(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 613 811**

(51) Int. CI.:

G09C 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.11.2012 PCT/JP2012/079210**

(87) Fecha y número de publicación internacional: **23.05.2013 WO2013073488**

(96) Fecha de presentación y número de la solicitud europea: **12.11.2012 E 12850218 (4)**

(97) Fecha y número de publicación de la concesión europea: **28.12.2016 EP 2782087**

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

(30) Prioridad:

18.11.2011 JP 2011252244

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.05.2017

(73) Titular/es:

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

(72) Inventor/es:

TAKASHIMA, KATSUYUKI y
OKAMOTO, TATSUAKI

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema de procesamiento criptográfico, método de procesamiento criptográfico, programa de procesamiento criptográfico y dispositivo de generación de claves

Campo técnico

La presente invención se refiere a cifrado de producto interior (IPE).

Antecedentes de la técnica

Las Literaturas No de Patente 13, 16 y 17 describen el cifrado de producto interior.

Según el cifrado de producto interior descrito en las Literaturas No de Patente 13, 16 y 17, un parámetro público y una clave secreta maestra se dan mediante la base de un espacio de vector.

Lista de citas

Literatura No de Patente

Literatura No de Patente 1: Abdalla, M., Kiltz, E., Neven, G.: Generalized key delegation for hierarchical identity-based encryption. ESORICS'07, LNCS 4734, páginas 139-154. Springer, (2007)

Literatura No de Patente 2: Attrapadung, N., Libert, B.: Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation. PKC 2010. LNCS, vol. 6056, páginas 384-402. Springer Heidelberg (2010)

Literatura No de Patente 3: Attrapadung, N., Libert, B., De Panafieu, E.: Expressive key-policy attribute-based encryption with constant-size ciphertexts. PKC 2011. LNCS, vol. 6571, páginas 90-108. Springer Heidelberg (2011)

Literatura No de Patente 4: 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 5: 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 6: Delerablee, C.: Identity-based broadcast encryption with constant size ciphertexts and private keys. En: ASIACRYPT 2007. LNCS, páginas 200-215. Springer-Verlag (2007)

Literatura No de Patente 7: Emura, K., Miyaji, A., Nomura, A., Omote, K., Soshi, M.: A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. Actas de ISPEC 2009, LNCS, páginas 13-23. Springer-Verlag (2009)

Literatura No de Patente 8: Gentry, C., Waters, B.: Adaptive security in broadcast encryption systems (with short ciphertexts). En: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, páginas 171-188. Springer Heidelberg (2009)

Literatura No de Patente 9: 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 10: Herranz, J., Laguillaumie, F., Rafols, C.: Constant size ciphertexts in thereshold attribute-based encryption. En Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, páginas 19-34. Springer Heidelberg (2010)

Literatura No de Patente 11: Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. En: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, páginas 146-162. Springer Heidelberg (2008)

Literatura No de Patente 12: Lewko, A., Sahai, A., Waters, B.: Revocation systems with very small private keys, En IEEE Symposium on Security and Privacy 2010 (2010)

Literatura No de Patente 13: 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) La versión completa está disponible en http://eprint.iacr.org/2010/110

Literatura No de Patente 14: 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 15: 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 16: Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products, En: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, páginas 214-231. Springer Heidelberg (2009)

Literatura No de Patente 17: 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 18: 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 19: Sakai, R., Furukawa, J.: Identity-based broadcast encryption, IACR ePrint Archive: Report 2007/217 http://eprint.iacr.org/2007/217 (2007).

Literatura No de Patente 20: 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

Según el cifrado de producto de producto interior descrito en las Literaturas No de Patente 13, 16 y 17, suponiendo que la longitud de un vector empleado en el cifrado de producto interior se define como N, los tamaños de los parámetros públicos y una clave secreta maestra son proporcionales a N^2 y el proceso de generación de una clave secreta a ser suministrada al usuario o un proceso de cifrado lleva un tiempo que es proporcional a N^2.

Es un objeto de la presente invención disminuir los tamaños de los parámetros públicos y la clave secreta maestra y acortar el tiempo que lleva el proceso de generación de la clave secreta a ser suministrada al usuario y el proceso de cifrado.

Solución al problema

Un sistema de procesamiento criptográfico según la presente invención se configura para utilizar una base B y una base B* generadas transformando una base A predeterminada usando una matriz dispersa en la que cada fila y cada columna tienen al menos un valor que es distinto del valor constante 0, para dirigir un proceso criptográfico, el sistema de procesamiento criptográfico que comprende:

un dispositivo de cifrado que genera un vector en la base B, el vector que está integrado con información predeterminada, como un vector de cifrado; y

un dispositivo de descifrado que, tratando un vector predeterminado en la base B* como un vector de clave, dirige una operación de emparejamiento para el vector de clave y el vector de cifrado que se genera por el dispositivo de cifrado, para descifrar el vector de cifrado y extrae información sobre la información predeterminada.

Efectos ventajosos de la invención

El sistema de procesamiento criptográfico según la presente invención usa una matriz dispersa como una matriz que se usa para generar las bases B y B* que son para formar parámetros públicos y una clave secreta maestra. Esto disminuye los tamaños de los parámetros públicos y la clave secreta maestra y acorta el tiempo que lleva el proceso de generación de la clave secreta a ser suministrada al usuario y al proceso de cifrado.

Breve descripción de los dibujos

La Fig. 1 es un diagrama de configuración de un sistema de procesamiento criptográfico 10 que ejecuta un esquema de cifrado de producto interior cero y un esquema de cifrado de producto interior no cero.

La Fig. 2 incluye un dibujo explicativo de una forma especial de transformación lineal aleatoria X.

La Fig. 3 es un diagrama de configuración de un dispositivo de generación de clave 100 según la Realización 2.

La Fig. 4 es un diagrama de configuración de un dispositivo de cifrado 200 según la Realización 2.

La Fig. 5 es un diagrama de configuración de un dispositivo de descifrado 300 según la Realización 2.

La Fig. 6 es un diagrama de flujo que muestra el proceso del algoritmo Setup según la Realización 2.

La Fig. 7 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen según la Realización 2.

La Fig. 8 es un diagrama de flujo que muestra el proceso del algoritmo Enc según la Realización 2.

La Fig. 9 es un diagrama de flujo que muestra el proceso del algoritmo Dec según la Realización 2.

La Fig. 10 es un diagrama de flujo que muestra el proceso del algoritmo Setup según la Realización 3.

La Fig. 11 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen según la Realización 3.

La Fig. 12 es un diagrama de flujo que muestra el proceso del algoritmo Enc según la Realización 3.

La Fig. 13 es un diagrama de flujo que muestra el proceso del algoritmo Dec según la Realización 3.

La Fig. 14 es un diagrama de flujo que muestra el proceso del algoritmo Setup según la Realización 4.

La Fig. 15 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen según la Realización 4.

La Fig. 16 es un diagrama de flujo que muestra el proceso del algoritmo Enc según la Realización 4.

La Fig. 17 es un diagrama de flujo que muestra el proceso del algoritmo Dec según la Realización 4.

La Fig. 18 es un diagrama de flujo que muestra el proceso del algoritmo Setup según la Realización 5.

La Fig. 19 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen según la Realización 5.

La Fig. 20 es un diagrama de flujo que muestra el proceso del algoritmo Enc según la Realización 5.

La Fig. 21 es un diagrama de flujo que muestra el proceso del algoritmo Dec según la Realización 5.

La Fig. 22 muestra una comparación de esquemas de cifrado de producto interior no cero y esquemas de cifrado de producto interior cero en las Realizaciones 2 a 4 con el esquema de cifrado de producto interior no cero y el esquema de cifrado de producto interior cero descritos en la Literatura No de Patente 2.

La Fig. 23 es un diagrama que muestra un ejemplo de la configuración hardware de cada uno del dispositivo de generación de clave 100, el dispositivo de cifrado 200, el dispositivo de descifrado 300 y un dispositivo de delegación de clave 400.

Descripción de las realizaciones

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

En la siguiente descripción, un dispositivo de procesamiento es, por ejemplo, una CPU 911 (a ser descrita más tarde). Un dispositivo de almacenamiento es, por ejemplo, una ROM 913, una RAM 914 o un disco magnético 920 (cada uno que se describirá más tarde). Un dispositivo de comunicación es, por ejemplo, una placa de comunicación 915 (a ser descrita más tarde). Un dispositivo de entrada es, por ejemplo, un teclado 902 o la placa de comunicación 915 (cada uno que se describirá más tarde). Un dispositivo de salida es, por ejemplo, la RAM 914, el disco magnético 920, la placa de comunicación 915 o un LCD 901 (cada uno que se describirá más tarde). Es decir, el dispositivo de procesamiento, el dispositivo de almacenamiento, el dispositivo de comunicación, el dispositivo de entrada y el dispositivo de salida son hardware.

Se explicarán las notaciones en la siguiente descripción.

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

[Fórmula 101]

$$y \xleftarrow{R} A$$

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

[Fórmula 102]

$$y \xleftarrow{U} A$$

Un símbolo de vector indica una representación de vector de orden q sobre un campo finito F_q. Por ejemplo, se establece la Fórmula 103.

[Fórmula 103]

$\vec{x}$ denota

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

La Fórmula 104 denota el producto interior, indicado por la Fórmula 106, de dos vectores $\vec{x}$ y $\vec{v}$ indicados por la Fórmula 105.

[Fórmula 104]

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

[Fórmula 105]

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

[Fórmula 106]

$$\sum_{i=1}^{n}x_iv_i$$

Señalar que X^T denota la traspuesta de la matriz X.

Donde b_i (i = 1, …, n) es un elemento de un vector en un espacio V, es decir donde se establece la Fórmula 107, la Fórmula 108 representa un subespacio generado por la Fórmula 109.

[Fórmula 107]

$$b_i\in\mathbb{V}\ (i=1,\ldots,L)$$

[Fórmula 108]

$$\mathrm{span}\langle b_1,\ldots,b_L\rangle\subseteq\mathbb{V}\ (\mathrm{resp.}\ \mathrm{span}\langle\vec{x}_1,\ldots,\vec{x}_L\rangle)$$

[Fórmula 109]

$$b_1,\ldots,b_L\ (\mathrm{resp.}\ \vec{x}_1,\ldots,\vec{x}_L)$$

Para las bases B y B* indicadas por la Fórmula 110, se establece la Fórmula 111.

[Fórmula 110]

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

[Fórmula 111]

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

Para n de los vectores j = 1, …, n, $\vec{e}_j$ denota el vector de base canónica indicado por la Fórmula 112.

[Fórmula 112]

$$\vec{e}_j : (\overbrace{0\cdots0}^{j-1}, 1, \overbrace{0\cdots0}^{n-j}) \in \mathbb{F}_q^n \text{ para } j = 1, \ldots, n,$$

Señalar que GL(n, F_q) representa un grupo lineal general con un orden n sobre el campo finito F_q.

En la siguiente descripción, cuando "→" que indica un vector se une a un subíndice o superíndice, "→" se une como un superíndice al subíndice o superíndice. Del mismo modo, cuando "*" en una base B* se une a un subíndice o superíndice, "*" se une como un superíndice al subíndice o superíndice. Del mismo modo, cuando "*" en una base B* se une a un subíndice o superíndice, "*" se une como un superíndice al subíndice o superíndice. Del mismo modo, cuando t en un espacio V_t se une a un subíndice o superíndice, "t" se une como un subíndice al subíndice o superíndice.

En la siguiente descripción, un proceso criptográfico incluye un proceso de cifrado, un proceso de descifrado y un proceso de generación de clave.

Realización 1

Esta realización explica un concepto básico para implementar un cifrado de producto interior y una estructura del cifrado de producto interior.

En primer lugar, se explicará el concepto del cifrado de producto interior.

En segundo lugar, se explicarán espacios de vector de emparejamiento dual (DPVS) que son un espacio para implementar el cifrado de producto interior.

En tercer lugar, se explicará la estructura básica de un esquema de cifrado de producto interior a ser descrito en las siguientes realizaciones.

En cuarto lugar, se explicará la estructura básica de un sistema de procesamiento criptográfico 10 que implementa el esquema de cifrado de producto interior a ser descrito en las siguientes realizaciones.

En quinto lugar, se explicará el planteamiento básico para el esquema de cifrado de producto interior a ser descrito en las siguientes realizaciones.

<1. Concepto de cifrado de producto interior>

En primer lugar, se explicará el cifrado funcional.

El cifrado funcional es un concepto avanzado de cifrado. El cifrado funcional también es una generalización del cifrado de clave pública (PKE) y cifrado basado en ID (cifrado basado en Identidad; IBE). En sistemas de cifrado funcional, un receptor puede descifrar un texto cifrado usando una clave secreta que corresponde a un parámetro x si el parámetro x está adecuadamente relacionado con un parámetro y especificado para el texto cifrado. Más específicamente, el descifrado requiere R(x, y) = 1 para alguna relación R (relación R que se mantiene para (x, y)).

El cifrado de producto interior es un tipo de cifrado funcional.

El cifrado de producto interior incluye cifrado de producto interior cero (ZIPE) y cifrado de producto interior no cero (NIPE).

Según el cifrado de producto interior cero, un cifrado cifrado con un vector $\vec{x}$ se puede descifrar mediante una clave secreta asociada con un vector $\vec{y}$ de manera que $\vec{x} \cdot \vec{y} = 0$. Es decir, $R^{ZIPE}(\vec{x}, \vec{y}) = 1$ si se requiere si y sólo si $\vec{x} \cdot \vec{y} = 0$.

Según el cifrado de producto interior no cero, un cifrado cifrado con un vector $\vec{x}$ se puede descifrar mediante una clave secreta asociada con un vector $\vec{y}$ de manera que $\vec{x} \cdot \vec{y} \neq 0$. Es decir, $R^{NIPE}(\vec{x}, \vec{y}) = 1$ si se requiere si y sólo si $\vec{x} \cdot \vec{y} \neq 0$.

<2. Espacios de vector de emparejamiento dual>

En primer lugar, se describirán los 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, un elemento $g \neq 0 \in G$ 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) = $e(g, g)^{st}$ donde $e(g, g) \neq 1$.

En la siguiente descripción, permitamos que G_{bpg} sea un algoritmo que toma la entrada 1^{λ} y saca el valor 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 los espacios de vector de emparejamiento dual.

