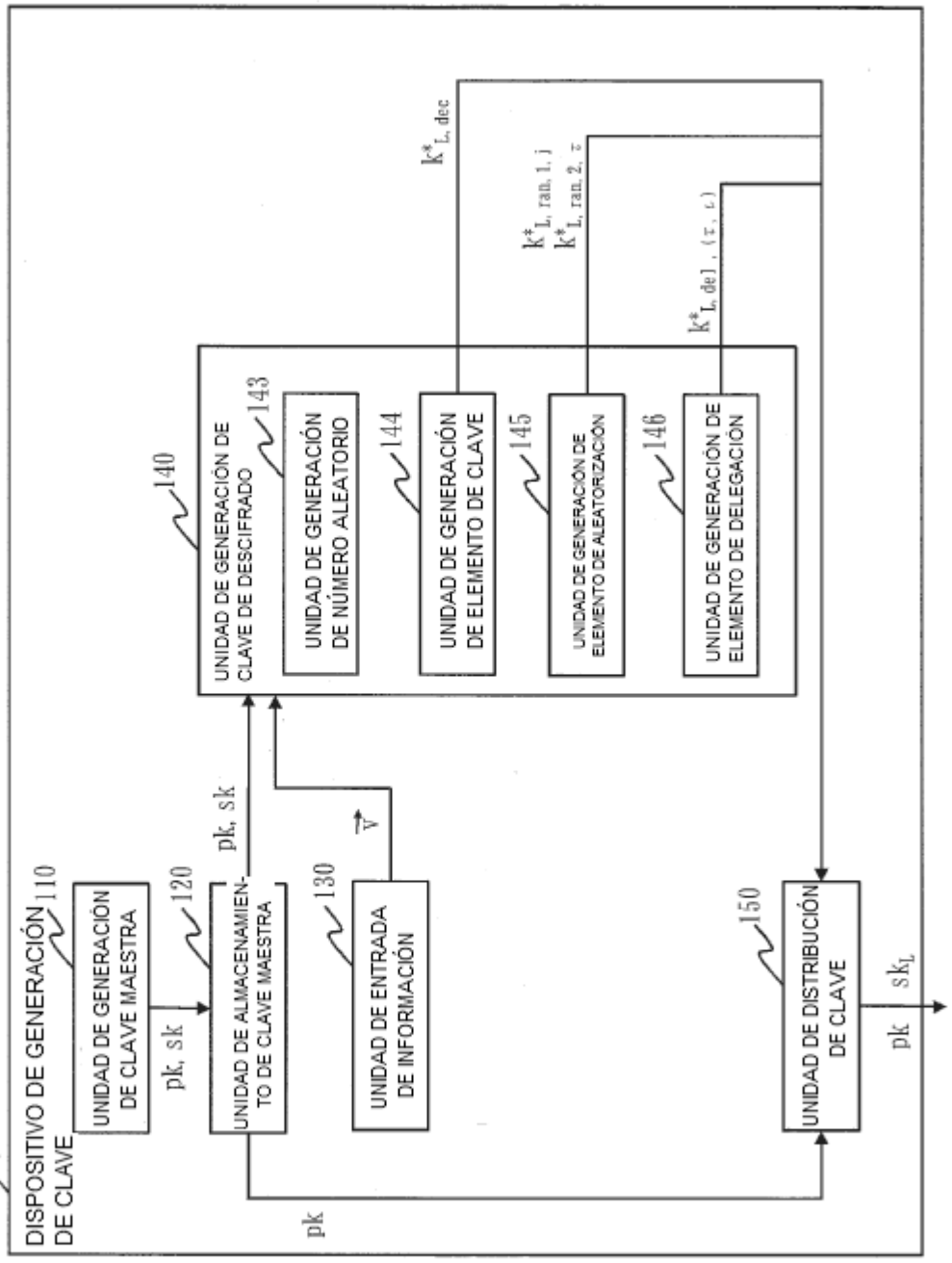

100
DISPOSITIVO DE GENERACIÓN DE CLAVE
110
UNIDAD DE GENERACIÓN DE CLAVE MAESTRA
pk, sk
120
UNIDAD DE ALMACENAMIENTO DE CLAVE MAESTRA
pk, sk
130
UNIDAD DE ENTRADA DE INFORMACIÓN
v
140
UNIDAD DE GENERACIÓN DE CLAVE DE DESCIFRADO
143
UNIDAD DE GENERACIÓN DE NÚMERO ALEATORIO
144
UNIDAD DE GENERACIÓN DE ELEMENTO DE CLAVE
145
UNIDAD DE GENERACIÓN DE ELEMENTO DE ALEATORIZACIÓN
146
UNIDAD DE GENERACIÓN DE ELEMENTO DE DELEGACIÓN
$k^*_{L,dec}$
$k^*_{L,ran.1,j}$
$k^*_{L,ran.2,\tau}$
$k^*_{L,del,(\tau,\epsilon)}$
150
UNIDAD DE DISTRIBUCIÓN DE CLAVE
pk
sk_L
pk

Fig. 22

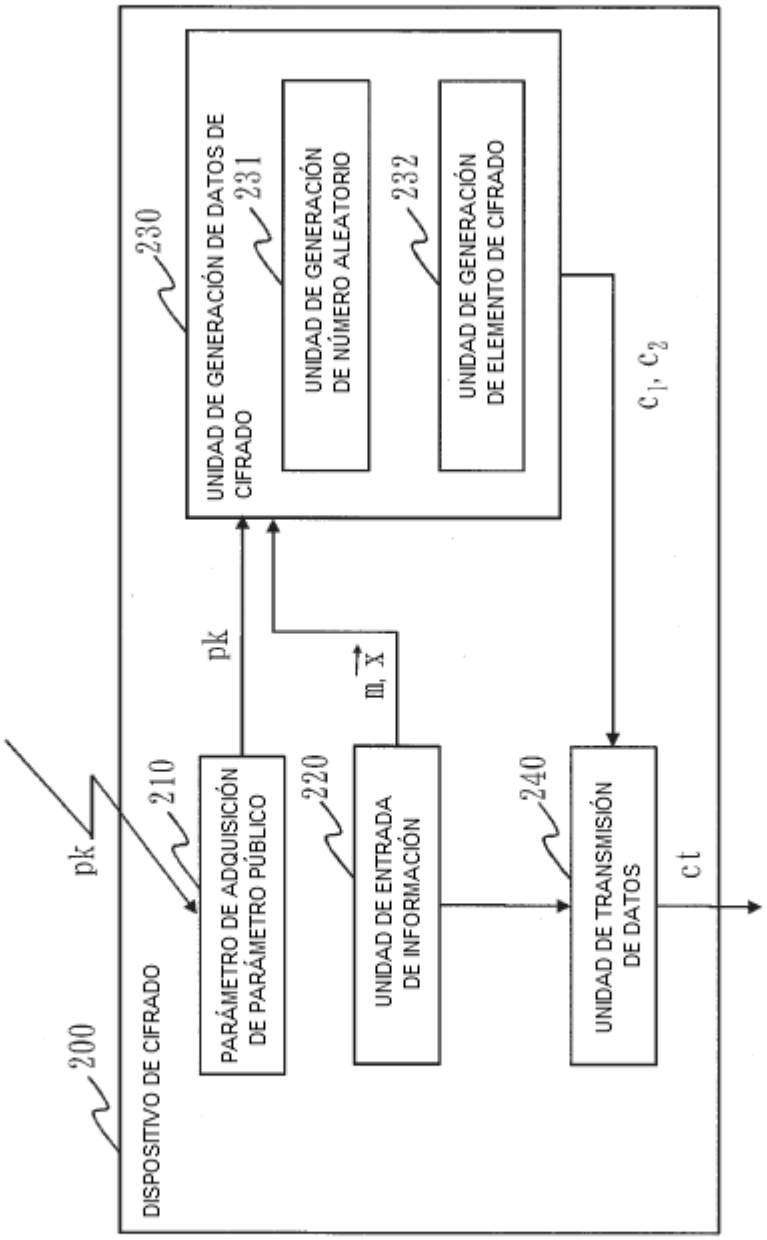

DISPOSITIVO DE CIFRADO
200
pk
PARÁMETRO DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
210
pk
UNIDAD DE GENERACIÓN DE DATOS DE CIFRADO
230
UNIDAD DE GENERACIÓN DE NÚMERO ALEATORIO
231
UNIDAD DE GENERACIÓN DE ELEMENTO DE CIFRADO
232
m, x
UNIDAD DE ENTRADA DE INFORMACIÓN
220
c1, c2
UNIDAD DE TRANSMISIÓN DE DATOS
240
ct

Fig. 23

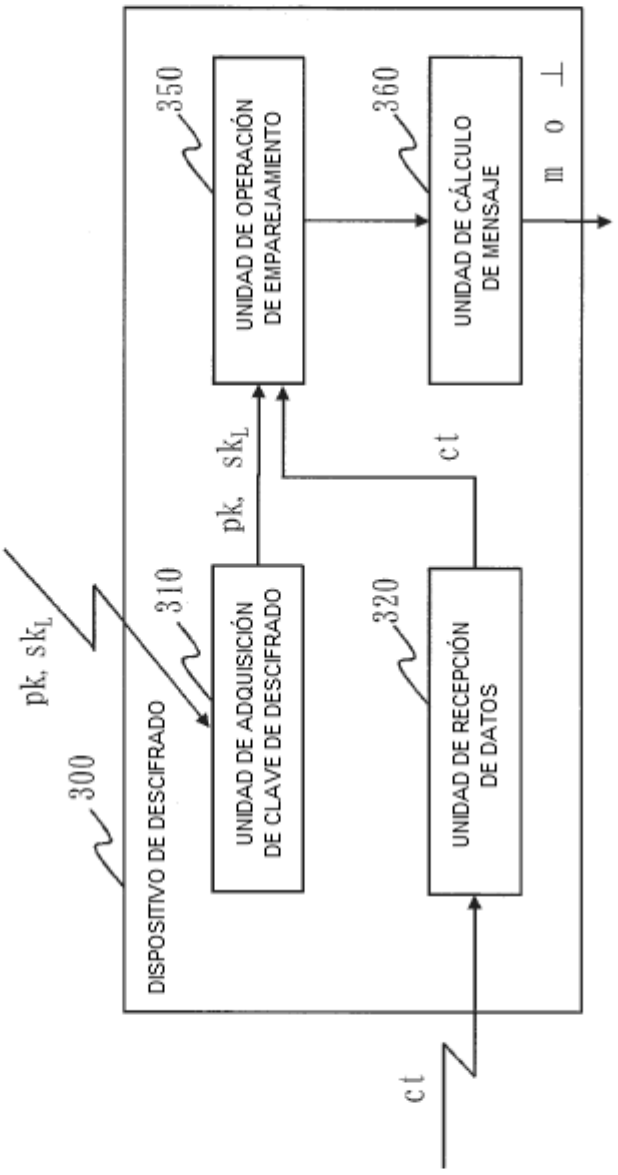

DISPOSITIVO DE DESCIFRADO
300
UNIDAD DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
310
UNIDAD DE RECEPCIÓN DE DATOS
320
UNIDAD DE OPERACIÓN DE EMPAREJAMIENTO
350
UNIDAD DE CÁLCULO DE MENSAJE
360
pk, sk_L
pk, sk_L
ct
ct
m o ⊥