Los espacios de vector de emparejamiento dual (q, V, G_T, A, e) se pueden constituir por un producto directo de 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 el campo finito F_q indicado en la Fórmula 113, un grupo cíclico G_T del orden q y una base canónica A := (a_1, …, a_N) de un espacio V y tienen las siguientes operaciones (1) y (2) donde a_i es como se indica por la Fórmula 114.

[Fórmula 113]

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

[Fórmula 114]

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

Operación (1): Emparejamiento bilineal no degenerado

El emparejamiento en el espacio V se define por la Fórmula 115.

[Fórmula 115]

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

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(s, y)st y si e(x, y) = 1 para todo y ∈ V, entonces x = 0. Para todo i y j, e(a_i, a_j) = e(g, g)$^{\delta i,j}$ (δi,j que significa $\delta_{i,j}$) donde $\delta_{i,j}$ = 1 si i = j y $\delta_{i,j}$ = 0 si i ≠ j. También, e(g, g) ≠ 1 ∈ G_T.

Operación (2): Mapas estándar

La transformación lineal $\phi_{i,j}$ en el espacio V indicado por la Fórmula 116 se puede implementar fácilmente por la Fórmula 117.

[Fórmula 116]

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

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

[Fórmula 117]

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

Señalar que

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

Las transformaciones lineales $\phi_{i,j}$ se llamarán “mapas estándar”.

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

Se describirá un caso donde los espacios de vector de emparejamiento dual se construyen a partir de los grupos de emparejamiento bilineal simétrico descritos anteriormente. Los espacios de vector de emparejamiento dual se pueden construir a partir de grupos de emparejamiento bilineal asimétrico también. La siguiente descripción se puede aplicar fácilmente a un caso en el que los espacios de vector de emparejamiento dual se construyen a partir de grupos de emparejamiento bilineal asimétrico.

<3. Estructura básica de esquema de cifrado de producto interior>

En primer lugar, se explicará el esquema de cifrado de producto interior cero.

Una relación R^{ZIPE} en el esquema de cifrado de producto interior cero se define sobre un vector $\vec{x} \in F^n_q \backslash \{\vec{0}\}$, donde $\vec{v} \in F^n_q \backslash \{\vec{0}\}$, donde $R^{ZIPE}(\vec{x}, \vec{y}) := 1$ si y sólo si $\vec{x} \cdot \vec{y} = 0$.

Del mismo modo, una relación R^{NIPE} en el esquema de cifrado de producto interior no cero se define sobre un vector $\vec{x} \in F^n_q \backslash \{\vec{0}\}$ y un vector $\vec{v} \in F^n_q \backslash \{\vec{0}\}$, donde $R^{NIPE}(\vec{x}, \vec{y}) := 1$ si y sólo si $\vec{x} \cdot \vec{y} \neq 0$.

El esquema de cifrado de producto interior cero y el esquema de cifrado de producto interior no cero cada uno consta de cuatro algoritmos: Setup, KeyGen, Enc y Dec.

(Setup)

Un algoritmo Setup es un algoritmo aleatorizado que toma como entrada un parámetro de seguridad λ y saca parámetros públicos pk y una clave secreta maestra sk.

(KeyGen)

Un algoritmo KeyGen es un algoritmo aleatorizado que toma como entrada un vector $\vec{v}$, parámetros públicos pk y una clave secreta maestra sk y saca una clave de descifrado $sk_{\vec{v}}$.

(Enc)

Un algoritmo Enc es un algoritmo aleatorizado que toma como entrada un mensaje m, un vector $\vec{x}$ y parámetros públicos pk y saca un texto cifrado $ct_{\vec{x}}$.

(Dec)

Un algoritmo Dec es un algoritmo que toma como entrada el texto cifrado $ct_{\vec{x}}$ que se cifró bajo un vector $\vec{x}$, una clave de descifrado $sk_{\vec{v}}$ para el vector $\vec{v}$ y parámetros públicos pk y saca o bien un mensaje m o bien un símbolo distinguido $\perp$. El símbolo distinguido $\perp$ indica que podría no ser logrado el descifrado.

<4. Estructura básica del sistema de procesamiento criptográfico 10>

La Fig. 1 es un diagrama de configuración de un sistema de procesamiento criptográfico 10 que ejecuta el esquema de cifrado de producto interior cero y el esquema de cifrado de producto interior no cero.

Un dispositivo de generación de clave 100 ejecuta el algoritmo Setup tomando como entrada un parámetro de seguridad λ, para generar los parámetros públicos pk y una clave secreta maestra sk. El dispositivo de generación de clave 100 publicita los parámetros públicos pk generados. El dispositivo de generación de clave 100 también ejecuta el algoritmo KeyGen tomando como entrada un vector $\vec{v}$, para generar una clave de descifrado $sk_{\vec{v}}$ y distribuye la clave de descifrado $sk_{\vec{v}}$ a un dispositivo de descifrado 300 en secreto.

Un dispositivo de cifrado 200 ejecuta el algoritmo Enc tomando como entrada un mensaje m, un vector $\vec{x}$ y los parámetros públicos pk, para generar un texto cifrado $ct_{\vec{x}}$. El dispositivo de cifrado 200 transmite el texto cifrado $ct_{\vec{x}}$ generado al dispositivo de descifrado 300.

El dispositivo de descifrado 300 ejecuta el algoritmo Dec tomando como entrada los parámetros públicos pk, la clave de descifrado $sk_{\vec{v}}$ y el texto cifrado $ct_{\vec{x}}$ y saca un mensaje m' (= m) o un símbolo distinguido $\perp$.

<5. Planteamiento básico para el esquema de cifrado>

En una aplicación típica en la que se aplican espacios de vector de emparejamiento dual a procesamiento criptográfico, se generan un par de bases duales (u ortogonales), B y B*. Las bases B y B* se generan usando una transformación lineal completamente aleatoria X (matriz de transformación de base) uniformemente seleccionada a partir de GL(N, F_q). Particularmente, las bases B y B* se generan cada una a través de conversión de una base

canónica A usando transformaciones lineales X y $(X^{-1})^T$ donde N es el número de dimensiones de span<B> y span<B*>.

La aplicación típica en la que los espacios de vector de emparejamiento dual se aplican a procesamiento criptográfico emplea parte de la base B (llamada B^) como un parámetro público y parte de la base B* correspondiente (llamada B^*) como una clave secreta o puerta trampa.

En el cifrado de producto interior que se explica en las siguientes realizaciones, una forma especial de transformación lineal aleatoria X, que es $X \in GL(N, F_q)$, se emplea en lugar de la transformación lineal completamente aleatoria X descrita anteriormente. Esta forma especial de transformación lineal X puede disminuir los tamaños del texto cifrado y la clave secreta y disminuir el número de operaciones de emparejamiento que consumen mucho tiempo de procesar.

La Fig. 2 incluye un dibujo explicativo de una forma especial de transformación lineal X.

La transformación lineal completamente aleatoria X se muestra en (a) de la Fig. 2 y una forma especial de transformación lineal X se muestra en (b) de la Fig. 2. En (a) y (b) de la Fig. 2, las partes cuadradas indican componentes los valores de los cuales son números aleatorios distintos de 0. En (b) de la Fig. 2, los elementos en blanco indican componentes los valores de los cuales son 0. En (b) de la Fig. 2, los cuadrados sombreados indican componentes los valores de los cuales son los mismos. Señalar que N = 5.

Como se muestra en (a) de la Fig. 2, una transformación lineal X convencional tiene un tamaño de N^2 (aquí $5^2 = 25$). Por el contrario, como se muestra en (b) de la Fig. 2, una transformación lineal X empleada en el cifrado de producto interior que se explica en las siguientes realizaciones (a ser referida como una nueva transformación lineal X en lo sucesivo) tiene un tamaño de N + 1 (aquí 5 +1 = 6).

Como se mencionó anteriormente, las bases B y B* se generan a través de conversión de la base canónica A usando la transformación lineal X. Por consiguiente, los tamaños de las bases B y B* son proporcionales al tamaño de la transformación lineal X. Como se describió anteriormente, parte de la base B y parte de la base B* forman el parámetro público y la clave secreta. Por lo tanto, los tamaños del parámetro público y la clave secreta son proporcionales a la transformación lineal X. Más específicamente, con la transformación lineal X convencional, los tamaños del parámetro público y la clave secreta son proporcionales a N^2, mientras que con la nueva transformación lineal X, los tamaños del parámetro público y la clave secreta son proporcionales a N+1.

Consecuentemente, con la transformación lineal X convencional, el proceso de generación de una clave de usuario o el proceso de cifrado lleva un tiempo que es proporcional a N^2, mientras que con la nueva transformación lineal X, el proceso de generación de la clave de usuario o el proceso de cifrado lleva un tiempo que es proporcional a N+1. Es decir, con la nueva transformación lineal X, el tiempo de cálculo es del orden de N.

Un método específico de realización de un texto cifrado de tamaño constante y descifrado eficiente se explicará con respecto al esquema de cifrado de producto interior no cero como ejemplo.

Señalar que en la explicación de un tamaño de texto cifrado, la descripción de vector no se incluirá como parte del texto cifrado. Del mismo modo, señalar que en la explicación de un tamaño de clave de descifrado también, la descripción de vector no se incluirá como parte del texto cifrado.

Una explicación se dará usando una forma simplificada del esquema de producto interior no cero que se describe en las siguientes realizaciones.

Un texto cifrado en un esquema de cifrado de producto interior no cero simplificado consta de dos elementos de vector $(c_0, c_1) \in G^5 \times G^n$ y $c_3 \in G_T$. Una clave secreta consta de dos elementos de vector k^*_0 y $k^*_1 \in G^5 \times G^n$. Señalar que $(c_0, c_1) \in G^5 \times G^n$ significa que c_0 consta de cinco elementos de G y c_1 consta de n elementos de G. Del mismo modo, k^*_0 y $k^*_1 \in G^5 \times G^n$ significa que k^*_0 consta de cinco elementos de G y k^*_1 consta de n elementos de G.

Por lo tanto, para lograr un texto cifrado de tamaño constante, $c_1 \in G^*$ necesita ser comprimido a un tamaño constante en n.

Se emplea la transformación lineal X especial indicada por la Fórmula 118.

[Fórmula 118]

$$X := \begin{pmatrix} \mu & & \mu_1' \\ & \ddots & \vdots \\ & \mu & \mu_{n-1}' \\ & & \mu_n' \end{pmatrix} \in \mathcal{H}(n, \mathbb{F}_q)$$

Señalar que μ, μ'$_1$, …, μ'$_n$ son valores seleccionados uniformemente a partir de un campo finito F_q y que un espacio en blanco en la transformación lineal X denota un valor constante 0 $\in F_q$. El valor constante 0 significa que el valor se fija a 0. Es decir, μ, μ'$_1$, …, μ'$_n$ son valores aleatorios uniformes que pueden tomar 0 también, mientras que un espacio en blanco en la transformación lineal X tiene un valor que se fija a 0. También, H(n, F_q) significa un conjunto de matrices de orden n que tienen el campo finito F_q como elemento.

El parámetro de sistema o la base pública de DPVS es la base B indicada por la Fórmula 119.

[Fórmula 119]

$$\mathbb{B} := \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} := \begin{pmatrix} \mu g & & \mu_1' g \\ & \ddots & \vdots \\ & \mu g & \mu_{n-1}' g \\ & & \mu_n' g \end{pmatrix}$$

Permitamos que un texto cifrado asociado con $\vec{x} := (x_1, \ldots, x_n)$ sea un texto cifrado c_1 indicado por la Fórmula 120.

[Fórmula 120]

$$c_1 := (\omega \vec{x})_{\mathbb{B}} = \omega(x_1 b_1 + \cdots + x_n b_n) = (x_1 \omega\mu g, \ldots, x_{n-1}\omega\mu g,\ \omega(\textstyle\sum_{i=1}^{n} x_i \mu_i')g)$$

Señalar que ω es un valor seleccionado uniformemente a partir del campo finito F_q.

Entonces, el texto cifrado c_1 se puede comprimir al vector $\vec{x}$ y dos elementos de grupo C_1 y C_2 indicados por la Fórmula 121.

[Fórmula 121]

$$C_1 := \omega\mu g,$$
$$C_2 := \omega(\textstyle\sum_{i=1}^{n} x_i \mu_i')g$$

Esto es debido a que el texto cifrado c_1 se puede obtener por (x_1C_1, …, $x_{n-1}C_1$, C_2). Señalar que $x_iC_1 = x_i\omega\mu g$ se mantiene para cada i de i = 1, …, n-1.

Por lo tanto, un texto cifrado (excluyendo el vector $\vec{x}$) puede constar de dos elementos de grupo y tiene un tamaño constante en n.

Permitamos que B* := (b*$_i$) sea la base ortogonal dual de B := (b_i) y que la base B* sea la clave secreta maestra en el esquema de cifrado de producto interior no cero simplificado. Señalar que (c_0, k*$_0$, c_3) se especifica de manera que $e(c_0, k^*_0) = g_T^{\zeta} \cdot g_T^{\omega\delta}$ y $c_3 := g_T^{\zeta} m \in G_T$. También, señalar que una clave secreta para el vector $\vec{v}$ se fija como $k^*_1 := (\delta\vec{v})_{B^*} = \delta(v_1 b^*_1 + \ldots + v_n b^*_n)$.

A partir de la ortonormalidad dual de las bases B y B*, entonces se mantiene que $e(c_1, k^*_1) = g_T^{\omega\delta(\vec{x}\cdot\vec{v})}$. Por lo tanto, un descifrador puede calcular $g_T^{\omega\delta}$ si y sólo si $\vec{x}\cdot\vec{y} \neq 0$. Es decir, el descifrador puede obtener un mensaje m por la Fórmula 122.

[Fórmula 122]

$$c_3 \cdot e(c_0, k_0^*)^{-1} \cdot e(c_1, k_1^*)^{(\vec{x}\cdot\vec{v})^{-1}}$$

El texto cifrado c_1 se expresa como (x_1C_1, …, $x_{n-1}C_1$, C_2) $\in G^n$ y la clave secreta k^*_1 se analiza sintácticamente como una n tupla (K_1, …, K_n). Por lo tanto, el valor de $e(c_1, k^*_1)$ es como se indica por la Fórmula 123.