Fig. 24

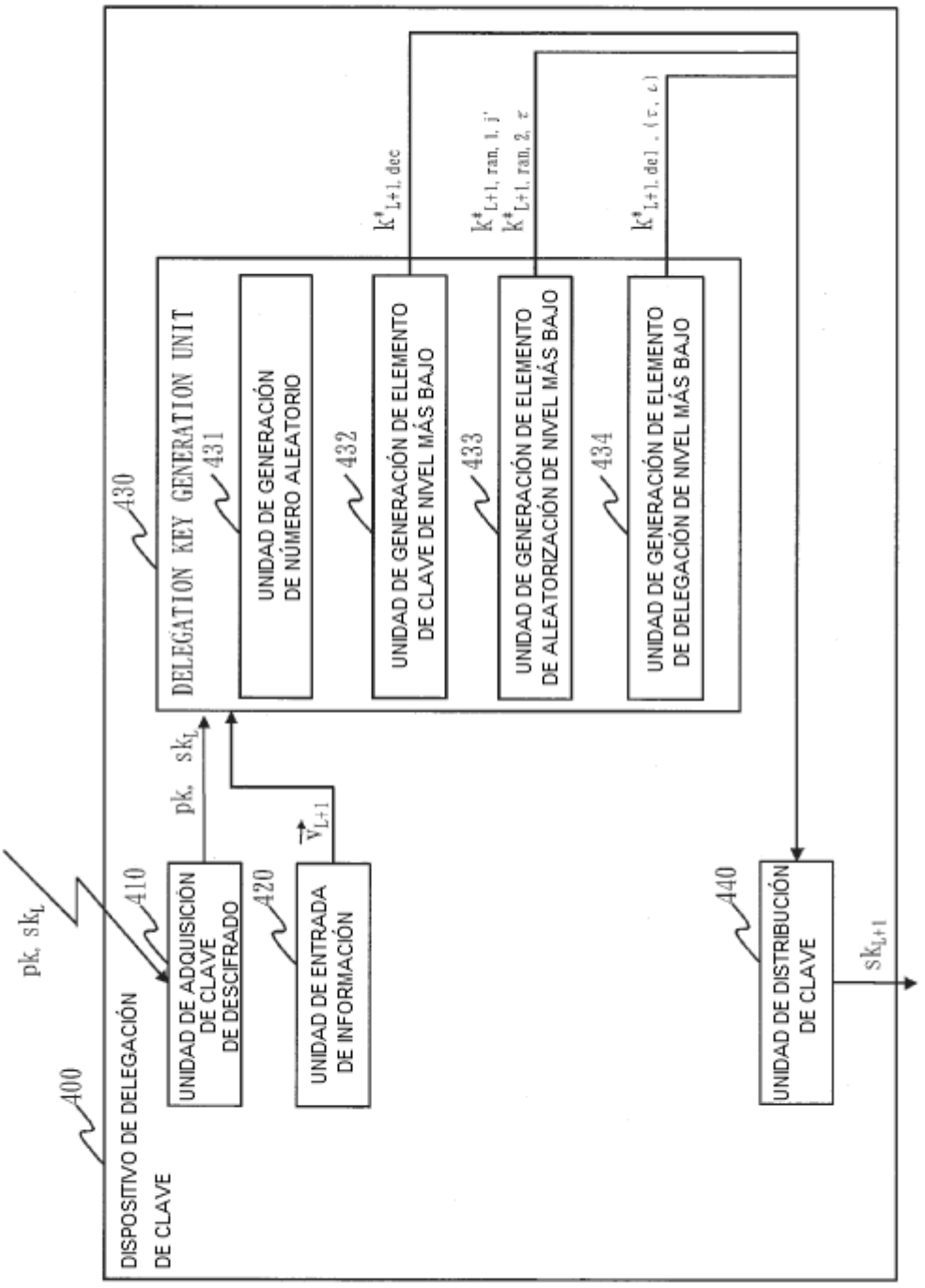

DISPOSITIVO DE DELEGACIÓN DE CLAVE
400
pk, sk_L
UNIDAD DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
410
pk, sk_L
UNIDAD DE ENTRADA DE INFORMACIÓN
420
$\vec{v}_{L+1}$
DELEGATION KEY GENERATION UNIT
430
UNIDAD DE GENERACIÓN DE NÚMERO ALEATORIO
431
UNIDAD DE GENERACIÓN DE ELEMENTO DE CLAVE DE NIVEL MÁS BAJO
432
UNIDAD DE GENERACIÓN DE ELEMENTO DE ALEATORIZACIÓN DE NIVEL MÁS BAJO
433
UNIDAD DE GENERACIÓN DE ELEMENTO DE DELEGACIÓN DE NIVEL MÁS BAJO
434
$k^*_{L+1,dec}$
$k^*_{L+1,ran,1,j}$
$k^*_{L+1,ran,2,\varepsilon}$
$k^*_{L+1,del,(\tau,c)}$
UNIDAD DE DISTRIBUCIÓN DE CLAVE
440
sk_{L+1}

Fig. 25

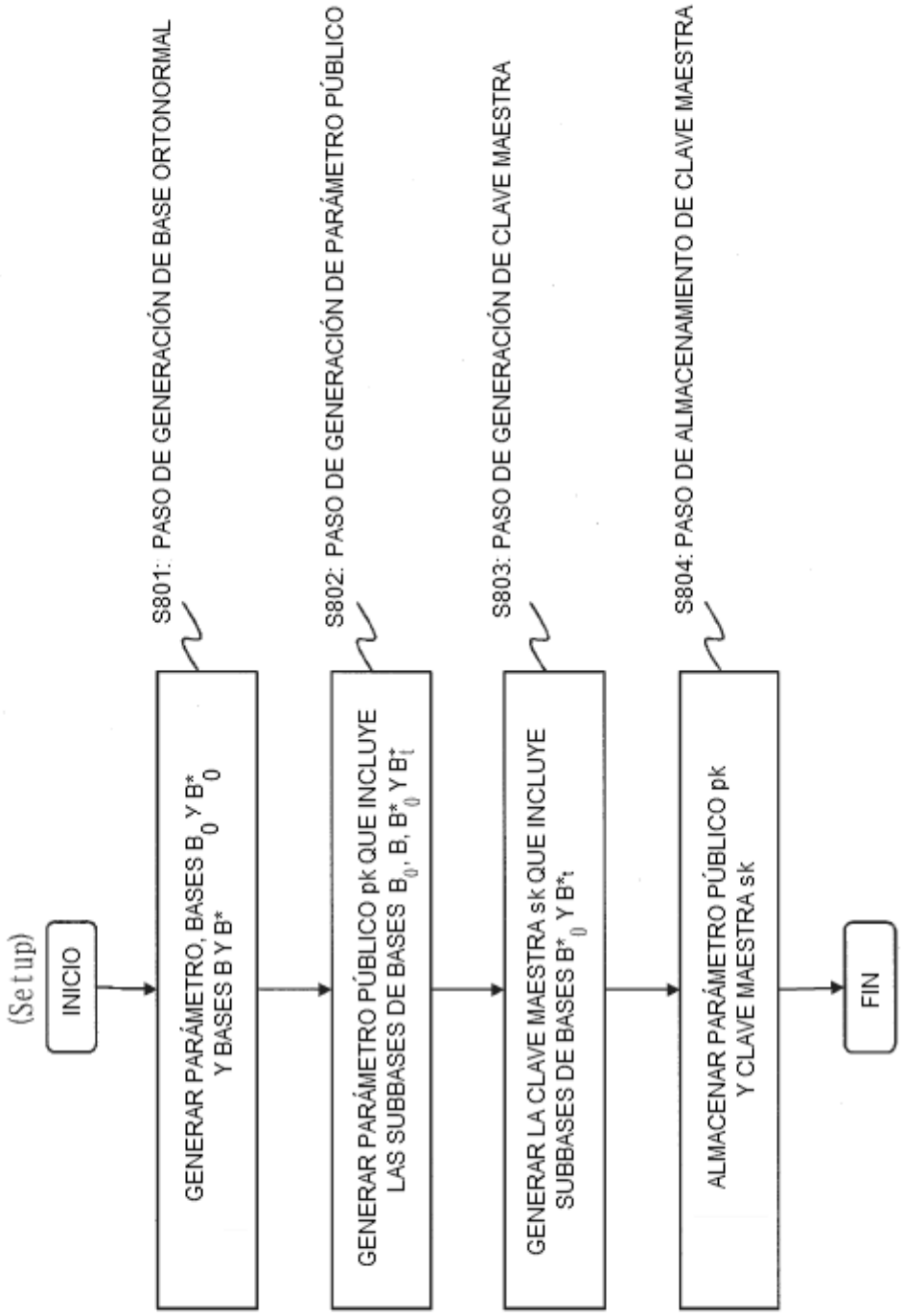

(Setup)
INICIO
S801: PASO DE GENERACIÓN DE BASE ORTONORMAL
GENERAR PARÁMETRO, BASES B_0 Y B^*_0 Y BASES B Y B*
S802: PASO DE GENERACIÓN DE PARÁMETRO PÚBLICO
GENERAR PARÁMETRO PÚBLICO pk QUE INCLUYE LAS SUBBASES DE BASES B_0, B, B^*_0 Y B^*_t
S803: PASO DE GENERACIÓN DE CLAVE MAESTRA
GENERAR LA CLAVE MAESTRA sk QUE INCLUYE SUBBASES DE BASES B^*_0 Y B^*_t
S804: PASO DE ALMACENAMIENTO DE CLAVE MAESTRA
ALMACENAR PARÁMETRO PÚBLICO pk Y CLAVE MAESTRA sk
FIN