[Fórmula 123]

$$\prod_{i=1}^{n-1} e(x_i C_1, K_i) \cdot e(C_2, K_n)$$
$$= \prod_{i=1}^{n-1} e(C_1, x_i K_i) \cdot e(C_2, K_n)$$
$$= e(C_1, \sum_{i=1}^{n-1} x_i K_i) \cdot e(C_2, K_n)$$

Es decir, n-1 multiplicaciones escalares en G y dos operaciones de emparejamiento son bastantes para calcular $e(c_1, k^*_1)$. Es decir, solamente se requiere un número (constante) pequeño de operaciones de emparejamiento para el descifrado. Generalmente, las operaciones de emparejamiento llevan un tiempo de procesamiento largo. Disminuyendo el número de operaciones de emparejamiento, se puede acortar el tiempo de procesamiento como el proceso entero.

En el esquema de cifrado de producto interior no cero simplificado, el texto cifrado c_1 consta de solamente un vector de base (parte de codificación real) donde se fija el vector $\vec{x}$ y la clave secreta k^*_1 consta solamente de un vector de base (parte de codificación real) donde se fija el vector $\vec{v}$.

En el esquema de cifrado de producto interior no cero que se describe en las siguientes realizaciones, a fin de mejorar la seguridad, los vectores de base para una parte de codificación real así como para una parte oculta, una parte de aleatoriedad de clave secreta y una parte de aleatoriedad de texto cifrado se añaden al texto cifrado c_1 y la clave secreta k^*_1.

Para este propósito, la transformación lineal X se extiende como se indica por la Fórmula 124.

[Fórmula 124]

$$X := \begin{pmatrix} X_{1,1} & \cdots & X_{1,4} \\ \vdots & & \vdots \\ X_{4,1} & \cdots & X_{4,4} \end{pmatrix}$$

Señalar que cada $X_{i,j}$ es de la forma de $X \in H(n, F_q)$ indicada por la Fórmula 118. El espacio de vector consta de cuatro subespacios ortogonales. Es decir, el espacio de vector consta de cuatro subespacios ortogonales para la parte de codificación real, la parte oculta, la parte de aleatoriedad de clave secreta y la parte de aleatoriedad de texto cifrado.

Realización 2

En la Realización 2, se describirá un esquema de cifrado de producto interior no cero que tiene un texto cifrado de tamaño constante.

La Fig. 3 es un diagrama de configuración de un dispositivo de generación de clave 100 según la Realización 2. La Fig. 4 es un diagrama de configuración de un dispositivo de cifrado 200 según la Realización 2. La Fig. 5 es un diagrama de configuración de un dispositivo de descifrado 300 según la Realización 2.

Las Fig. 6 y 7 son diagramas de flujo que muestran la operación del dispositivo de generación de clave 100 según la realización 2, en la cual la Fig. 6 es un diagrama de flujo que muestra el proceso del algoritmo Setup según la Realización 2 y la Fig. 7 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen según la Realización 2. La Fig. 8 es un diagrama de flujo que muestra la operación del dispositivo de cifrado 200 según la Realización 2, es decir, un diagrama de flujo que muestra el proceso del algoritmo Enc según la Realización 2. La Fig. 9 es un diagrama de flujo que muestra la operación del dispositivo de descifrado 300 según la Realización 2, es decir, un diagrama de flujo que muestra el proceso del algoritmo Dec según la Realización 2.

En la siguiente descripción, permitamos que un vector $\vec{x} := (x_1, \ldots, x_n)$ a ser introducido mantenga $x_L \neq 0$ para cada entero L de L = 1, …, n-1 y permitamos que un vector $\vec{v} := (v_1, \ldots, v_n)$ a ser introducido mantenga $v_n \neq 0$

Se describirá el dispositivo de generación de clave 100.

Como se muestra en la Fig. 3, el dispositivo de generación de clave 100 se dota con una parte de generación de clave maestra 110, una parte de almacenamiento de clave maestra 120, una parte de entrada de información 130, una parte de generación de clave de descifrado 140 y una parte de distribución de clave 150. La parte de generación de clave maestra 110 se dota con una parte de generación de espacio 111, una parte de generación de matriz 112, una parte de generación de base 113 y una parte de generación de clave 114. La parte de generación de clave 140 se dota con una parte de generación de número aleatorio 141 y una parte de generación de elemento de clave 142.

El proceso del algoritmo Setup se describirá con referencia a la Fig. 6.

(S101: Paso de generación de espacio)

La parte de generación de espacio 111 toma el parámetro de seguridad 1^{λ} como entrada y ejecuta G_{bpg} con un dispositivo de procesamiento, para generar el parámetro $param_G := (q, G, G_T, g, e)$ de grupos de emparejamiento bilineal simétrico.

Además, la parte de generación de espacio 111 fija $N_0 := 5$ y $N_1 := 4n$. Entonces, para cada t de t = 0, 1, la parte de generación de espacio 111 toma como entrada el parámetro de seguridad 1^{λ}, N_t y el parámetro $param_G$ de los grupos de emparejamiento bilineal simétrico y ejecuta G_{dpvs} con el dispositivo de procesamiento, para generar un parámetro $param_{vt} := (q, V_t, G_T, A_t, e)$ de los espacios de vector de emparejamiento dual.

(S102: Paso de generación de transformación lineal)

Con el dispositivo de procesamiento, la parte de generación de matriz 112 genera una transformación lineal X_0, como se indica por la Fórmula 125.

[Fórmula 125]

$$X_0 := (\chi_{0,i,j})_{i,j=1,\ldots,5} \xleftarrow{U} GL(N_0, \mathbb{F}_q)$$

Señalar que $(\chi_{0,i,j})_{i,j=1,\ldots,5}$ en la Fórmula 125 significa una matriz que concierne a los subíndices i y j de una matriz $\chi_{0,i,j}$.

Con el dispositivo de procesamiento, la parte de generación de matriz 112 genera la transformación lineal X_t, como se indica por la fórmula 126.

[Fórmula 126]

$$X_1 \xleftarrow{U} \mathcal{L}(N_1, \mathbb{F}_q)$$

Señalar que $L(N, F_q)$ en la Fórmula 126 es como se indica por la Fórmula 127.

[Fórmula 127]

$$\mathcal{L}(N, \mathbb{F}_q) :=$$

$$\left\{ X := \begin{pmatrix} X_{1,1} \cdots X_{1,4} \\ \vdots \quad \vdots \\ X_{4,1} \cdots X_{4,4} \end{pmatrix} \middle| X_{i,j} := \begin{pmatrix} \mu_{i,j} & & \mu'_{i,j,1} \\ & \ddots & \vdots \\ & \mu_{i,j} & \mu'_{i,j,n-1} \\ & & \mu'_{i,j,n} \end{pmatrix} \in \mathcal{H}(n, \mathbb{F}_q) \text{ para } i,j = 1,\ldots,4 \right\}$$

$$\cap\ GL(N, \mathbb{F}_q),$$

$$\mathcal{H}(n, \mathbb{F}_q) := \left\{ \begin{pmatrix} u & & u'_1 \\ & \ddots & \vdots \\ & u & u'_{n-1} \\ & & u'_n \end{pmatrix} \middle| \begin{array}{l} u, u'_L \in \mathbb{F}_q \text{ para } L = 1,\ldots,n, \\ \text{un elemento en blanco en la} \\ \text{matriz denota } 0 \in \mathbb{F}_q \end{array} \right\}$$

Señalar que $\{\mu_{i,j}, \mu'_{i,j,L}\}_{i,j=1,\ldots,4;L=1,\ldots,n}$ en la siguiente descripción denota un elemento distinto del valor constante 0 en la transformación lineal X_1.

(S103: Paso de generación de base B)

Con el dispositivo de procesamiento, la parte de generación de base 113 genera una base B_0 y las variables $B_{i,j}$ y $B'_{i,j,L}$, como se indica por la Fórmula 128.

[Fórmula 128]

$$b_{0,i} := (\chi_{0,i,1},\ldots,\chi_{0,i,5})_{\mathbb{A}} = \sum_{j=1}^{5} \chi_{0,i,j} a_j \quad \text{para } i = 1,\ldots,5,$$

$$\mathbb{B}_0 := (b_{0,1},\ldots,b_{0,5}),$$

$$B_{i,j} := \mu_{i,j} g,\ B'_{i,j,L} := \mu'_{i,j,L} g \quad \text{para } i,j = 1,\ldots,4; L = 1,\ldots,n$$

Con el dispositivo de procesamiento, la parte de generación de base 113 también genera una base B^*_0 y una base B^*_1, como se indica por la Fórmula 129.

[Fórmula 129]

$$\text{para } t = 0,1$$

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

$$b^*_{t,i} := (\vartheta_{t,i,1},\ldots,\vartheta_{t,i,N_t})_{\mathbb{A}} = \sum_{j=1}^{N_t} \vartheta_{t,i,j} a_j \text{ para } i = 1,\ldots,N_t,$$

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

(S104: Paso de generación de base B^)

Con el dispositivo de procesamiento, la parte de generación de clave 114 genera las bases $B^\wedge_0$, $B^{\wedge *}_0$ y $B^{\wedge *}_1$, como se indica por la Fórmula 130.

[Fórmula 130]

$$\hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,3}, b_{0,5}),$$

$$\hat{\mathbb{B}}^*_0 := (b^*_{0,1}, b^*_{0,3}, b^*_{0,4}),$$

$$\hat{\mathbb{B}}^*_1 := (b^*_{1,1},\ldots,b^*_{1,n}, b^*_{1,2n+1},\ldots,b^*_{1,3n})$$

(S105: Paso de generación de clave maestra)

Con el dispositivo de procesamiento, la parte de generación de clave 114 fija los parámetros públicos pk := (1^λ, $param_n$, $B^\wedge_0$, $\{B_{i,j}, B'_{i,j,L}\}_{i=1,4;j=1,\ldots,4;L=1,\ldots,n}$) y la clave secreta maestra sk := $\{B^{\wedge *}_t\}_{t=0,1}$. Entonces, la parte de generación de clave 114 almacena los parámetros públicos pk y la clave secreta maestra sk en la parte de almacenamiento de clave maestra 120.

Señalar que $param_n := (\{param_{Vt}\}_{t=0,1}, g_T)$.

Más específicamente, desde S101 hasta S105, el dispositivo de generación de clave 100 ejecuta el algoritmo Setup indicado por la Fórmula 132 usando el algoritmo $G^{(1)}_{ab}$ indicado por la Fórmula 131, para generar los parámetros públicos pk y la clave secreta maestra sk.

[Fórmula 131]

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

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

$N_0 := 5,\ N_1 := 4n$,

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

$\psi \xleftarrow{U} \mathbb{F}_q^{\times},\ g_T := e(g,g)^{\psi}, \mathrm{param}_n := (\{\mathrm{param}_{\mathbb{V}_t}\}_{t=0,1}, g_T)$,

$X_0 := (\chi_{0,i,j})_{i,j=1,..,5} \xleftarrow{U} GL(N_0,\mathbb{F}_q), X_1 \xleftarrow{U} \mathcal{L}(N_1,\mathbb{F}_q)$, a partir de entonces,

$\{\mu_{i,j},\mu'_{i,j,L}\}_{i,j=1,..,4;L=1,..,n}$ denota entradas no cero de X_1,

$b_{0,i} := (\chi_{0,i,1},..,\chi_{0,i,5})_{\mathbb{A}} = \sum_{j=1}^{5} \chi_{0,i,j} a_j$ para $i=1,\ldots,5,\ \mathbb{B}_0 := (b_{0,1},\ldots,b_{0,5})$,

$B_{i,j} := \mu_{i,j} g,\ B'_{i,j,L} := \mu'_{i,j,L} g$ para $i,j=1,\ldots,4; L=1,\ldots,n$,

para $t=0,1$ $(\vartheta_{t,i,j})_{i,j=1,..,N_t} := \psi \cdot (X_t^T)^{-1}$,

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

devolver $(\mathrm{param}_n,\mathbb{B}_0,\mathbb{B}^*_0\{B_{i,j},B'_{i,j,L}\}_{i,j=1,..,4;L=1,..,n},\mathbb{B}^*_1)$.

[Fórmula 132]

$\mathrm{Setup}(1^{\lambda},n)$:

$(\mathrm{param}_n,\mathbb{B}_0,\mathbb{B}^*_0,\{B_{i,j},B'_{i,j,L}\}_{i,j=1,..,4;L=1,..,n},\mathbb{B}^*_1) \xleftarrow{R} \mathcal{G}_{\mathrm{ob}}^{(1)}(1^{\lambda},n)$,

$\hat{\mathbb{B}}_0 := (b_{0,1},b_{0,3},b_{0,5}), \hat{\mathbb{B}}^*_0 := (b^*_{0,1},b^*_{0,3},b^*_{0,4}), \hat{\mathbb{B}}^*_1 := (b^*_{1,1},..,b^*_{1,n},b^*_{1,2n+1},..,b^*_{1,3n})$,

devolver $\mathrm{pk} := (1^{\lambda},\mathrm{param}_n,\hat{\mathbb{B}}_0,\{B_{i,j},B'_{i,j,L}\}_{i=1,4;j=1,..,4;L=1,..,n}), \mathrm{sk} := \{\hat{\mathbb{B}}^*_t\}_{t=0,1}$.

Señalar que los parámetros públicos se publicitan a través de, por ejemplo, una red, de modo que el dispositivo de cifrado 200 y el dispositivo de descifrado 300 puede adquirirlos.

En S103, en lugar de la base B_1, se generó la variable $B_{i,j}$. Si la base B_1 tiene que ser generada, será como se indica por la Fórmula 133.

[Fórmula 133]

$$\begin{pmatrix} b_{1,(i-1)n+1} \\ \vdots \\ b_{1,in} \end{pmatrix} := \begin{pmatrix} B_{i,1} & & B'_{i,1,1} & & B_{i,4} & & B'_{i,4,1} \\ & \ddots & \vdots & \cdots & & \ddots & \vdots \\ & & B_{i,1} & B'_{i,1,n-1} & & B_{i,4} & B'_{i,4,n-1} \\ & & & B'_{i,1,n} & & & B'_{i,4,n} \end{pmatrix}$$

para *i = 1, …, 4*

$\mathbb{B}_1 := (b_{1,1},\ldots,b_{1,4n})$

Un elemento en blanco en la matriz de la Fórmula 133 indica un valor de componente $0 \in G$. La base B_1 es una base ortogonal de la base B^*_1. Es decir, $e(b_{1,j}, b^*_{1,j}) = g_T$ y $e(b_{1,j}, b^*_{1,j}) = 1$ para enteros i, j que satisfacen $1 \leq i \neq j \leq 4n$.