Fig. 26

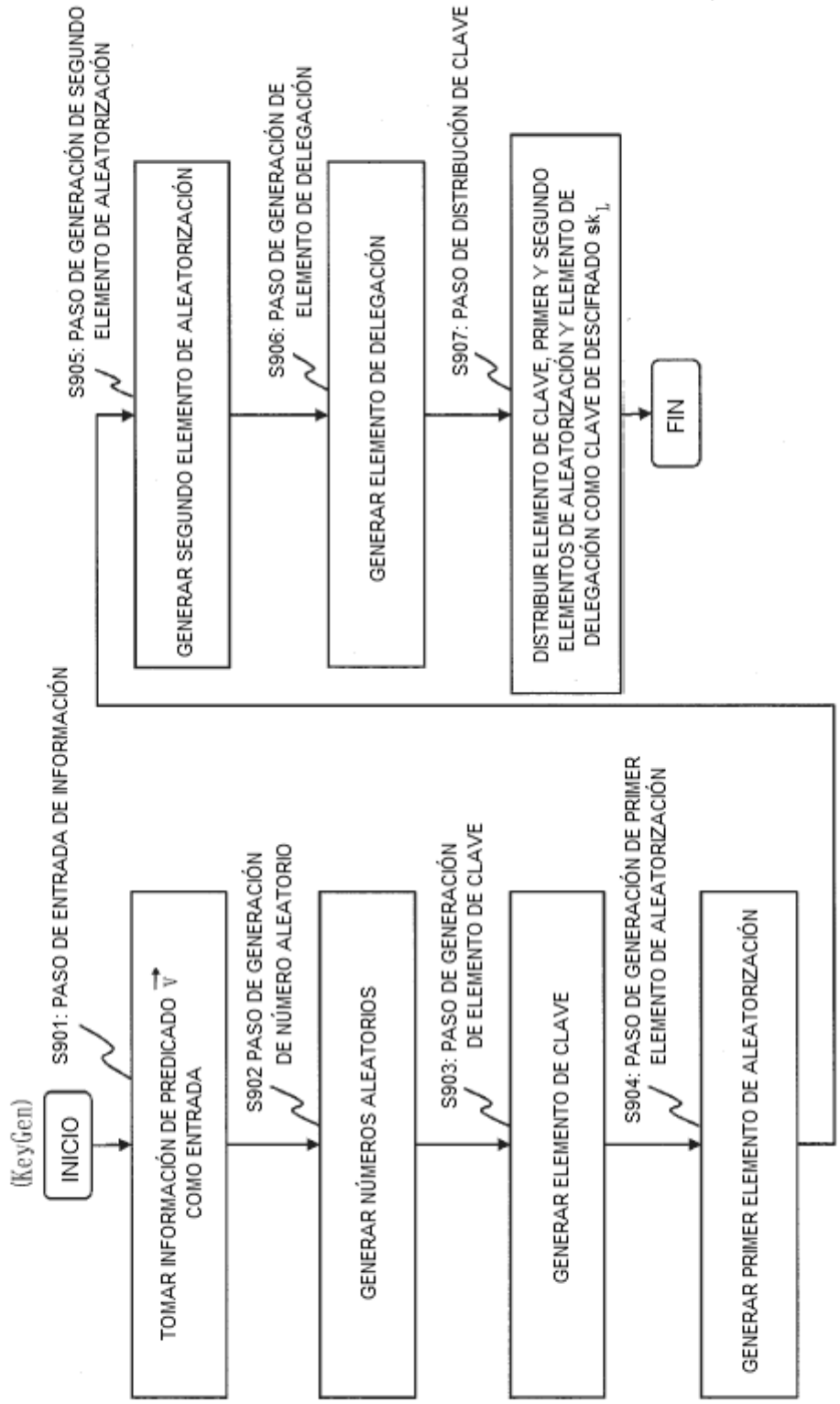

(KeyGen)
INICIO
S901: PASO DE ENTRADA DE INFORMACIÓN
TOMAR INFORMACIÓN DE PREDICADO $\vec{v}$ COMO ENTRADA
S902 PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S903: PASO DE GENERACIÓN DE ELEMENTO DE CLAVE
GENERAR ELEMENTO DE CLAVE
S904: PASO DE GENERACIÓN DE PRIMER ELEMENTO DE ALEATORIZACIÓN
GENERAR PRIMER ELEMENTO DE ALEATORIZACIÓN
S905: PASO DE GENERACIÓN DE SEGUNDO ELEMENTO DE ALEATORIZACIÓN
GENERAR SEGUNDO ELEMENTO DE ALEATORIZACIÓN
S906: PASO DE GENERACIÓN DE ELEMENTO DE DELEGACIÓN
GENERAR ELEMENTO DE DELEGACIÓN
S907: PASO DE DISTRIBUCIÓN DE CLAVE
DISTRIBUIR ELEMENTO DE CLAVE, PRIMER Y SEGUNDO ELEMENTOS DE ALEATORIZACIÓN Y ELEMENTO DE DELEGACIÓN COMO CLAVE DE DESCIFRADO sk_L
FIN

Fig. 27

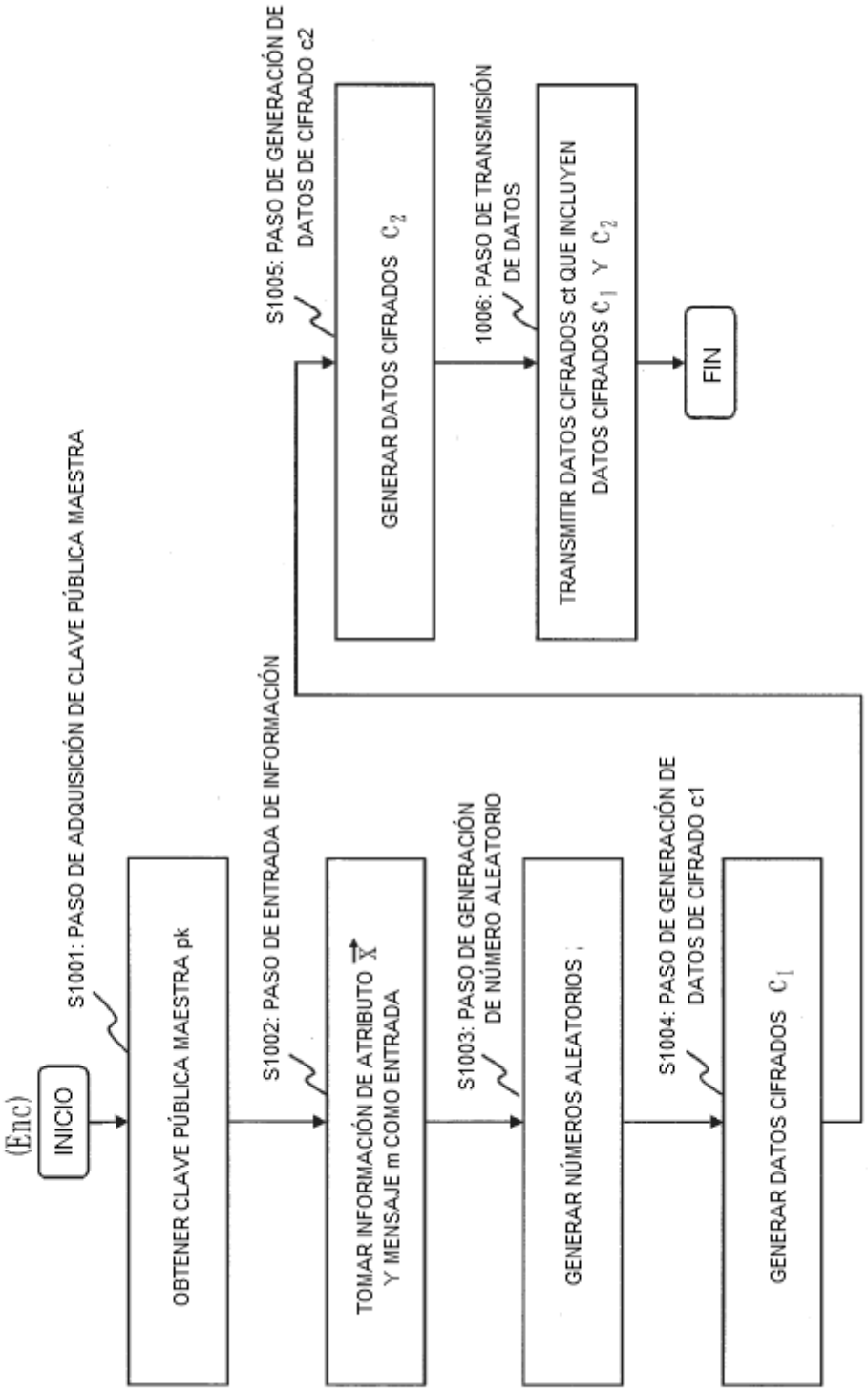

(Enc)
INICIO
S1001: PASO DE ADQUISICIÓN DE CLAVE PÚBLICA MAESTRA
OBTENER CLAVE PÚBLICA MAESTRA pk
S1002: PASO DE ENTRADA DE INFORMACIÓN
TOMAR INFORMACIÓN DE ATRIBUTO $\vec{x}$ Y MENSAJE m COMO ENTRADA
S1003: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS r
S1004: PASO DE GENERACIÓN DE DATOS DE CIFRADO c1
GENERAR DATOS CIFRADOS c_1
S1005: PASO DE GENERACIÓN DE DATOS DE CIFRADO c2
GENERAR DATOS CIFRADOS c_2
1006: PASO DE TRANSMISIÓN DE DATOS
TRANSMITIR DATOS CIFRADOS ct QUE INCLUYEN DATOS CIFRADOS c_1 Y c_2
FIN

Fig. 28

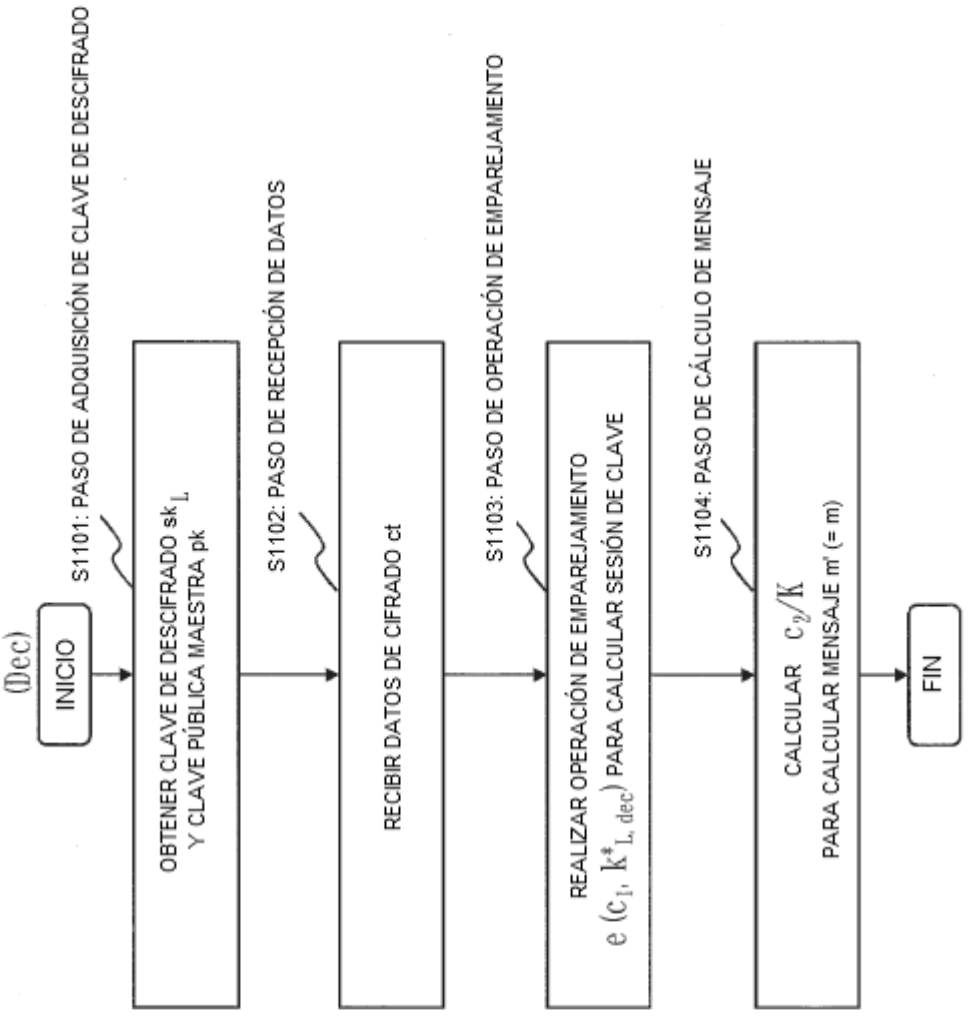

(Dec)
INICIO
S1101: PASO DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
OBTENER CLAVE DE DESCIFRADO sk_L
Y CLAVE PÚBLICA MAESTRA pk
S1102: PASO DE RECEPCIÓN DE DATOS
RECIBIR DATOS DE CIFRADO ct
S1103: PASO DE OPERACIÓN DE EMPAREJAMIENTO
REALIZAR OPERACIÓN DE EMPAREJAMIENTO
$e(c_1, k^*_{L,dec})$ PARA CALCULAR SESIÓN DE CLAVE
S1104: PASO DE CÁLCULO DE MENSAJE
CALCULAR c_2/K
PARA CALCULAR MENSAJE m' (= m)
FIN

Fig. 29

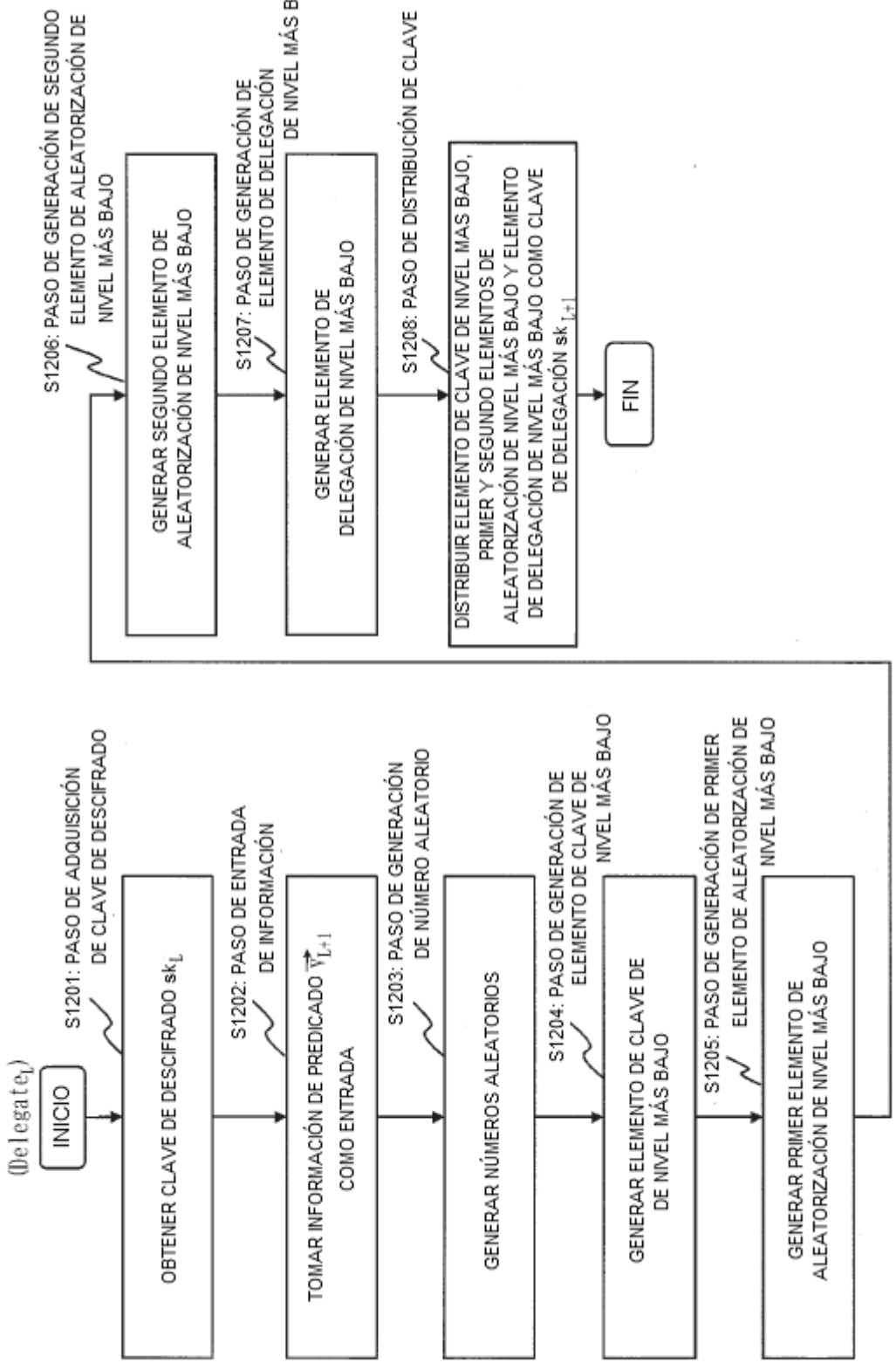

(Delegatee_L)
INICIO
S1201: PASO DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
OBTENER CLAVE DE DESCIFRADO sk_L
S1202: PASO DE ENTRADA DE INFORMACIÓN
TOMAR INFORMACIÓN DE PREDICADO y_{L+1} COMO ENTRADA
S1203: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S1204: PASO DE GENERACIÓN DE ELEMENTO DE CLAVE DE NIVEL MÁS BAJO
GENERAR ELEMENTO DE CLAVE DE DE NIVEL MÁS BAJO
S1205: PASO DE GENERACIÓN DE PRIMER ELEMENTO DE ALEATORIZACIÓN DE NIVEL MÁS BAJO
GENERAR PRIMER ELEMENTO DE ALEATORIZACIÓN DE NIVEL MÁS BAJO
S1206: PASO DE GENERACIÓN DE SEGUNDO ELEMENTO DE ALEATORIZACIÓN DE NIVEL MÁS BAJO
GENERAR SEGUNDO ELEMENTO DE ALEATORIZACIÓN DE NIVEL MÁS BAJO
S1207: PASO DE GENERACIÓN DE ELEMENTO DE DELEGACIÓN DE NIVEL MÁS BAJO
GENERAR ELEMENTO DE DELEGACIÓN DE NIVEL MÁS BAJO
S1208: PASO DE DISTRIBUCIÓN DE CLAVE
DISTRIBUIR ELEMENTO DE CLAVE DE NIVEL MAS BAJO, PRIMER Y SEGUNDO ELEMENTOS DE ALEATORIZACIÓN DE NIVEL MÁS BAJO Y ELEMENTO DE DELEGACIÓN DE NIVEL MÁS BAJO COMO CLAVE DE DELEGACIÓN sk_{L+1}
FIN

Fig. 30

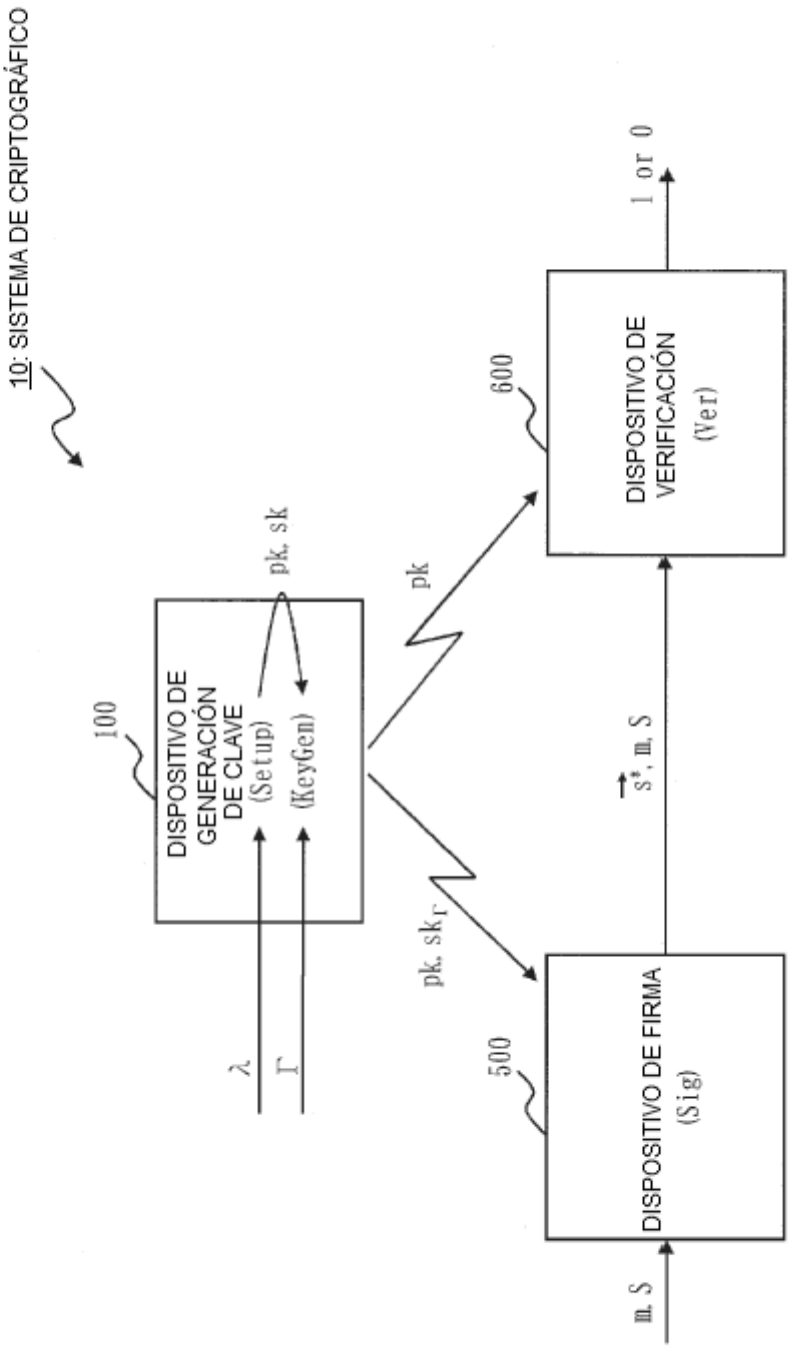

10: SISTEMA DE CRIPTOGRÁFICO
100
DISPOSITIVO DE GENERACIÓN DE CLAVE
(Setup)
(KeyGen)
pk, sk
λ
Γ
pk
pk, sk_Γ
600
DISPOSITIVO DE VERIFICACIÓN
(Ver)
1 or 0
500
DISPOSITIVO DE FIRMA
(Sig)
m, S
s, m, S