El proceso del algoritmo KeyGen se describirá con referencia a la Fig. 7.

(S111: Paso de entrada de información)

Con el dispositivo de entrada, la parte de tuerca de información 130 toma como entrada el vector $\vec{v}$.

(S112: Paso de generación de número aleatorio)

Con el dispositivo de procesamiento, la parte de generación de número aleatorio 141 genera números aleatorios, como se indica por la Fórmula 134.

[Fórmula 134]

$$\delta, \varphi_0, \varphi_1, \xleftarrow{U} \mathbb{F}_q$$

(S113: Paso de generación de elemento k^*_0)

Con el dispositivo de procesamiento, la parte de generación de elemento de clave 142 genera el elemento k^*_0, que es un elemento de una clave de descifrado $sk_{\vec{v}}$, como se indica por la Fórmula 135.

[Fórmula 135]

$$k_0^* := (\delta, 0, 1, \varphi_0, 0)_{\mathbb{B}_0^*}$$

Como se mencionó anteriormente, para las bases B y B* indicadas por la Fórmula 110, se establece la Fórmula 111. Por lo tanto, la Fórmual 135 significa que: δ se fija como el coeficiente para el vector de base $b^*_{0,1}$ de la base B^*_0; 0 se fija como el coeficiente para el vector de base $b^*_{0,2}$; 1 se fija como el coeficiente para el vector de base $b^*_{0,3}$; ϕ_0 se fija como el coeficiente para el vector de base $b^*_{0,4}$; y 0 se fija como el coeficiente para el vector de base $b^*_{0,5}$.

(S114: Paso de generación de elemento k^*_1)

Con el dispositivo de procesamiento, la parte de generación de elemento de clave 142 genera el elemento k^*_1, que es un elemento de una clave de descifrado $sk_{\vec{v}}$, como se indica por la Fórmula 136.

[Fórmula 136]

$$k_1^* := (\overbrace{\delta\vec{v}}^{n}, \overbrace{0^n}^{n}, \overbrace{\varphi_1\vec{v}}^{n}, \overbrace{0^n}^{n})_{\mathbb{B}_1^*}$$

Como con la Fórmula 135, la Fórmula 136 significa que: $\delta v_1, \ldots, \delta v_n$ se fijan cada uno como el coeficiente para los vectores de base $b^*_{1,1}, \ldots, b^*_{1,n}$ de la base B^*_1; 0 se fija como el coeficiente para los vectores de base $b^*_{1,n+1}, \ldots, b^*_{1,2n}$; $\phi_1 v_1, \ldots, \phi_1 v_n$ se fijan cada uno como el coeficiente para los vectores de base $b^*_{1,2n+1}, \ldots, b^*_{1,3n}$; y 0 se fija como el coeficiente para los vectores de base $b^*_{1,3n+1}, \ldots, b^*_{1,4n}$.

(S115: Paso de distribución de clave)

Por ejemplo, con el dispositivo de comunicación, la parte de distribución de clave 150 distribuye la clave de descifrado $sk_{\vec{v}}$, constituida, como elementos, por: el vector $\vec{v}$ introducido en S111; el elemento k^*_0 generado en S113; y el elemento k^*_1 generado en S114, al dispositivo de descifrado 300 en secreto a través de la red. Como una cuestión de rutina, la clave de descifrado $sk_{\vec{v}}$ se podría distribuir también al dispositivo de descifrado 300 mediante otro método.

Más específicamente, desde S111 hasta S114, el dispositivo de generación de clave 100 ejecuta el algoritmo KeyGen indicado por la Fórmula 137, para generar la clave de descifrado $sk_{\vec{v}}$. Entonces, en S115, el dispositivo de generación de clave 100 distribuye la clave de descifrado $sk_{\vec{v}}$ generada al dispositivo de descifrado 300.

[Fórmula 137]

$$\begin{aligned}
&\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v}):\\
&\delta, \varphi_0, \varphi_1, \xleftarrow{U} \mathbb{F}_q,\\
&k_0^* := (\delta, 0, 1, \varphi_0, 0)_{\mathbb{B}_0^*},\\
&k_1^* := (\overbrace{\delta\vec{v}}^{n}, \overbrace{0^n}^{n}, \overbrace{\varphi_1\vec{v}}^{n}, \overbrace{0^n}^{n})_{\mathbb{B}_1^*},\\
&\text{devolver } \mathsf{sk}_{\vec{v}} := (\vec{v}, k_0^*, k_1^*).
\end{aligned}$$

Se describirá el dispositivo de cifrado 200.

Como se muestra en la Fig. 4, el dispositivo de cifrado 200 se dota con una parte de adquisición de parámetro público 210, una parte de entrada de información 220, una parte de generación de texto cifrado 230 y una parte de transmisión de datos 240. La parte de generación de texto cifrado 230 se dota con una parte de generación de número aleatorio 231 y una parte de generación de elemento de cifrado 232.

El proceso del algoritmo Enc se describirá con referencia a la Fig. 8.

(S121: Paso de adquisición de parámetro público)

Por ejemplo, con el dispositivo de comunicación, la parte de adquisición de parámetro público 210 adquiere los parámetros públicos pk generados por el dispositivo de generación de clave 100, a través de la red.

(S122: Paso de entrada de información)

Con el dispositivo de entrada, la parte de entrada de información 220 toma como entrada el vector $\vec{x}$.

También, con el dispositivo de entrada, la parte de entrada de informaicón 222 toma como entrada un mensaje m.

(S123: Paso de generación de número aleatorio)

Con el dispositivo de procesamiento, la parte de generación de número aleatorio 231 genera números aleatorios, como se indica por la Fórmula 138.

[Fórmula 138]

$$\omega, \eta_0, \eta_1, \zeta \xleftarrow{U} \mathbb{F}_q$$

(S124: Paso de generación de elemento c_0)

Con el dispositivo de procesamiento, la parte de generación de elemento de cifrado 232 genera el elemento c_0, que es un elemento de un texto cifrado $ct_{\vec{x}}$, como se indica por la Fórmula 139.

[Fórmula 139]

$$c_0 := (-\omega, 0, \zeta, 0, \eta_0)_{\mathbb{B}_0}$$

Como con la Fórmula 135, la Fórmula 139 signfica que: -ω se fija como el coeficiente para el vector de base $b_{0,1}$, de la base B_0; 0 se fija como el coeficiente para el vector de base $b_{0,2}$; ζ se fija como el coeficiente para el vector de base $b_{0,3}$; 0 se fija como el coeficiente para el vector de base $b_{0,4}$; y η_0 se fija como el coeficiente para el vector de base $b_{0,5}$.

(S125: Paso de generación de elemento C)

Con el dispositivo de procesamiento, la parte de generación de elemento de cifrado 232 genera un elemento $C_{1,j}$ y un elemento $C_{2,j}$, que son elementos del texto cifrado $ct_{\vec{x}}$, como se indica por la Fórmula 140.

[Fórmula 140]

$$\text{para } j = 1, \ldots, 4$$

$$C_{1,j} := \omega B_{1,j} + \eta_1 B_{4j},$$

$$C_{2,j} := \sum_{L=1}^{n} x_L (\omega B'_{1,j,L} + \eta_1 B'_{4,j,L})$$

(S126: Paso de generación de elemento c_3)

Con el dispositivo de procesamiento, la parte de generación de elemento de cifrado 232 genera el elemento c_3, que es un elemento del texto cifrado $ct_{\vec{x}}$, como se indica por la Fórmula 141.

[Fórmula 141]

$$c_3 := g_T^{\zeta} m$$

(S127: Paso de transmisión de datos)

Por ejemplo, con el dispositivo de comunicación, la parte de transmisión de datos 240 transmite el texto cifrado $ct_{\vec{x}}$, constituido, como elementos, por: el vector $\vec{x}$ introducido en S122, el elemento c_0 generado en S124; los elementos $C_{1,j}$ y $C_{2,j}$ generados en S125; y el elemento c_3 generado en S126, al dispositivo de descifrado 300 a través de la red. Como una cuestión de rutina, el texto cifrado $ct_{\vec{x}}$ se podría transmitir también al dispositivo de descifrado 300 mediante otro método.

Más específicamente, desde S121 hasta S126, el dispositivo de cifrado 200 ejecuta el algoritmo Enc indicado por la Fórmula 142, para generar el texto cifrado $ct_{\vec{x}}$. En S127, el dispositivo de cifrado 200 transmite el texto cifrado $ct_{\vec{x}}$ generado al dispositivo de descifrado 300.

[Fórmula 142]

$$\mathrm{Enc}(\mathrm{pk}, m, \vec{x}):$$

$$\omega, \eta_0, \eta_1, \zeta \xleftarrow{\cup} \mathbb{F}_q,\ c_0 := (-\omega, 0, \zeta, 0, \eta_0)_{\mathbb{B}_0},\ c_3 := g_T^{\zeta} m,$$

$$C_{1,j} := \omega B_{1,j} + \eta_1 B_{4j},\ C_{2,j} := \sum_{L=1}^{n} x_L (\omega B'_{1,j,L} + \eta_1 B'_{4,j,L}) \text{ para } j = 1, \ldots, 4,$$

$$\text{devolver } \mathrm{ct}_{\vec{x}} := (\vec{x}, c_0, \{C_{1,j}, C_{2,j}\}_{j=1,\ldots,4}, c_3).$$

Se describirá el dispositivo de descifrado 300.

Como se muestra en la Fig. 5, el dispositivo de descifrado 300 se dota con una parte de adquisición de clave de descifrado 310, una parte de recepción de datos 320, una parte de operación de emparejamiento 330 y una parte de cálculo de mensaje 340.

El proceso del algoritmo Dec se describirá con referencia a la Fig. 9.

(S131: Paso de adquisición de clave de descifrado)

Por ejemplo, con el dispositivo de comunicación, la parte de adquisición de clave de descifrado 310 adquiere $sk_{\vec{v}}$ distribuido por el dispositivo de generación de clave 100, a través de la red.

La parte de adquisición de clave de descifrado 310 también adquiere los parámetros públicos pk generados por el dispositivo de generación de clave 100.

(S132: Paso de recepción de datos)

Por ejemplo, con el dispositivo de comunicación, la parte de recepción de datos 320 recibe el texto cifrado $ct_{\vec{x}}$ transmitido por el dispositivo de cifrado 200, a través de la red.

(S133: Paso de cálculo de valor D^*_j)

Con el dispositivo de procesamiento, la parte de operación de emparejamiento 330 calcula el valor D^*_j, como se indica por la Fórmula 143.

[Fórmula 143]

para j = 1, …, 4

$$D_j^* := \sum_{L=1}^{n-1} ((\vec{x} \cdot \vec{v})^{-1} x_L) K^*_{(j-1)n+L}$$

Señalar que el elemento k^*_1 se analiza sintácticamente como 4n tuplas $(K^*_1, \ldots, K^*_{4n}) \in G^{4n}$.

(S134: Paso de operación de emparejamiento)

Con el dispositivo de procesamiento, la parte de operación de emparejamiento 330 ejecuta una operación de emparejamiento, como se indica por la Fórmula 144, para calcular el valor F.

[Fórmula 144]

$$F := e(c_0, k_0^*) \cdot \prod_{j=1}^{4} \left(e(C_{1,j}, D_j^*) \cdot e(C_{2,j}, K_{jn}^*) \right)$$

(S135: Paso de cálculo de mensaje)

Con el dispositivo de procesamiento, la parte de cálculo de mensaje 340 calcula un mensaje m', como se indica por la Fórmula 145.

[Fórmula 145]

$$m' := c_3 / F$$

Más específicamente, desde S131 hasta S135, el dispositivo de descifrado 300 ejecuta el algoritmo Dec indicado por la Fórmula 146, para calcular el mensaje m'.

[Fórmula 146]

$$\mathrm{Dec}(\mathrm{pk}, \mathrm{sk}_{\vec{v}} := (\vec{v}, k_0^*, k_1^*),\ \mathrm{ct}_{\vec{x}} := (\vec{x}, c_0, \{C_{1,j}, C_{2,j}\}_{j=1,\ldots,4}, c_3)):$$

Analizar sintácticamente k_1^* como una tupla 4n $(K_1^*, \ldots, K_{4n}^*) \in \mathbb{G}^{4n}$,

$$D_j^* := \sum_{L=1}^{n-1} ((\vec{x} \cdot \vec{v})^{-1} x_L) K_{(j-1)n+L}^* \quad \text{para} \quad j = 1, \ldots, 4,$$

$$F := e(c_0, k_0^*) \cdot \prod_{j=1}^{4} \left(e(C_{1,j}, D_j^*) \cdot e(C_{2,j}, K_{jn}^*) \right),$$

devolver $m' := c_3 / F$.

La Fórmula 133 indica que $B_1 := (b_{1,1}, \ldots, b_{1,4n})$ se especifica por $\{B_{i,j}, B'_{i,j,L}\}_{i,j=1,\ldots,4;L=1,\ldots,n}$. También, $\{B_{i,j}, B'_{i,j,L}\}_{i=1,4;j=1,\ldots,4;L=1,\ldots,n}$ incluido en una salida del algoritmo Setup se especifica por $B^{\wedge}_1 := (b_{1,1}, \ldots, b_{1,n}, b_{1,3n+1}, \ldots, b_{1,4n})$.

El algoritmo Dec se puede describir como el algoritmo Dec' indicado por la Fórmula 147.

[Fórmula 147]

$$\mathrm{Dec}'(\mathrm{pk}, \mathrm{sk}_{\vec{v}} := (\vec{v}, k_0^*, k_1^*),\ \mathrm{ct}_{\vec{x}} := (\vec{x}, c_0, \{C_{1,j}, C_{2,j}\}_{j=1,\ldots,4}, c_3)):$$

$$c_1 := (\overbrace{x_1 C_{1,1}, \ldots, x_{n-1} C_{1,1}, C_{2,1}}^{n} \quad \ldots, \overbrace{x_1 C_{1,4}, \ldots, x_{n-1} C_{1,4}, C_{2,4}}^{n}),$$

es decir, $c_1 = (\overbrace{\omega \vec{x}}^{n}, \overbrace{0^n}^{n}, \overbrace{0^n}^{n}, \overbrace{\eta_1 \vec{x}}^{n})_{\mathbb{B}_1}$, $F := e(c_0, k_0^*) \cdot e(c_1, (\vec{x} \cdot \vec{v})^{-1} k_1^*)$,

devolver $m' := c_3 / F$.