Fig. 31

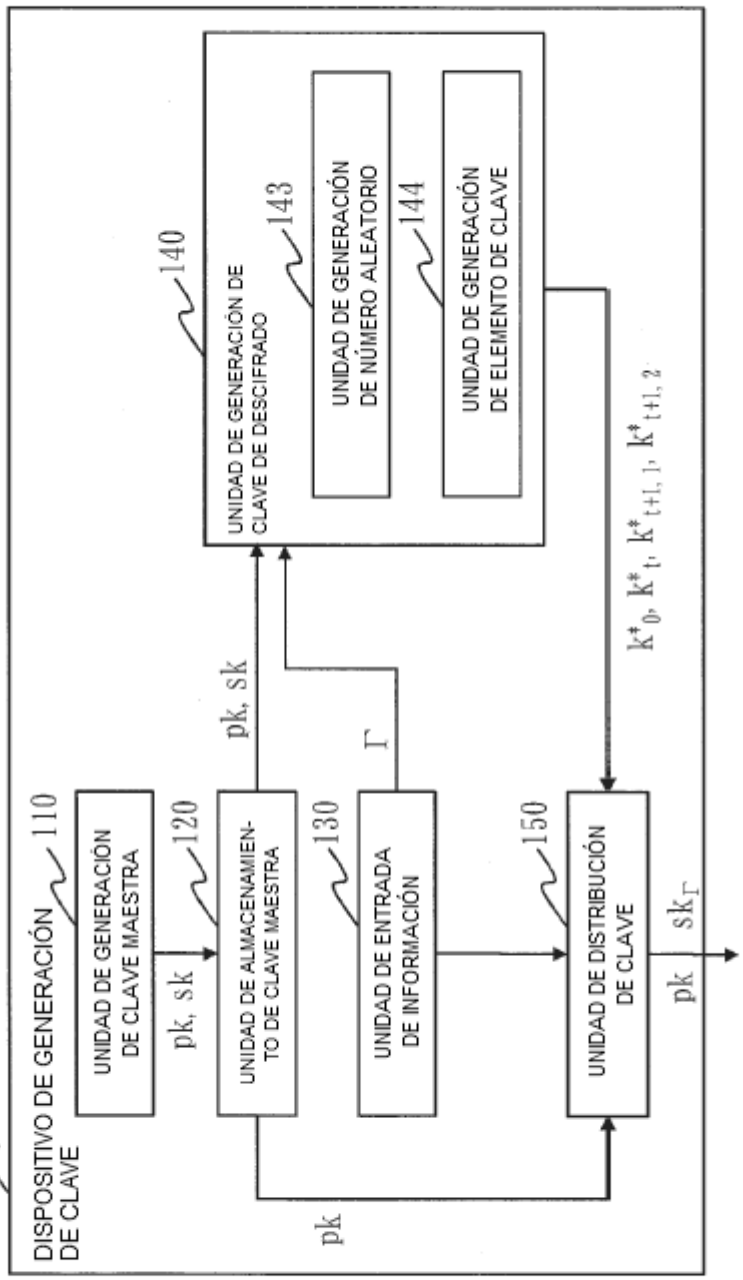

100
DISPOSITIVO DE GENERACIÓN DE CLAVE
110
UNIDAD DE GENERACIÓN DE CLAVE MAESTRA
120
UNIDAD DE ALMACENAMIENTO DE CLAVE MAESTRA
130
UNIDAD DE ENTRADA DE INFORMACIÓN
140
UNIDAD DE GENERACIÓN DE CLAVE DE DESCIFRADO
143
UNIDAD DE GENERACIÓN DE NÚMERO ALEATORIO
144
UNIDAD DE GENERACIÓN DE ELEMENTO DE CLAVE
150
UNIDAD DE DISTRIBUCIÓN DE CLAVE
pk, sk
pk, sk
Γ
pk
pk
sk_Γ
$k^*_0, k^*_t, k^*_{t+1,1}, k^*_{t+1,2}$

Fig. 32

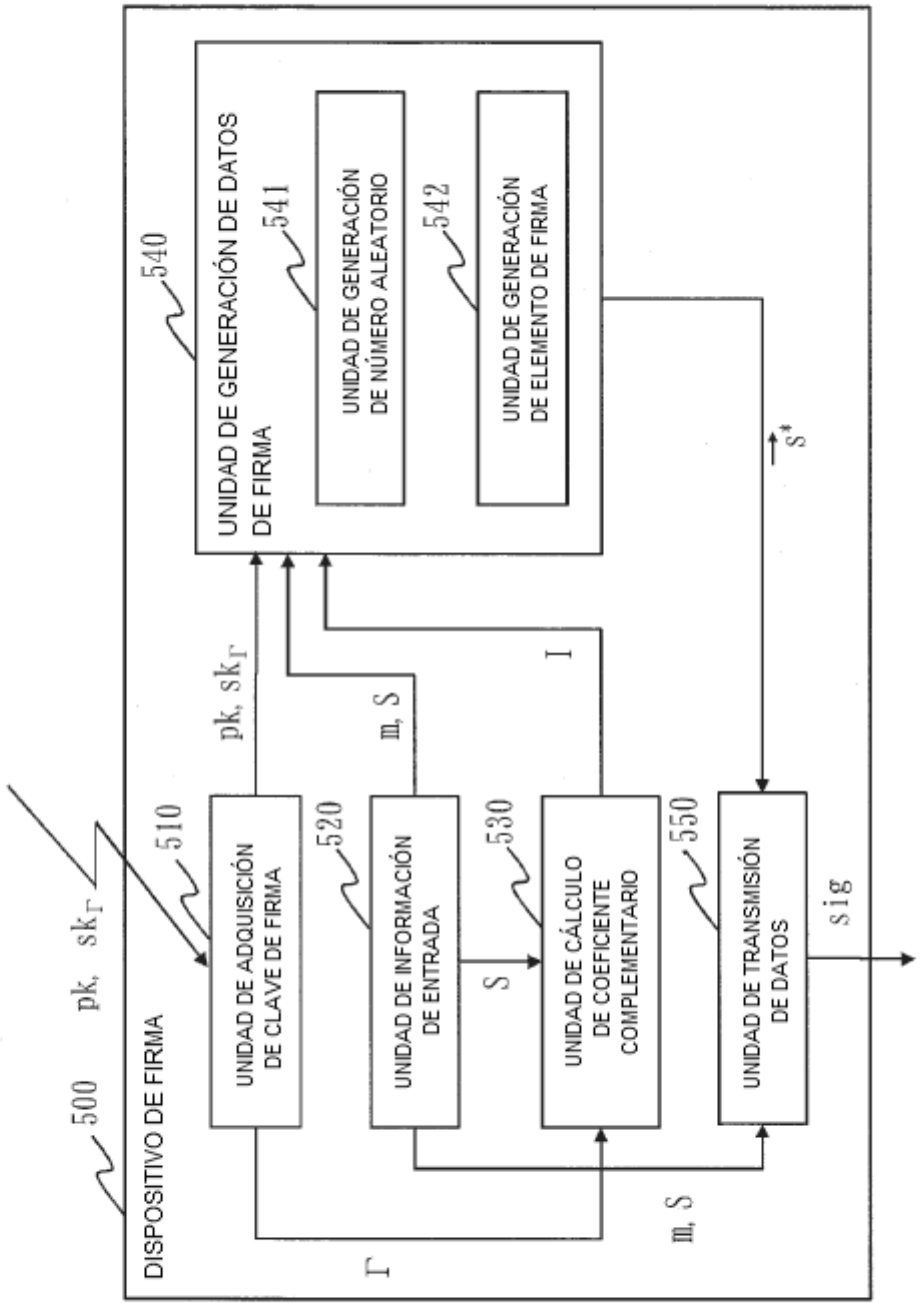

DISPOSITIVO DE FIRMA
500
pk, skΓ
510
UNIDAD DE ADQUISICIÓN DE CLAVE DE FIRMA
520
UNIDAD DE INFORMACIÓN DE ENTRADA
530
UNIDAD DE CÁLCULO DE COEFICIENTE COMPLEMENTARIO
550
UNIDAD DE TRANSMISIÓN DE DATOS
sig
540
UNIDAD DE GENERACIÓN DE DATOS DE FIRMA
541
UNIDAD DE GENERACIÓN DE NÚMERO ALEATORIO
542
UNIDAD DE GENERACIÓN DE ELEMENTO DE FIRMA
pk, skΓ
m, S
I
s4
S
m, S
Γ

Fig. 33

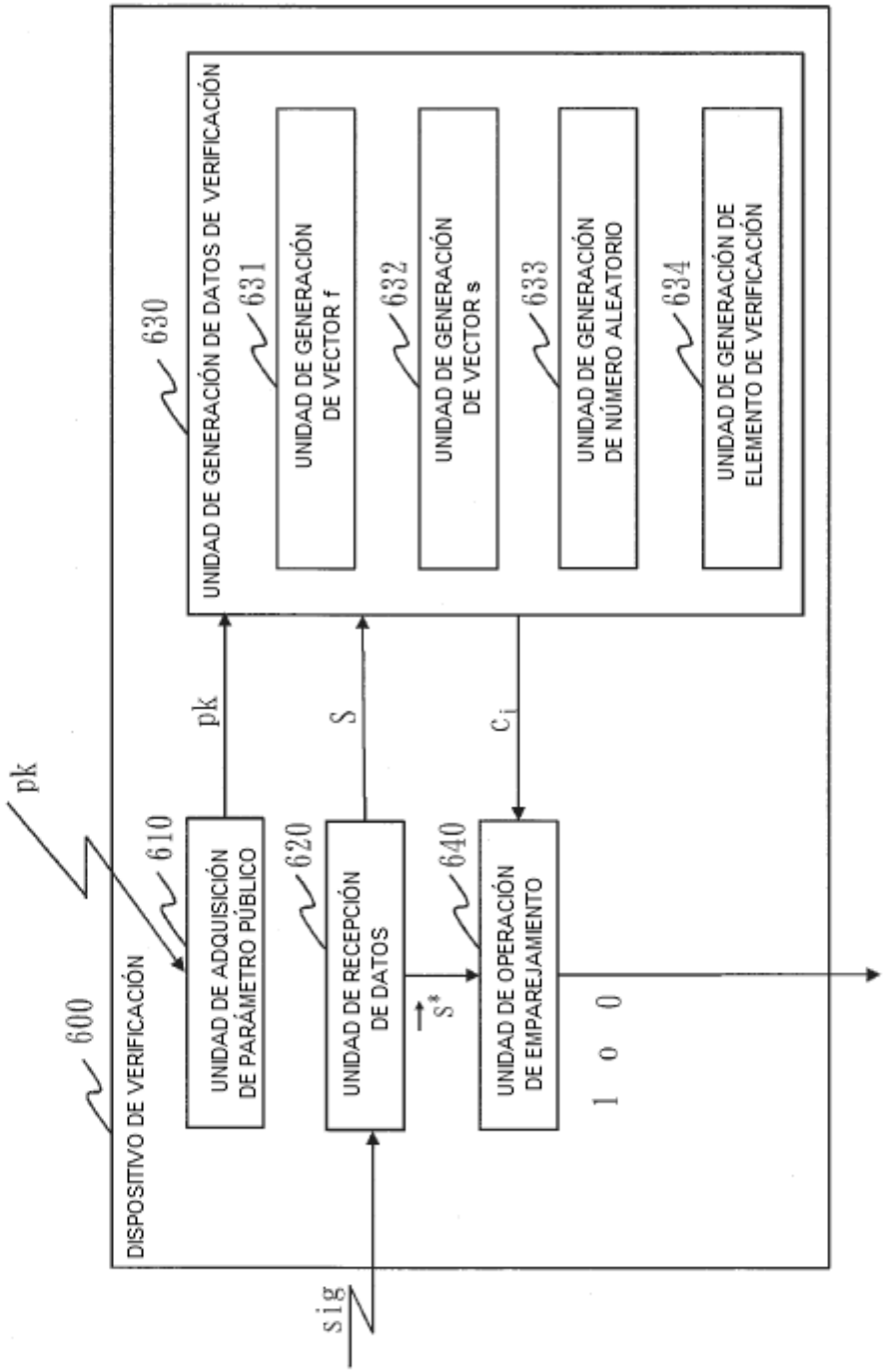

DISPOSITIVO DE VERIFICACIÓN
600
UNIDAD DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
610
UNIDAD DE RECEPCIÓN DE DATOS
620
UNIDAD DE OPERACIÓN DE EMPAREJAMIENTO
640
UNIDAD DE GENERACIÓN DE DATOS DE VERIFICACIÓN
630
UNIDAD DE GENERACIÓN DE VECTOR f
631
UNIDAD DE GENERACIÓN DE VECTOR s
632
UNIDAD DE GENERACIÓN DE NÚMERO ALEATORIO
633
UNIDAD DE GENERACIÓN DE ELEMENTO DE VERIFICACIÓN
634
pk
pk
S
c_i
$\vec{s}^*$
sig
1 o 0