Como se indicó por la Fórmula 148, usando el algoritmo Dec', $F = g_T^{\zeta}$ se obtiene si $\vec{x} \cdot \vec{v} \neq 0$. Por lo tanto, el mensaje m' (=m) se puede obtener dividiendo $c_3 = g_T^{\zeta} m$ por F.

[Fórmula 148]

$$\begin{aligned} F &= e(c_0, k_0^*) \cdot e(c_1, (\vec{x} \cdot \vec{v})^{-1} k_1^*) \\ &= g_T^{-\omega\delta + \zeta} g_T^{\omega\delta (\vec{x} \cdot \vec{v}) / (\vec{x} \cdot \vec{v})} \\ &= g_T^{\zeta} \quad \text{si} \quad \vec{x} \cdot \vec{v} \neq 0. \end{aligned}$$

En el esquema de cifrado de producto interior no cero explicado en la Realización 2, el texto cifrado $ct_{\vec{x}}$ incluye un total de 13 elementos de G, es decir, 5 por elemento c_0 indicados por la Fórmula 139 y 8 por elementos $C_{1,j}$ y $C_{2,j}$ para cada entero j de j = 1, …, 4 indicado por la Fórmula 140. También, el texto cifrado $ct_{\vec{x}}$ incluye 1 elemento de G_T, es decir, 1 por elemento c_3 indicado por la Fórmula 141. En fin, el texto cifrado $ct_{\vec{x}}$ tiene un tamaño constante en n.

También, en el esquema de cifrado de producto interior no cero explicado en la Realización 2, el proceso de descifrado (algoritmo Dec) ejecuta un total de solamente 13 operaciones de emparejamiento, es decir, 5 por $e(c_0, k^*_0)$ y 8 por $\Pi_{j=1}^{4}(e(C_{1,j}, D^*_j) \cdot e(C_{2,j}, K^*_{jn}))$ indicado por la Fórmula 144. En fin, el proceso de descifrado requiere solamente un pequeño número de operaciones de emparejamiento.

Realización 3

En la realización 3, se describirá un esquema de cifrado de producto interior no cero que tiene una clave secreta de tamaño constante.

Las configuraciones de un dispositivo de generación de clave 100, un dispositivo de cifrado 200 y un dispositivo de descifrado 300 son respectivamente las mismas que las configuraciones del dispositivo de generación de clave 100, el dispositivo de cifrado 200 y el dispositivo de descifrado 300 mostrados en las Fig. 3, 4 y 5 según la Realización 2.

Las Fig. 10 y 11 son diagramas de flujo que muestran la operación del dispositivo de generación de clave 100 según la Realización 3, en la cual la Fig. 10 es un diagrama de flujo que muestra el proceso del algoritmo Setup según la Realización 3 y la Fig. 11 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen según la Realización 3. La Fig. 12 es un diagrama de flujo que muestra la operación del dispositivo de cifrado 200 según la Realización 3, es decir, un diagrama de flujo que muestra el proceso del algoritmo Enc según la Realización 3. La Fig. 13 es un diagrama de flujo que muestra la operación del dispositivo de descifrado 300 según la Realización 3, es decir, un diagrama de flujo que muestra el proceso del algoritmo Dec según la Realización 3.

En la siguiente descripción, permitamos que un vector $\vec{v} := (v_1, \ldots, v_n)$ a ser introducido mantenga $v_L \neq 0$ para cada entero L de L = 1, …, n-1 y permitamos que un vector $\vec{x} := (x_1, \ldots, x_n)$ a ser introducido mantenga $x_n \neq 0$.

Se describirá el dispositivo de generación de clave 100.

El proceso del algoritmo Setup se describirá con referencia a la Fig. 10.

Los procesos de S201 a S202 son los mismos que los procesos de S101 a S102 mostrados en la Fig. 6.

(S203: Paso de generación de base B)

Con un dispositivo de procesamiento, una parte de generación de base 113 genera una base D_0 y las variables $D_{i,j}$ y $D'_{i,j,L}$, como se indica por la Fórmula 149, de la misma manera que son la base B_0 y la variable $B_{i,j}$ de la Realización 2.

[Fórmula 149]

$$b_{0,i} := (\chi_{0,i,1},\ldots,\chi_{0,i,5})_{\mathbb{A}} = \sum_{j=1}^{5} \chi_{0,i,j} a_j \quad \text{para } i = 1,\ldots,5,$$

$$\mathbb{D}_0 := (b_{0,1},\ldots,b_{0,5}),$$

$$D_{i,j} := \mu_{i,j} g,\ D'_{i,j,L} := \mu'_{i,j,L} g \quad \text{para } i,j = 1,\ldots,4; L = 1,\ldots,n$$

Con el dispositivo de procesamiento, la parte de generación de base 113 también genera una base D^*_0 y una base D^*_1, como se indica por la Fórmula 150, de la misma manera que son la base B^*_0 y la base B^*_1 de la Realización 2.

[Fórmula 150]

para t = 0,1

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

$$b^*_{t,i} := (\vartheta_{t,i,1},\ldots,\vartheta_{t,i,N_t})_{\mathbb{A}} = \sum_{j=1}^{N_t} \vartheta_{t,i,j} a_j \quad \text{para } i = 1,\ldots,N_t,$$

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

Entonces, la parte de generación de base 113 trata la base D^*_0 como la base B_0, la base D_0 como una base B^*_0 y la base D^*_1 como una base B_1. También, para cada uno de los enteros i, j de i, j = 1, …, 4 y cada entero L de L = 1, …, n, la parte de generación de base 113 trata la variable $D_{i,j}$ como una variable $B^*_{i,j}$ y la variable $D'_{i,j,L}$ como una variable $B'^*_{i,j,L}$.

(S204: Paso de generación de base B^)

Con el dispositivo de procesamiento, la parte de generación de clave 114 genera las bases $B\hat{}_0$, $B\hat{}_1$ y $B\hat{}^*_0$, como se indica por la Fórmula 151.

[Fórmula 151]

$$\hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,3}, b_{0,5}),$$

$$\hat{\mathbb{B}}_0^* := (b_{0,1}^*, b_{0,3}^*, b_{0,4}^*),$$

$$\hat{\mathbb{B}}_1 := (b_{1,1,\ldots}, b_{1,n}, b_{1,3n+1,\ldots}, b_{1,4n})$$

(S205: Paso de generación de clave maestra)

Con el dispositivo de procesamiento, la parte de generación de clave 114 fija los parámetros públicos pk := (1^{λ}, $param_n$, $\{B^{\wedge}\}_{t=0,1}$) y la clave secreta maestra sk := $B^{\wedge *}_0$, $\{B^*_{i,j}, B'^*_{i,j,L}\}_{i=1,3;j=1,\ldots,4;L=1,\ldots,n}$. Entonces, la parte de generación de clave 114 almacena los parámetros públicos pk y la clave secreta maestra sk en una parte de almacenamiento de clave maestra 120.

Señalar que $param_n := (\{param_{VI}\}_{t=0,1}, g_T)$.

Más específicamente, desde S201 hasta S205, el dispositivo de generación de clave 100 ejecuta el algoritmo Setup indicado por la Fórmula 153 usando el algoritmo $G^{(2)}_{ob}$ indicado por la Fórmula 152, para generar los parámetros públicos pk y la clave secreta maestra sk. Como se indica por la Fórmula 152, el algoritmo $G^{(2)}_{ob}$ emplea el algoritmo $G^{(1)}_{ob}$ indicado por la Fórmula 131.

[Fórmula 152]

$$\mathcal{G}_{ob}^{(2)}(1^{\lambda}, n):$$

$$(param_n, \mathbb{D}_0, \mathbb{D}_0^*, \{D_{i,j}, D'_{i,j,L}\}_{i,j=1,\ldots,4;L=1,\ldots,n}, \mathbb{D}_1^*) \xleftarrow{R} \mathcal{G}_{ob}^{(1)}(1^{\lambda}, n),$$

$$\mathbb{B}_0 := \mathbb{D}_0^*,\ \mathbb{B}_0^* := \mathbb{D}_0,\ \mathbb{B}_1 := \mathbb{D}_1^*,\ B^*_{i,j} := D_{i,j},\ B'^*_{i,j,L} = D'_{i,j,L}$$

$$\text{para } i,j = 1,\ldots 4; L = 1,\ldots,n,$$

$$\text{devolver } (param_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B^*_{i,j}, B'^*_{i,j,L}\}_{i,j=1,\ldots,4;L=1,\ldots,n}).$$

[Fórmula 153]

$$\text{Setup}(1^{\lambda}, n):$$

$$(param_n, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}_1, \{B^*_{i,j}, B'^*_{i,j,L}\}_{i,j=1,\ldots,4;L=1,\ldots,n}) \xleftarrow{R} \mathcal{G}_{ob}^{(2)}(1^{\lambda}, n),$$

$$\hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,3}, b_{0,5}),\ \hat{\mathbb{B}}_0^* := (b_{0,1}^*, b_{0,3}^*, b_{0,4}^*),$$

$$\hat{\mathbb{B}}_1 := (b_{1,1,\ldots}, b_{1,n}, b_{1,3n+1,\ldots}, b_{1,4n}),$$

$$\text{devolver } pk := (1^{\lambda}, param_n, \{\hat{\mathbb{B}}_t\}_{t=0,1}),$$

$$sk := (\hat{\mathbb{B}}_0^*, \{B^*_{i,j}, B'^*_{i,j,L}\}_{i=1,3;j=1,\ldots,4;L=1,\ldots,n}).$$

Señalar que los parámetros públicos se publicitan a través de, por ejemplo, una red, de modo que el dispositivo de cifrado 200 y el dispositivo de descifrado 300 pueden adquirirlos.

El proceso del algoritmo KeyGen se describirá con referencia a la Fig. 11.

Los procesos de S211 a S213 son los mismos que los procesos de S111 a S113 mostrados en la Fig. 7.

(S214: Paso de generación de elemento K*)

Con el dispositivo de procesamiento, una parte de generación de elemento de clave 142 genera los elementos $K^*_{1,j}$ y $K^*_{2,j}$ que son elementos de una clave de descifrado $sk_{v\rightarrow}$, como se indica por la Fórmula 154.

[Fórmula 154]

para j = 1, …, 4

$$K^*_{1,j} := \delta B^*_{1,j} + \varphi_1 B^*_{3,j},$$

$$K^*_{2,j} := \sum_{L=1}^{n} v_L (\delta B'^*_{1,j,L} + \varphi_1 B'^*_{3,j,L})$$

(S215: Paso de distribución de clave)

Por ejemplo, con un dispositivo de comunicación, una parte de distribución de clave 150 distribuye la clave de descifrado $sk_{\vec{v}}$, constituida, como elementos, por: el vector $\vec{v}$ introducido en S211; un elemento k^*_0 generado en S213; y los elementos $K^*_{1,j}$ y $K^*_{2,j}$ generados en S214, al dispositivo de descifrado 300 en secreto a través de la red. Como una cuestión de rutina, la clave de descifrado $sk_{\vec{v}}$ se podría distribuir también al dispositivo de descifrado 300 mediante otro método.

Más específicamente, desde S211 hasta S214, el dispositivo de generación de clave 100 ejecuta el algoritmo KeyGen indicado por la Fórmula 155, para generar la clave de descifrado $sk_{\vec{v}}$. Entonces, en S215, el dispositivo de generación de clave 100 distribuye la clave de descifrado $sk_{\vec{v}}$ generada al dispositivo de descifrado 300.

[Fórmula 155]

$$\begin{aligned}
&\text{KeyGen(pk, sk, } \vec{v}\text{)}: \\
&\delta, \varphi_0, \varphi_1 \xleftarrow{\cup} \mathbb{F}_q, \\
&k^*_0 := (\delta, 0, 1, \varphi_0, 0)_{\mathbb{B}^*_0}, \\
&K^*_{1,j} := \delta B^*_{1,j} + \varphi_1 B^*_{3,j}, \\
&K^*_{2,j} := \sum_{L=1}^{n} v_L (\delta B'^*_{1,j,L} + \varphi_1 B'^*_{3,j,L}) \text{ para } j = 1, \ldots, 4, \\
&\text{devolver } sk_{\vec{v}} := (\vec{v}, k^*_0, \{K^*_{1,j}, K^*_{2,j}\}_{j=1,\ldots,4}).
\end{aligned}$$

Se describirá el dispositivo de cifrado 200.

El proceso del algoritmo Enc se describirá con referencia a la Fig. 12.

Los procesos de S221 a S224 son los mismos que los procesos de S121 a S124 mostrados en la Fig. 8.

(S225: Paso de generación de elemento c_1)

Con el dispositivo de procesamiento, una parte de generación de elemento de cifrado 232 genera el elemento c_1, que es un elemento de un texto cifrado $ct_{\vec{x}}$, como se indica por la Fórmula 156.

[Fórmula 156]

$$c_1 := (\omega \vec{x}, 0^n, 0^n, \eta_1 \vec{x})_{\mathbb{B}_1}$$

Como con la Fórmula 135, la Fórmula 156 significa que: ω_{x1}, …, ω_{xn} se fijan cada uno como el coeficiente para los vectores de base $b^*_{1,1}$, …, $b^*_{1,n}$ de la base B_1; 0 se fija como el coeficiente para los vectores de base $b^*_{1,n+1}$, …, $b^*_{1,3n}$; y $\eta_1 x_1$, …, $\eta_1 x_n$ se fijan cada uno como el coeficiente para los vectores de base $b^*_{1,3n+1}$, …, $b^*_{1,4n}$.

El proceso de S226 es el mismo que el proceso de S126 mostrado en la Fig. 8.

(S227: Paso de transmisión de datos)

Por ejemplo, con el dispositivo de comunicación, una parte de transmisión de datos 240 transmite el texto cifrado $ct_{\vec{x}}$, constituida, como elementos, por: el vector $\vec{x}$ introducido en S222; un elemento c_0 generado en S224; el elemento c_1 generado en S225; y un elemento c_3 generado en S226, al dispositivo de descifrado 300 a través de la red. Como una cuestión de rutina, el texto cifrado $ct_{\vec{x}}$ se podría transmitir también al dispositivo de descifrado 300 mediante otro método.

Más específicamente, desde S221 hasta S226, el dispositivo de cifrado 200 ejecuta el algoritmo Enc indicado por la Fórmula 157, para generar el texto cifrado $ct_{\vec{x}}$. En S227, el dispositivo de cifrado 200 transmite el texto cifrado $ct_{\vec{x}}$ generado al dispositivo de descifrado 300.

[Fórmula 157]

$\mathsf{Enc}(\mathsf{pk}, m, \vec{x})$:

$\omega, \eta_0, \eta_1, \zeta \xleftarrow{\cup} \mathbb{F}_q,$

$c_0 := (-\omega, 0, \varsigma, 0, \eta_0)_{\mathbb{B}_0},$

$c_1 := (\omega\vec{x}, 0^n, 0^n, \eta_1\vec{x})_{\mathbb{B}_1},$

$c_3 := g_T^{\zeta} m,$

devolver $\mathsf{ct}_{\vec{x}} := (\vec{x}, c_0, c_1, c_3).$

Se describirá el dispositivo de descifrado 300.

El proceso del algoritmo Dec se describirá con referencia a la Fig. 13.

Los procesos de S231 a S232 son los mismos que los procesos de S131 a S132 mostrados en la Fig. 9.

(S233: Paso de cálculo de valor D_j)

Con el dispositivo de procesamiento, una parte de operación de emparejamiento 330 calcula el valor D_j, como se indica por la Fórmula 158.

[Fórmula 158]

para j = 1, …, 4

$$D_j := \sum_{L=1}^{n-1} ((\vec{x} \cdot \vec{v})^{-1} v_L) C_{(j-1)n+L}$$

Señalar que el elemento c_1 se analiza sintácticamente como 4n tuplas $(C_1, \ldots, C_{4n}) \in G^{4n}$.

(S234: Paso de operación de emparejamiento)

Con el dispositivo de procesamiento, la parte de operación de emparejamiento 330 ejecuta una operación de emparejamiento, como se indica por la Fórmula 159, para calcular el valor F.

[Fórmula 159]

$$F := e(c_0, k_0^*) \cdot \prod_{j=1}^{4} \left(e(D_j, K_{1,j}^*) \cdot e(C_{jn}, K_{2,j}^*) \right)$$

El proceso de S235 es el mismo que el proceso de S135 mostrados en la Fig. 9.

Más específicamente, desde S231 hasta S235, el dispositivo de descifrado 300 ejecuta el algoritmo Dec indicado por la Fórmula 160, para calcular un mensaje m'.

[Fórmula 160]

$\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_{\vec{v}} := (\vec{v}, k_0^*, \{K_{1,j}^*, K_{2,j}^*\}_{j=1,..,4}), \mathsf{ct}_{\vec{x}} := (\vec{x}, c_0, c_1, c_3))$:

Analizar sintácticamente c_1 como una tupla 4n $(C_1, \ldots, C_{4n}) \in \mathbb{G}^{4n}$,

$D_j := \sum_{L=1}^{n-1} ((\vec{x} \cdot \vec{v})^{-1} v_L) C_{(j-1)n+L}$ para $j = 1, \ldots, 4,$

$F := e(c_0, k_0^*) \cdot \prod_{j=1}^{4} \left(e(D_j, K_{1,j}^*) \cdot e(C_{jn}, K_{2,j}^*) \right),$

devolver $m' := c_3 / F.$

Señalar que $B^*_1 := (b^*_{i,1}, \ldots, b^*_{1,4n})$ se especifica por $\{B^*_{i,j}, B'^*_{i,j,L}\}_{i,j=1, \ldots, 4; L=1, \ldots, n}$. También, $\{B^*_{i,j}, B'^*_{i,j,L}\}_{i=1,3; j=1, \ldots, 4; L=1, \ldots, n}$ incluido en una salida del algoritmo Setup se especifica por $B^{\wedge *}_1 := (b^*_{1,1}, \ldots, b^*_{1,n}, b^*_{1,2+1}, \ldots, b^*_{1,3n})$.

El algoritmo Dec se puede describir como el algoritmo Dec' indicado por la Fórmula 161.

[Fórmula 161]

$\mathrm{Dec'}(\mathrm{pk}, \mathrm{sk}_{\vec{v}} := (\vec{v}, k_0^*, \{K_{1,j}^*, K_{2,j}^*\}_{j=1,\ldots,4}), \mathrm{ct}_{\vec{x}} := (\vec{x}, c_0, c_1, c_3)):$

$k_1^* := (\overbrace{v_1 K_{1,1}^*, \ldots, v_{n-1} K_{1,1}^*, K_{2,1}^*}^{n}, \quad \ldots, \overbrace{v_1 K_{1,4}^*, \ldots, v_{n-1} K_{1,4}^*, K_{2,4}^*}^{n}),$

es decir, $k_1^* = (\delta \vec{v}, 0^n, 0^n, \varphi_1 \vec{v})_{\mathbb{B}_1^*}$, $F := e(c_0, k_0^*) \cdot e((\vec{x} \cdot \vec{v})^{-1} c_1, k_1^*),$

devolver $m' := c_3 / F.$

En el esquema de cifrado de producto interior no cero explicado en la Realización 3, la clave de descifrado $sk_{v\rightarrow}$ incluye un total de 13 elementos de G, es decir, 5 por el elemento k^*_0 indicado por la Fórmula 135 y 8 por los elementos $K^*_{i,j}$ y $K^*_{2,j}$ para cada entero j de j = 1, …, 4 indicado por la Fórmula 154. En fin, la clave de descifrado $sk_{v\rightarrow}$ tiene un tamaño constante en n.

También, en el esquema de cifrado de producto interior no cero explicado en la Realización 3, el proceso de descifrado (algoritmo Dec) ejecuta un total de solamente 13 operaciones de emparejamiento, es decir, 5 por $e(c_0, k^*_0)$ y 8 por $\Pi_{j=1}^{4}(e(D_j, K^*_{1,j}) \cdot e(C_{jn}, K^*_{2,j})$ indicado por la Fórmula 159. En fin, el proceso de descifrado requiere solamente un número pequeño de operaciones de emparejamiento.

Realización 4.

En la Realización 4, se describirá un esquema de cifrado de producto interior cero que tiene un texto cifrado de tamaño constante.

Las configuraciones de un dispositivo de generación de clave 100, un dispositivo de cifrado 200 y un dispositivo de descifrado 300 son respectivamente las mismas que las configuraciones del dispositivo de generación de clave 100, el dispositivo de cifrado 200 y el dispositivo de descifrado 300 mostrados en las Fig. 3, 4 y 5 según la Realización 2.

Las Fig. 14 y 15 son diagramas de flujo que muestran la operación del dispositivo de generación de clave 100 según la Realización 4, en la que la Fig. 14 es un diagrama de flujo que muestra el proceso del algoritmo Setup según la Realización 4 y la Fig. 15 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen según la Realización 4. La Fig. 16 es un diagrama de flujo que muestra la operación del dispositivo de cifrado 200 según la Realización 4, es decir, un diagrama de flujo que muestra el proceso del algoritmo Enc según la Realización 4. La Fig. 17 es un diagrama de flujo que muestra la operación del dispositivo de descifrado 300 según la Realización 4, es decir, un diagrama de flujo que muestra el proceso del algoritmo Dec según la Realización 4.

En la siguiente descripción, permitamos que un vector $\vec{x} := (x_1, \ldots, x_n)$ a ser introducido mantenga $x_L \neq 0$ para cada entero L de L = 1, …, n-1 y permitamos que un vector $\vec{v} := (v_1, \ldots, v_n)$ a ser introducido mantenga $v_n \neq 0$

Se describirá el dispositivo de generación de clave 100.

El proceso del algoritmo Setup se describirá con referencia a la Fig. 14.

(S301: Paso de generación de espacio)

La parte de generación de espacio 111 toma el parámetro de seguridad 1^λ como entrada y ejecuta G_{bpg} con un dispositivo de procesamiento, para generar el parámetro $param_G := (q, G, G_T, g, e)$ de grupos de emparejamiento bilineal simétrico.

Además, la parte de generación de espacio 111 fija N := 4 + 1. Entonces, la parte de generación de espacio 111 toma como entrada el parámetro de seguridad 1^λ, N y el parámetro $param_G$ de los grupos de emparejamiento bilineal simétrico y ejecuta G_{dpvs} con el dispositivo de procesamiento, para generar un parámetro $param_{vt} := (q, V, G_T, A, e)$ de los espacios de vector de emparejamiento dual.

(S302: Paso de generación de transformación lineal)

Con el dispositivo de procesamiento, una parte de generación de matriz 112 genera una transformación lineal X, como se indica por la Fórmula 162.

[Fórmula 162]

$$X := \xleftarrow{U} \mathcal{L}'(N, \mathbb{F}_q)$$

Señalar que $L'(N, F_q)$ en la Fórmula 162 es como se indica por la Fórmula 163.

[Fórmula 163]

$$\mathcal{L}'(N,\mathbb{F}_q) :=$$
$$\left\{ X := \begin{pmatrix} \chi_{0,0} & \chi_{0,1}\vec{e}_n & \cdots & \chi_{0,4}\vec{e}_n \\ \vec{\chi}_{1,0}^T & X_{1,1} & \cdots & X_{1,4} \\ \vdots & \vdots & & \vdots \\ \vec{\chi}_{4,0}^T & X_{4,1} & \cdots & X_{4,4} \end{pmatrix} \middle| \begin{array}{l} X_{i,j} \in \mathcal{H}(n,\mathbb{F}_q), \\ \vec{\chi}_{i,0} := (\chi_{i,0,L})_{L=1,\ldots,n} \in \mathbb{F}_q^n, \\ \chi_{0,0}, \chi_{0,j} \in \mathbb{F}_q \\ \quad \text{for } i,j = 1,\ldots,4 \end{array} \right\}$$
$$\cap\ GL(N,\mathbb{F}_q),$$

$$\mathcal{H}(n,\mathbb{F}_q) := \left\{ \begin{pmatrix} u & & & u_1' \\ & \ddots & & \vdots \\ & & u & u_{n-1}' \\ & & & u_n' \end{pmatrix} \middle| \begin{array}{l} u, u_L' \in \mathbb{F}_q \text{ para } L = 1,\ldots,n, \\ \text{un elemento en blanco en la} \\ \text{matriz denota } 0 \in \mathbb{F}_q \end{array} \right\}$$

Señalar que $\{\chi_{0,0}, \chi_{0,j}, \chi_{i,0,L}, \mu_{i,j}, \mu'_{i,j,L}\}_{i,j=1,\ldots,4;L=1,\ldots,n}$ en la siguiente descripción denota un elemento distinto del valor constante 0 en la transformación lineal X.

(S303: Paso de generación de base B)

Con el dispositivo de procesamiento, una parte de generación de base 113 genera las variables $B_{0,0}$, $B_{0,j}$, $B_{i,0,L}$, $B_{i,j}$ y $B'_{i,j,L}$, como se indica por la Fórmula 164.

[Fórmula 164]

para *i, j* = 1, …, 4; *L* = 1, …, n

$$B_{0,0} := \chi_{0,0} g,$$
$$B_{0,j} := \chi_{0,j} g,$$
$$B_{i,0,L} := \chi_{i,0,L} g,$$
$$B_{i,j} := \mu_{i,j} g,$$
$$B'_{i,j,L} := \mu'_{i,j,L} g$$

Con el dispositivo de procesamiento, la parte de generación de base 113 también genera una base B*, como se indica por la Fórmula 165.

[Fórmula 165]

$$(\vartheta_{i,j})_{i,j=0,\ldots,4n} := \psi \cdot (X^T)^{-1},$$
$$b_i^* := (\vartheta_{i,1},\ldots,\vartheta_{i,N})_{\mathbb{A}} = \sum_{j=0}^{4n} \vartheta_{i,j} a_j \text{ para } i = 0,\ldots,4n,$$
$$\mathbb{B}^* := (b_0^*,\ldots,b_{4n}^*)$$

(S304: Paso de generación de base B^)

Con el dispositivo de procesamiento, una parte de generación de clave 114 genera una base B^*_0, como se indica por la Fórmula 166.

[Fórmula 166]

$$\hat{\mathbb{B}}^* := (b_0^*,\ldots,b_n^*,b_{2n+1}^*,\ldots,b_{3n}^*)$$

(S305: Paso de generación de clave maestra)

Con el dispositivo de procesamiento, la parte de generación de clave 114 fija los parámetros públicos pk := (1^λ, $param_n$, $B^_0$, $\{B_{0,0}, B_{0,j}, B_{i,0,L}, B_{i,j}, B'_{i,j,L}\}_{i=1,4;j=1,\ldots,4;L=1,\ldots,n}$) y la clave secreta maestra sk := B^*. Entonces, la parte de

generación de clave 114 almacena los parámetros públicos pk y la clave secreta maestra sk en una parte de almacenamiento de clave maestra 120.

Señalar que $param_n := (param_V, g_T)$.

Más específicamente, desde S301 hasta S305, el dispositivo de generación de clave 100 ejecuta el algoritmo Setup indicado por la Fórmula 168 usando el algoritmo $G^{(3)}_{ob}$ indicado por la Fórmula 167, para generar los parámetros públicos pk y la clave secreta maestra sk.