Fig. 34

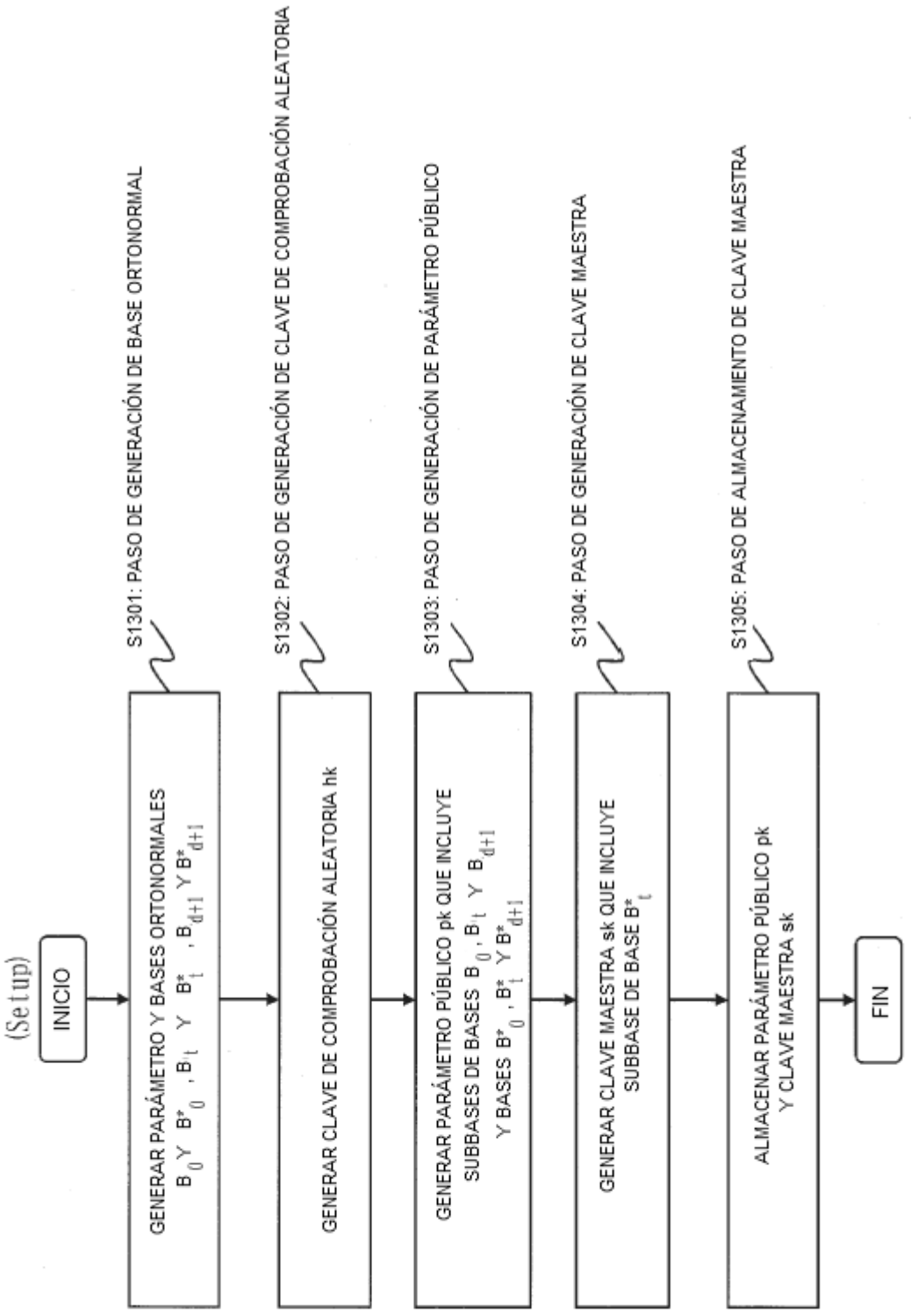

(Setup)
INICIO
S1301: PASO DE GENERACIÓN DE BASE ORTONORMAL
GENERAR PARÁMETRO Y BASES ORTONORMALES
B 0 Y B* 0 , B t Y B* t , B d+1 Y B* d+1
S1302: PASO DE GENERACIÓN DE CLAVE DE COMPROBACIÓN ALEATORIA
GENERAR CLAVE DE COMPROBACIÓN ALEATORIA hk
S1303: PASO DE GENERACIÓN DE PARÁMETRO PÚBLICO
GENERAR PARÁMETRO PÚBLICO pk QUE INCLUYE
SUBBASES DE BASES B 0 , B t Y B d+1
Y BASES B* 0 , B* t Y B* d+1
S1304: PASO DE GENERACIÓN DE CLAVE MAESTRA
GENERAR CLAVE MAESTRA sk QUE INCLUYE
SUBBASE DE BASE B* t
S1305: PASO DE ALMACENAMIENTO DE CLAVE MAESTRA
ALMACENAR PARÁMETRO PÚBLICO pk
Y CLAVE MAESTRA sk
FIN

Fig. 35

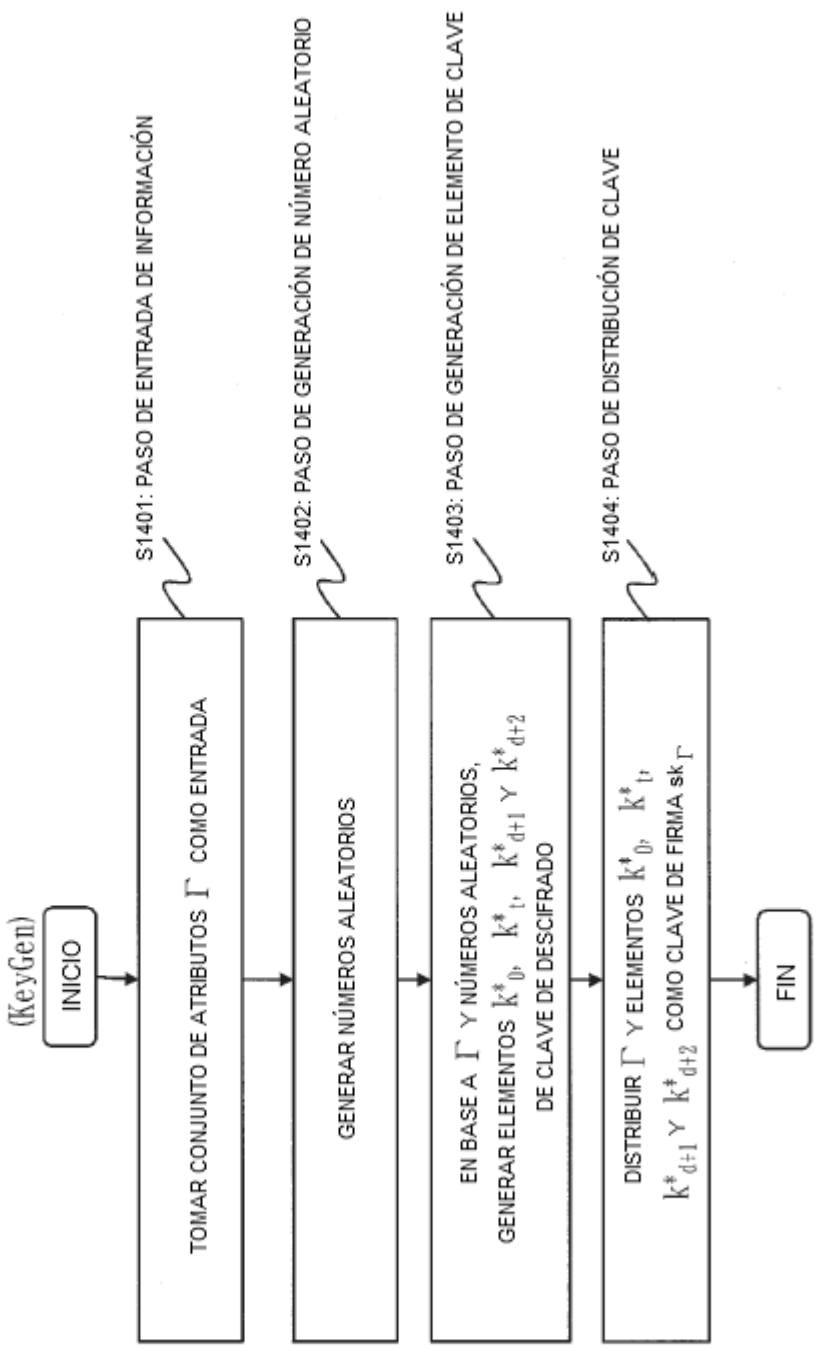

(KeyGen)
INICIO
S1401: PASO DE ENTRADA DE INFORMACIÓN
TOMAR CONJUNTO DE ATRIBUTOS Γ COMO ENTRADA
S1402: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S1403: PASO DE GENERACIÓN DE ELEMENTO DE CLAVE
EN BASE A Γ Y NÚMEROS ALEATORIOS,
GENERAR ELEMENTOS k*0, k*t, k*d+1 Y k*d+2
DE CLAVE DE DESCIFRADO
S1404: PASO DE DISTRIBUCIÓN DE CLAVE
DISTRIBUIR Γ Y ELEMENTOS k*0, k*t,
k*d+1 Y k*d+2 COMO CLAVE DE FIRMA skΓ
FIN