[Fórmula 167]

$$\mathcal{G}^{(3)}_{\mathsf{ob}}(1^\lambda, n):$$

$$\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, g, e) \xleftarrow{R} \mathcal{G}_{\mathsf{bpg}}(1^\lambda),\ N := 4n+1,$$

$$\psi \xleftarrow{U} \mathbb{F}_q^\times,\ g_T := e(g,g)^\psi,$$

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

$$\mathsf{param}_n := (\mathsf{param}_{\mathbb{V}}, g_T),\ X \xleftarrow{U} \mathcal{L}'(N, \mathbb{F}_q),\ \text{a partir de entonces,}$$

$$\{\chi_{0,0}, \chi_{0,j}, \chi_{i,0,L}, \mu_{i,j}, \mu'_{i,j,L}\}_{i,j=1,\ldots,4;L=1,\ldots,n}\ \text{denota entradas no cero de } X,$$

$$(\vartheta_{i,j})_{i,j=0,\ldots,4n} := \psi \cdot (X^T)^{-1},$$

$$B_{0,0} := \chi_{0,0} g,\ B_{0,j} := \chi_{0,j} g,\ B_{i,0,L} := \chi_{i,0,L} g,\ B_{i,j} := \mu_{i,j} g,\ B'_{i,j,L} := \mu'_{i,j,L} g$$

$$\text{para } i,j = 1,\ldots,4; L = 1,\ldots,n,$$

$$b_i^* := (\vartheta_{i,1},\ldots,\vartheta_{i,N})_{\mathbb{A}} = \sum_{j=0}^{4n} \vartheta_{i,j} a_j \ \text{ para } i = 0,\ldots,4n,\ \mathbb{B}^* := (b_0^*,\ldots,b_{4n}^*),$$

$$\text{devolver } (\mathsf{param}_n, \{B_{0,0}, B_{0,j}, B_{i,0,L}, B_{i,j}, B'_{i,j,L}\}_{i,j=1,\ldots,4;L=1,\ldots,n}, \mathbb{B}^*).$$

[Fórmula 168]

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

$$(\mathsf{param}_n, \{B_{0,0}, B_{0,j}, B_{i,0,L}, B_{i,j}, B'_{i,j,L}\}_{i,j=1,\ldots,4;L=1,\ldots,n}, \mathbb{B}^*) \xleftarrow{R} \mathcal{G}^{(3)}_{\mathsf{ob}}(1^\lambda, n),$$

$$\hat{\mathbb{B}}^* := (b_0^*,\ldots,b_n^*, b_{2n+1}^*,\ldots,b_{3n}^*),$$

$$\text{devolver } \mathsf{pk} := (1^\lambda, \mathsf{param}_n, \{B_{0,0}, B_{0,j}, B_{i,0,L}, B_{i,j}, B'_{i,j,L}\}_{i=1,4;j=1,\ldots,4;L=1,\ldots,n}),$$

$$\mathsf{sk} := \hat{\mathbb{B}}^*.$$

Señalar que los parámetros públicos se publicitan a través de, por ejemplo, una red, de modo que el dispositivo de cifrado 200 y el dispositivo de descifrado 300 pueden adquirirlos.

El proceso del algoritmo KeyGen se describirán con referencia a la Fig. 15.

El proceso de S311 es el mismo que el proceso de S111 mostrado en la Fig. 7.

(S312: Paso de generación de número aleatorio)

Con el dispositivo de procesamiento, una parte de generación de número aleatorio 141 genera números aleatorios, como se indica por la Fórmula 169.

[Fórmula 169]

$$\delta, \varphi \xleftarrow{U} \mathbb{F}_q$$

(SS313: Paso de generación de elemento k*)

Con el dispositivo de procesamiento, una parte de generación de elemento de clave 142 genera el elemento k*, que es un elemento de una clave de descifrado $sk_{\vec{v}}$, como se indica por la Fórmula 170.

[Fórmula 170]

$$k^* := (\ 1,\ \overbrace{\delta\vec{v}}^{n},\ \overbrace{0^n}^{n},\ \overbrace{\varphi\vec{v}}^{n},\ \overbrace{0^n}^{n}\ )_{\mathbb{B}^*}$$

Como con la Fórmula 135, la Fórmula 170 significa que: 1 se fija como el coeficiente para el vector de base b^*_0 de una base B*; δv_1, …, δv_n se fijan cada uno como el coeficiente para los vectores de base b^*_1, …, b^*_n; 0 se fija como el coeficiente para los vectores de base b^*_{n+1}, …, b^*_{2n}; ϕv_1, …, ϕv_n se fijan cada uno como el coeficiente para los vectores de base b^*_{2n+1}, …, b^*_{3n}; y 0 se fija como el coeficiente para los vectores de base b^*_{3n+1}, …, b^*_{4n}.

(S314: Paso de distribución de clave)

Por ejemplo, con el dispositivo de comunicación, una parte de distribución de clave 150 distribuye la clave de descifrado $sk_{\vec{v}}$, constituida, como elementos, por el elemento k* generado en S313, al dispositivo de descifrado 300 en secreto a través de la red. Como una cuestión de rutina, la clave de descifrado $sk_{\vec{v}}$ se podría distribuir también al dispositivo de descifrado 300 mediante otro método.

Más específicamente, desde S311 hasta S313, el dispositivo de generación de clave 100 ejecuta el algoritmo KeyGen indicado por la Fórmula 171, para generar la clave de descifrado $sk_{\vec{v}}$. Entonces, en S314, el dispositivo de generación de clave 100 distribuye la clave de descifrado $sk_{\vec{v}}$ generada al dispositivo de descifrado 300.

[Fórmula 171]

$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$:

$$\delta, \varphi \xleftarrow{\cup} \mathbb{F}_q,$$

$$k^* := (\ 1,\ \overbrace{\delta\vec{v}}^{n},\ \overbrace{0^n}^{n},\ \overbrace{\varphi\vec{v}}^{n},\ \overbrace{0^n}^{n}\ )_{\mathbb{B}^*},$$

devolver $\mathsf{sk}_{\vec{v}} := k^*$.

Se describirá el dispositivo de cifrado 200.

El proceso del algoritmo Enc se describirá con referencia a la Fig. 16.

Los procesos de S321 a S322 son los mismos que los procesos S121 a S122 mostrados en la Fig. 8.

(S323: Paso de generación de número aleatorio)

Con el dispositivo de procesamiento, una parte de generación de número aleatorio 231 genera números aleatorios, como se indica por la Fórmula 172.

[Fórmula 172]

$$\omega, \eta, \zeta \xleftarrow{\cup} \mathbb{F}_q$$

(S324: Paso de generación de elemento C)

Con el dispositivo de procesamiento, una parte de generación de elemento de cifrado 232 genera elementos C_0, $C_{1,j}$ y $C_{2,j}$, que son elementos de un texto cifrado $ct_{\vec{x}}$, como se indica por la Fórmula 173.

[Fórmula 173]

$$C_0 := \zeta B_{0,0} + \sum_{L=1}^{n} x_L(\omega B_{1,0,L} + \eta B_{4,0,L})\ ,$$

para $j = 1, \ldots, 4$

$$C_{1,j} := \omega B_{1,j} + \eta B_{4,j},$$

$$C_{2,j} := \zeta B_{0,j} + \sum_{L=1}^{n} x_L(\omega B'_{1,j,L} + \eta B'_{4,j,L})$$

El proceso de S325 es el mismo que el proceso de S126 mostrado en la Fig. 8.

(S326: Paso de transmisión de datos)

Por ejemplo, con el dispositivo de comunicación, una parte de transmisión de datos 240 transmite el texto cifrado $ct_{\vec{x}}$, constituido, como elementos, por: el vector $\vec{x}$ introducido en S322, los elementos C_0, $C_{1,j}$ y $C_{2,j}$ generados en S324; y un elemento c_3 generado en S325, al dispositivo de descifrado 300 a través de la red. Como una cuestión de rutina, el texto cifrado $ct_{\vec{x}}$ se podría transmitir también al dispositivo de descifrado 300 mediante otro método.

Más específicamente, desde S321 hasta S325, el dispositivo de cifrado 200 ejecuta el algoritmo Enc indicado por la Fórmula 174, para generar el texto cifrado $ct_{\vec{x}}$. En S326, el dispositivo de cifrado 200 transmite el texto cifrado $ct_{\vec{x}}$ generado al dispositivo de descifrado 300.

[Fórmula 174]

$$\mathsf{Enc}(\mathsf{pk}, m, \vec{x}):$$
$$\omega, \eta, \zeta \xleftarrow{\cup} \mathbb{F}_q,$$
$$C_0 := \zeta B_{0,0} + \sum_{L=1}^{n} x_L(\omega B_{1,0,L} + \eta B_{4,0,L}),$$
$$c_3 := g_T^{\zeta} m,$$
$$C_{1,j} := \omega B_{1,j} + \eta B_{4,j},$$
$$C_{2,j} := \zeta B_{0,j} + \sum_{L=1}^{n} x_L(\omega B'_{1,j,L} + \eta B'_{4,j,L}) \text{ for } j = 1, \ldots, 4,$$
$$\text{devolver } \mathsf{ct}_{\vec{x}} := (\vec{x}, C_0, \{C_{1,j}, C_{2,j}\}_{j=1,\ldots,4}, c_3).$$

Se describirá el dispositivo de descifrado 300.

El proceso del algoritmo Dec se describirá con referencia a la Fig. 17.

Los procesos de S331 a S332 son los mismos que los procesos S131 a S132 mostrados en la Fig. 9.

(S333: Paso de cálculo de valor D^*_j)

Con el dispositivo de procesamiento, una parte de operación de emparejamiento 330 calcula el valor D^*_j, como se indica por la Fórmula 175.

[Fórmula 175]

para j = 1, …, 4

$$D_j^* := \sum_{L=1}^{n-1} x_L K^*_{(j-1)n+L}$$

Señalar que el elemento k^*_1 se analiza sintácticamente como (4n+1) tuplas $(K^*_0, \ldots, K^*_{4n}) \in G^{4n+1}$.

(S334: Paso de operación de emparejamiento)

Con el dispositivo de procesamiento, la parte de operación de emparejamiento 330 ejecuta una operación de emparejamiento, como se indica por la Fórmula 176, para calcular el valor F.

[Fórmula 176]

$$F := e(C_0, K_0^*) \cdot \prod_{j=1}^{4} \left(e(C_{1,j}, D_j^*) \cdot e(C_{2,j}, K_{jn}^*) \right)$$

El proceso de S335 es el mismo que el proceso de S135 mostrado en la Fig. 9.

Más específicamente, desde S331 hasta S335, el dispositivo de descifrado 300 ejecuta el algoritmo Dec indicado por la Fórmula 177, para calcular un mensaje m'.

[Fórmula 177]

$\mathrm{Dec}(\mathrm{pk}, \mathrm{sk}_{\vec{v}} := k^*,\ \mathrm{ct}_{\vec{x}} := (\vec{x}, C_0, \{C_{1,j}, C_{2,j}\}_{j=1,..,4}, c_3))$:

Analizar sintácticamente k^* como una tupla $(4n+1)$ $(K_0^*, \ldots, K_{4n}^*) \in \mathbb{G}^{4n+1}$,

$D_j^* := \sum_{L=1}^{n-1} x_L K_{(j-1)n+L}^*$ para $j = 1, \ldots, 4$,

$F := e(C_0, K_0^*) \cdot \prod_{j=1}^{4} \left(e(C_{1,j}, D_j^*) \cdot e(C_{2,j}, K_{jn}^*) \right)$,

devolver $m' := c_3 / F$.

Señalar que B := (b_0, …, b_{4n}) se especifica por {$B_{0,0}$, $B_{0,j}$, $B_{i,0,L}$, $B_{i,j}$, $B'_{i,j,L}$}$_{i,j=1, \ldots, 4; L=1, \ldots, n}$. También, {$B_{0,0}$, $B_{0,j}$, $B_{i,0,L}$, $B_{i,j}$, $B'_{i,j,L}$}$_{i=1,4; j=1, \ldots, 4; L=1, \ldots, n}$ incluidos en una salida del algortimo Setup se especifica por B^ := (b_0, …, b_n, b_{3n+1}, …, b_{4n}).

El algoritmo Dec se puede describir como el algoritmo Dec' indicado por la Fórmula 178.

[Fórmula 178]

$\mathrm{Dec}'(\mathrm{pk}, \mathrm{sk}_{\vec{v}} := k^*,\ \mathrm{ct}_{\vec{x}} := (\vec{x}, C_0, \{C_{1,j}, C_{2,j}\}_{j=1,..,4}, c_3))$:

$c := (\ C_0,\ \overbrace{x_1 C_{1,1}, \ldots, x_{n-1} C_{1,1}, C_{2,1}}^{n},\ \ \ldots,\ \overbrace{x_1 C_{1,4}, \ldots, x_{n-1} C_{1,4}, C_{2,4}}^{n}\ )$,

es decir, $c = (\ \zeta,\ \overbrace{\omega \vec{x}}^{n},\ \overbrace{0^n}^{n},\ \overbrace{0^n}^{n},\ \overbrace{\eta \vec{x}}^{n}\ )_{\mathbb{B}}$, $F := e(c, k^*)$,

devolver $m' := c_3 / F$.

Como se indica por la Fórmula 179, usando el algoritmo Dec', F = g_T^{ζ} se obtiene si $\vec{x} \cdot \vec{v}$ = 0. Por lo tanto, el mensaje m' (=m) se puede obtener dividiendo $c_3 = g_T^{\zeta} m$ por F.

[Fórmula 179]

$$F = e(c, k) = g_T^{\zeta + \omega \delta \vec{x} \cdot \vec{v}} = g_T^{\zeta} \quad \text{si} \quad \vec{x} \cdot \vec{v} = 0.$$

En el esquema de cifrado de producto interior cero explicado en la Realización 4, el texto cifrado $\mathrm{ct}_{\vec{x}}$ incluye un total de 9 elementos de G, es decir, 1 por elemento C_0 y 8 por elementos $C_{1,j}$ y $C_{2,j}$ para cada entero j de j = 1, …, 4 indicado por la Fórmula 173. También, el texto cifrado $\mathrm{ct}_{\vec{x}}$ incluye 1 elemento de G_T, es decir, 1 por elemento c_3. En fin, el texto cifrado $\mathrm{ct}_{\vec{x}}$ tiene un tamaño constante en n.

También, en el esquema de cifrado de producto interior cero explicado en la Realización 4, el proceso de descifrado (algoritmo Dec) ejecuta un total de solamente 9 operaciones de emparejamiento, es decir, 1 por $e(C_0, K^*_0)$ y 8 por $\Pi_{j=1}^{4}(e(C_{1,j}, D^*_j) \cdot e(C_{2,j}, K^*_{jn}))$ indicado por la Fórmula 176. En fin, el proceso de descifrado requiere solamente un pequeño número de operaciones de emparejamiento.

Realización 5.

En la realización 5, se describirá un esquema de cifrado de producto interior cero que tiene una clave secreta de tamaño constante.

Las configuraciones de un dispositivo de generación de clave 100, un dispositivo de cifrado 200 y un dispositivo de descifrado 300 son respectivamente las mismas que las configuraciones del dispositivo de generación de clave 100, el dispositivo de cifrado 200 y el dispositivo de descifrado 300 mostrados en las Fig. 3, 4 y 5 según la Realización 2.