Fig. 36

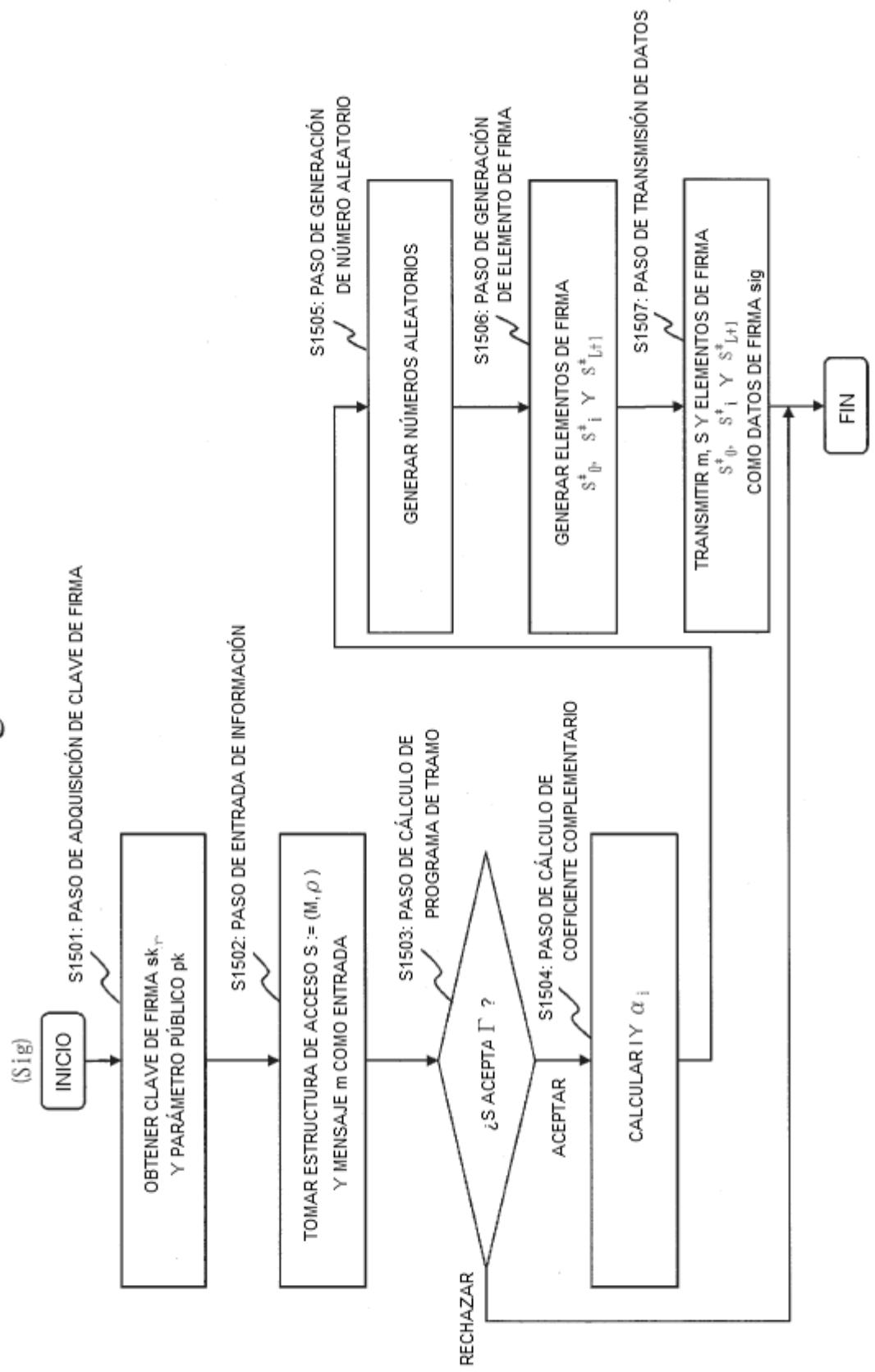

(Sig)
INICIO
S1501: PASO DE ADQUISICIÓN DE CLAVE DE FIRMA
OBTENER CLAVE DE FIRMA sk
Y PARÁMETRO PÚBLICO pk
S1502: PASO DE ENTRADA DE INFORMACIÓN
TOMAR ESTRUCTURA DE ACCESO S := (M, ρ)
Y MENSAJE m COMO ENTRADA
S1503: PASO DE CÁLCULO DE
PROGRAMA DE TRAMO
¿S ACEPTA Γ ?
RECHAZAR
ACEPTAR
S1504: PASO DE CÁLCULO DE
COEFICIENTE COMPLEMENTARIO
CALCULAR I Y α i
S1505: PASO DE GENERACIÓN
DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S1506: PASO DE GENERACIÓN
DE ELEMENTO DE FIRMA
GENERAR ELEMENTOS DE FIRMA
S0, Si Y SL+1
S1507: PASO DE TRANSMISIÓN DE DATOS
TRANSMITIR m, S Y ELEMENTOS DE FIRMA
S0, Si Y SL+1
COMO DATOS DE FIRMA sig
FIN

Fig. 37

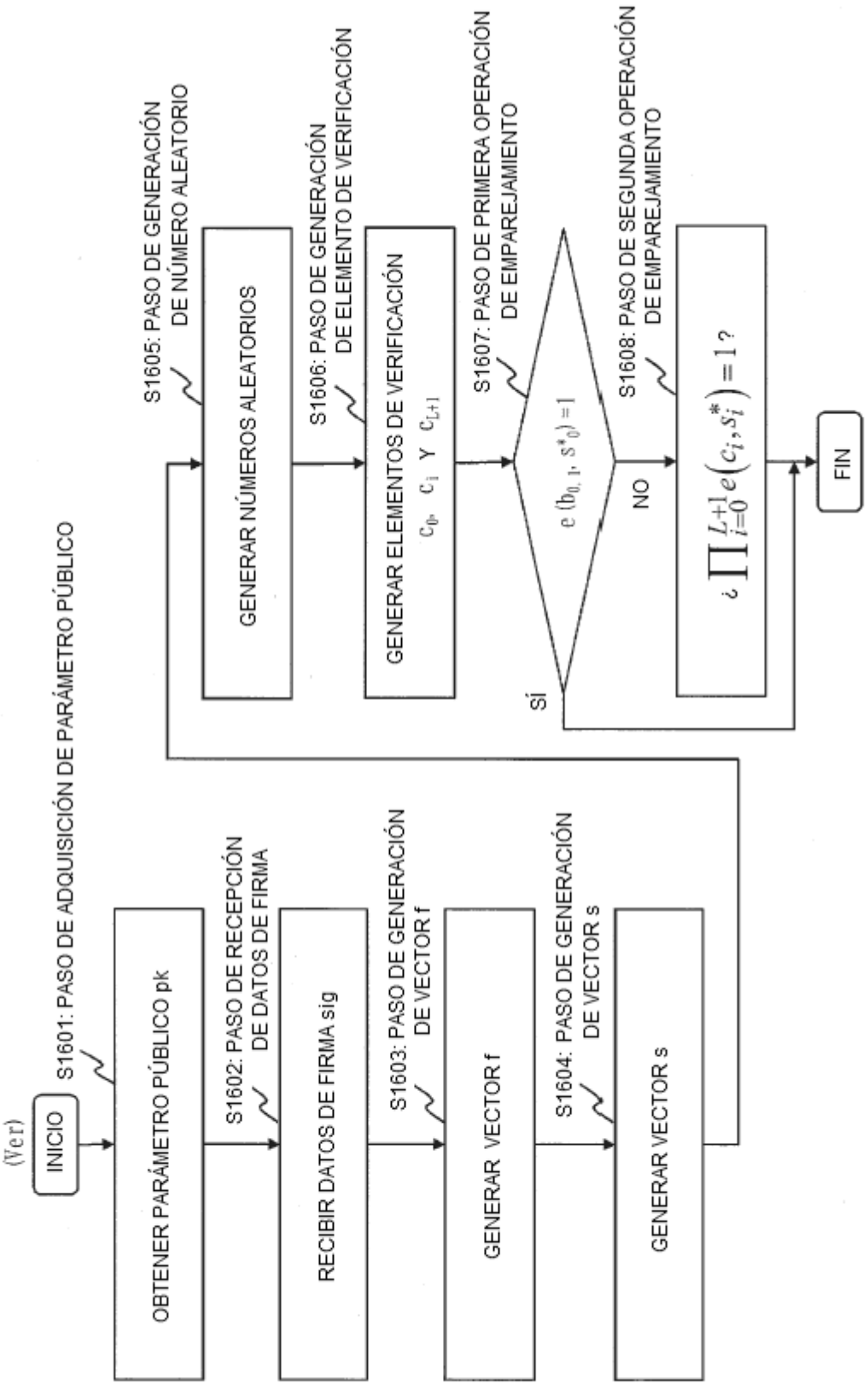

(Ver)
INICIO
S1601: PASO DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
OBTENER PARÁMETRO PÚBLICO pk
S1602: PASO DE RECEPCIÓN DE DATOS DE FIRMA
RECIBIR DATOS DE FIRMA sig
S1603: PASO DE GENERACIÓN DE VECTOR f
GENERAR VECTOR f
S1604: PASO DE GENERACIÓN DE VECTOR s
GENERAR VECTOR s
S1605: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S1606: PASO DE GENERACIÓN DE ELEMENTO DE VERIFICACIÓN
GENERAR ELEMENTOS DE VERIFICACIÓN
c_0, c_i Y c_{i+1}
S1607: PASO DE PRIMERA OPERACIÓN DE EMPAREJAMIENTO
$e(b_{0,1}, s^*_0) = 1$
SÍ
NO
S1608: PASO DE SEGUNDA OPERACIÓN DE EMPAREJAMIENTO
$\prod_{i=0}^{L+1} e(c_i, s_i^*) = 1$?
FIN

Fig. 38

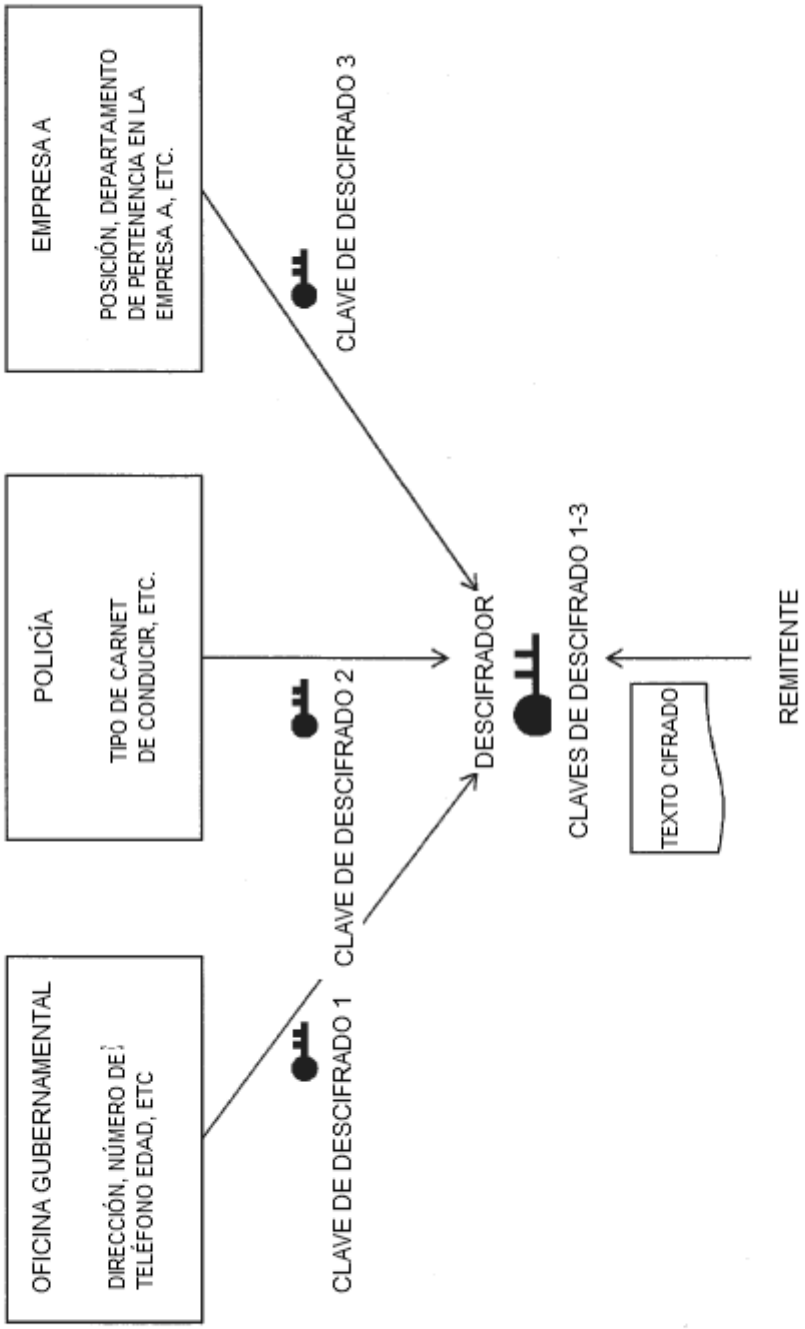

EMPRESA A
POSICIÓN, DEPARTAMENTO DE PERTENENCIA EN LA EMPRESA A, ETC.
POLICÍA
TIPO DE CARNET DE CONDUCIR, ETC.
OFICINA GUBERNAMENTAL
DIRECCIÓN, NÚMERO DE TELÉFONO EDAD, ETC
CLAVE DE DESCIFRADO 1
CLAVE DE DESCIFRADO 2
CLAVE DE DESCIFRADO 3
DESCIFRADOR
CLAVES DE DESCIFRADO 1-3
TEXTO CIFRADO
REMITENTE

Fig. 39

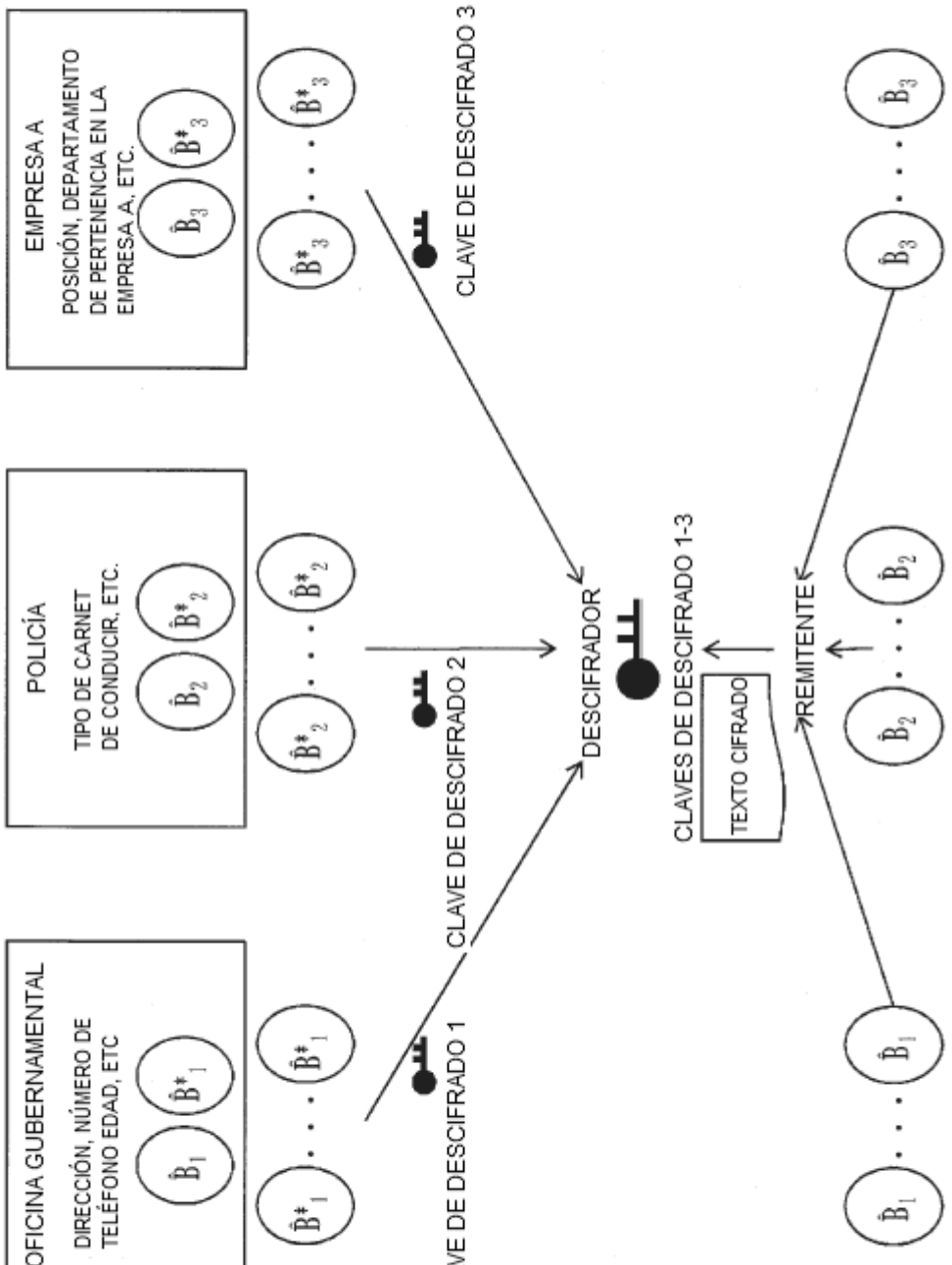
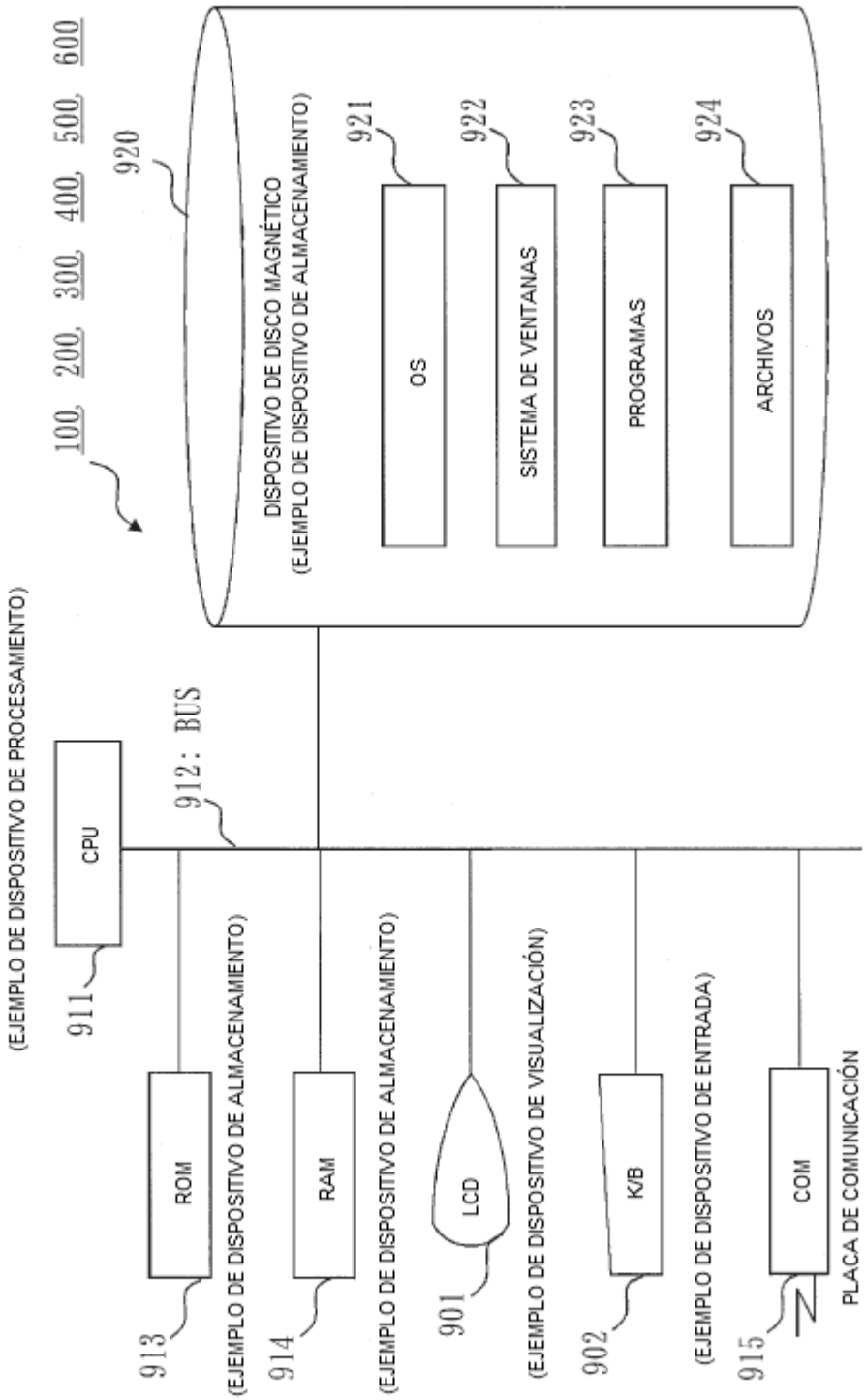

OFICINA GUBERNAMENTAL
DIRECCIÓN, NÚMERO DE TELÉFONO EDAD, ETC
POLICÍA
TIPO DE CARNET DE CONDUCIR, ETC.
EMPRESA A
POSICIÓN, DEPARTAMENTO DE PERTENENCIA EN LA EMPRESA A, ETC.
CLAVE DE DESCIFRADO 1
CLAVE DE DESCIFRADO 2
CLAVE DE DESCIFRADO 3
DESCIFRADOR
CLAVES DE DESCIFRADO 1-3
TEXTO CIFRADO
REMITENTE

Fig. 40


100, 200, 300, 400, 500, 600
920
DISPOSITIVO DE DISCO MAGNÉTICO
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
921
OS
922
SISTEMA DE VENTANAS
923
PROGRAMAS
924
ARCHIVOS
912: BUS
(EJEMPLO DE DISPOSITIVO DE PROCESAMIENTO)
911
CPU
913
ROM
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
914
RAM
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
901
LCD
(EJEMPLO DE DISPOSITIVO DE VISUALIZACIÓN)
902
K/B
(EJEMPLO DE DISPOSITIVO DE ENTRADA)
915
COM
PLACA DE COMUNICACIÓN