Las Fig. 18 y 19 son diagramas de flujo que muestran la operación del dispositivo de generación de clave 100 según la Realización 5, en la cual la Fig. 18 es un diagrama de flujo que muestra el proceso del algoritmo Setup según la Realización 5 y la Fig. 19 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen según la Realización 5. La Fig. 20 es un diagrama de flujo que muestra la operación del dispositivo de cifrado 200 según la Realización 5, es decir, un diagrama de flujo que muestra el proceso del algoritmo Enc según la Realización 5. La Fig. 21 es un diagrama de flujo que muestra la operación del dispositivo de descifrado 300 según la Realización 5, es decir, un diagrama de flujo que muestra el proceso del algoritmo Dec según la Realización 5.

En la siguiente descripción, permitamos que un vector $\vec{v}$:= (v_1, …, v_n) a ser introducido mantenga $v_L \neq 0$ para cada entero L de L = 1, …, n-1 y permitamos que un vector $\vec{x}$:= (x_1, …, x_n) a ser introducido mantenga $x_n \neq 0$.

Se describirá el dispositivo de generación de clave 100.

El proceso del algoritmo Setup se describirá con referencia a la Fig. 18.

Los procesos de S401 a S402 son los mismos que los procesos de S301 a S302 mostrados en la Fig. 14.

(S403: Paso de generación de base B)

Con un dispositivo de procesamiento, una parte de generación de base 113 genera las bases $D_{0,0}$, $D_{0,j}$, $D_{i,0,L}$, $D_{i,j}$ y $D'_{i,j,L}$, como se indica por la Fórmula 180, de la misma manera que son las bases $B_{0,0}$, $B_{0,j}$, $B_{i,0,L}$, $B_{i,j}$ y $B'_{i,j,L}$ de la Realización 4.

[Fórmula 180]

para *i, j* = 1, …, 4; L = 1, …, *n*

$$D_{0,0} := \chi_{0,0} g,$$
$$D_{0,j} := \chi_{0,j} g,$$
$$D_{i,0,L} := \chi_{i,0,L} g,$$
$$D_{i,j} := \mu_{i,j} g,$$
$$D'_{i,j,L} := \mu'_{i,j,L} g$$

Con el dispositivo de procesamiento, la parte de generación de base 113 también genera una base D* como se indica por la Fórmula 181, de la misma manera que es la base B* de la Realización 4.

[Fórmula 181]

$$(\vartheta_{i,j})_{i,j=0,\ldots,4n} := \psi \cdot (X^T)^{-1},$$
$$b_i^* := (\vartheta_{i,1},\ldots,\vartheta_{i,N})_{\mathbb{A}} = \sum_{j=0}^{4n} \vartheta_{i,j} a_j \quad \text{para } i = 0,\ldots,4n,$$
$$\mathbb{D}^* := (b_0^*,\ldots,b_{4n}^*)$$

Entonces, la parte de generación de base 113 trata la base D* como una base B. También, para cada uno de los enteros i, j de i, j = 1, …, 4 y cada entero L de L = 1, …, n, la parte de generación de base 113 trata la variable $D_{0,0}$ como una variable $B^*_{0,0}$, la variable $D_{0,j}$ como una variable $B^*_{0,j}$, la variable $D_{i,0,L}$ como una variable $B^*_{i,0,L}$, la variable $D_{i,j}$ como una variable $B^*_{i,j}$ y la variable $D'_{i,j,L}$ como una variable $B'^*_{i,j,L}$.

(S404: Paso de generación de base B^)

Con el dispositivo de procesamiento, una parte de generación de clave 114 genera una base B^, como se indica por la Fórmula 182.

[Fórmula 182]

$$\hat{\mathbb{B}} := (b_0,\ldots,b_n,b_{3n+1},\ldots,b_{4n})$$

(S405: Paso de generación de clave maestra)

Con el dispositivo de procesamiento, la parte de generación de clave 114 fija los parámetros públicos pk := (1^λ, $param_n$, B^) y la clave secreta maestra sk := ($\{B^*_{0,0}, B^*_{0,j}, B^*_{i,0,L}, B^*_{i,j}, B'^*_{i,j,L}\}_{i=1,3;j=1,\ldots,4;L=1,\ldots,n}$). Entonces, la parte de generación de clave 114 almacena los parámetros públicos pk y la clave secreta maestra sk en una parte de almacenamiento de clave maestra 120.

Señalar que $param_n := (param_V, g_T)$.

Más específicamente, desde S401 hasta S405, el dispositivo de generación de clave 100 ejecuta el algoritmo Setup indicado por la Fórmula 184 usando el algoritmo $G^{(4)}_{ob}$ indicado por la Fórmula 183, para generar los parámetros públicos pk y la clave secreta maestra sk. Como se indica por la Fórmula 183, el algoritmo $G^{(4)}_{ob}$ emplea el algoritmo $G^{(3)}_{ob}$ indicado por la Fórmula 167.

[Fórmula 183]

$\mathcal{G}_{ob}^{(4)}(1^{\lambda},n)$:

$(\text{param}_n, \{D_{0,0}, D_{0,j}, D_{i,0,L}, D_{i,j}, D'_{i,j,L}\}_{i,j=1,..,4;L=1,..,n}, \mathbb{D}^*) \xleftarrow{R} \mathcal{G}_{ob}^{(3)}(1^{\lambda},n)$,

$\mathbb{B} := \mathbb{D}^*$, $B^*_{0,0} := D_{0,0}$, $B^*_{0,j} := D_{0,j}$, $B^*_{i,0,L} := D_{i,0,L}$, $B^*_{i,j} := D_{i,j}$, $B'^*_{i,j,L} := D'_{i,j,L}$

para $i,j = 1,..4; L = 1,..,n$,

devolver $(\text{param}_n, \mathbb{B}, \{B^*_{0,0}, B^*_{0,j}, B^*_{i,0,L}, B^*_{i,j}, B'^*_{i,j,L}\}_{i,j=1,..,4;L=1,..,n})$.

[Fórmula 184]

$\text{Setup}(1^{\lambda},n)$:

$(\text{param}_n, \mathbb{B}, \{B^*_{0,0}, B^*_{0,j}, B^*_{i,0,L}, B^*_{i,j}, B'^*_{i,j,L}\}_{i,j=1,..,4;L=1,..,n}) \xleftarrow{R} \mathcal{G}_{ob}^{(4)}(1^{\lambda},n)$,

$\hat{\mathbb{B}} := (b_0,\ldots,b_n,b_{3n+1},\ldots,b_{4n})$,

devolver $\text{pk} := (1^{\lambda}, \text{param}_n, \hat{\mathbb{B}})$,

$\text{sk} := \{B^*_{0,0}, B^*_{0,j}, B^*_{i,0,L}, B^*_{i,j}, B'^*_{i,j,L}\}_{i=1,3;j=1,..,4;L=1,..,n}$.

Señalar que los parámetros públicos se publicitan a través de, por ejemplo, una red, de modo que el dispositivo de cifrado 200 y el dispostivo de descifrado 300 pueden adquirirlos.

El proceso del algoritmo KeyGen se describirá con referencia a la Fig. 19.

Los procesos de S411 a S412 son los mismos que los procesos de S311 a S312 mostrados en la Fig. 15.

(S413: Paso de generación de elemento K*)

Con el dispositivo de procesamiento, una parte de generación de elemento de clave 142 genera los elementos K^*_0, $K^*_{1,j}$ y $K^*_{2,j}$, que son elementos de una clave de descifrado $sk_{\vec{v}}$, como se indica por la Fórmula 185.

[Fórmula 185]

$$K^*_0 := B^*_{0,0} + \sum_{L=1}^{n} v_L(\delta B^*_{1,0,L} + \varphi B^*_{3,0,L}),$$

para $j = 1,\ldots,4$

$$K^*_{1,j} := \delta B^*_{1,j} + \varphi B^*_{3,j},$$

$$K^*_{2,j} := B^*_{0,j} + \sum_{L=1}^{n} v_L(\delta B'^*_{1,j,L} + \varphi B'^*_{3,j,L})$$

(S414: Paso de distribución de clave)

Por ejemplo, con un dispositivo de comunicación, una parte de distribución de clave 150 distribuye la clave de descifrado $sk_{\vec{v}}$, constituida, como elementos, por: el vector $\vec{v}$ introducido en S411; y los elementos K^*_0, $K^*_{1,j}$ y $K^*_{2,j}$ generados en S313, al dispositivo de descifrado 300 en secreto a través de la red. Como una cuestión de rutina, la clave de descifrado $sk_{\vec{v}}$ se podría distribuir también al dispositivo de descifrado 300 mediante otro método.

Más específicamente, desde S411 hasta S413, el dispositivo de generación de clave 100 ejecuta el algoritmo KeyGen indicado por la Fórmula 186, para generar la clave de descifrado $sk_{\vec{v}}$. Entonces, en S414, el dispositivo de generación de clave 100 distribuye la clave de descifrado $sk_{\vec{v}}$ generada al dispositivo de descifrado 300.

[Fórmula 186]

$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$:

$\delta, \varphi \xleftarrow{\cup} \mathbb{F}_q,$

$K_0^* := B_{0,0}^* + \sum_{L=1}^{n} v_L(\delta B_{1,0,L}^* + \varphi B_{3,0,L}^*),$

$K_{1,j}^* := \delta B_{1,j}^* + \varphi B_{3,j}^*, \ K_{2,j}^* := B_{0,j}^* + \sum_{L=1}^{n} v_L(\delta B_{1,j,L}'^* + \varphi B_{3,j,L}'^*)$

para $j = 1, \ldots, 4,$

devolver $\mathsf{sk}_{\vec{v}} := (\vec{v}, K_0^*, \{K_{1,j}^*, K_{2,j}^*\}_{j=1,\ldots,4}).$

Se describirá el dispositivo de cifrado 200.

El proceso del algoritmo Enc se describirá con referencia a la Fig. 20.

Los procesos de S421 a S423 son los mismos que los procesos de S321 a S323 mostrados en la Fig. 16.

(S424: Paso de generación de elemento c)

Con el dispositivo de procesamiento, una parte de generación de elemento de cifrado 232 genera el elemento c, que es un elemento de un texto cifrado $ct_{\vec{x}}$, como se indica por la Fórmula 187.

[Fórmula 187]

$$c := (\ \zeta,\ \overbrace{\omega\vec{x}}^{n},\ \overbrace{0^n}^{n},\ \overbrace{0^n}^{n},\ \overbrace{\eta\vec{x}}^{n}\ )_{\mathbb{B}}$$

Como con la Fórmula 135, la Fórmula 187 significa que: ζ se fija como el coeficiente para un vector de base b_0 de la base B; ω_{x1}, …, ω_{xn}, se fijan cada uno como el coeficiente para los vectores de base b_1, …, b_n; 0 se fija como el coeficiente para los vectores de base b_{n+1}, …, b_{3n}; y ηx_1, …, ηx_n se fijan cada uno como el coeficiente para los vectores de base b_{3n+1}, …, b_{4n}.

El proceso de S425 es el mismo que el proceso de S325 mostrado en la Fig. 16.

(S426: Paso de transmisión de datos)

Por ejemplo, con el dispositivo de comunicación, una parte de transmisión de datos 240 transmite el texto cifrado $ct_{\vec{x}}$, constituido, como elementos, por: el vector $\vec{x}$ introducido en S422; el elemento c generado en S424; y un elemento c_3 generado en S425, al dispositivo de descifrado 300 a través de la red. Como una cuestión de rutina, el texto cifrado $ct_{\vec{x}}$ se podría transmitir también al dispositivo de descifrado 300 mediante otro método.

Más específicamente, desde S421 hasta S425, el dispositivo de cifrado 200 ejecuta el algoritmo Enc indicado por la Fórmula 188, para generar el texto cifrado $ct_{\vec{x}}$. En S426, el dispositivo de cifrado 200 transmite el texto cifrado $ct_{\vec{x}}$ generado al dispositivo de descifrado 300.

[Fórmula 188]

$\mathsf{Enc}(\mathsf{pk}, m, \vec{x})$:

$\omega, \eta, \zeta \xleftarrow{\cup} \mathbb{F}_q,$

$$c := (\ \zeta,\ \overbrace{\omega\vec{x}}^{n},\ \overbrace{0^n}^{n},\ \overbrace{0^n}^{n},\ \overbrace{\eta\vec{x}}^{n}\ )_{\mathbb{B}},$$

$c_3 := g_T^{\zeta} m,$

devolver $\mathsf{ct}_{\vec{x}} := (\vec{x}, c, c_3).$

Se describirá el dispositivo de descifrado 300.

El proceso del algoritmo Dec se describirá con referencia a la Fig. 21.

Los procesos de S431 a S432 son los mismos que los procesos de S331a S332 mostrados en la Fig. 17.

(S433: Paso de cálculo de valor D_j)

Con el dispositivo de procesamiento, una parte de operación de emparejamiento 330 calcula el valor D_j, como se indica por la Fórmula 189.

[Fórmula 189]

para j = 1, …, 4

$$D_j := \sum_{L=1}^{n-1} v_L C_{(j-1)n+L}$$

Señalar que el elemento c se analiza sintácticamente como (4n+1) tuplas $(C^*_0, \ldots, C^*_{4n}) \in G^{4n+1}$.

(S434: Paso de operación de emparejamiento)

Con el dispositivo de procesamiento, la parte de operación de emparejamiento 330 ejecuta una operación de emparejamiento, como se indica por la Fórmula 190, para calcular el valor F.

[Fórmula 190]

$$F := e(C_0, K_0^*) \cdot \prod_{j=1}^{4} \left(e(D_j, K_{1,j}^*) \cdot e(C_{jn}, K_{2,j}^*) \right)$$

El proceso de S435 es el mismo que el proceso de S335 mostrado en la Fig. 17.

Más específicamente, desde S431 hasta S435, el dispositivo de descifrado 300 ejecuta el algoritmo Dec indicado por la Fórmula 191, para calcular un mensaje m'.

[Fórmula 191]

$$\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_{\vec{v}} := (\vec{v}, K_0^*, \{K_{1,j}^*, K_{2,j}^*\}_{j=1,\ldots,4}),\ \mathsf{ct}_{\vec{x}} := (\vec{x}, c, c_3)):$$

Analizar sintácticamente c como una tupla $(4n+1)$ $(C_0, \ldots, C_{4n}) \in \mathbb{G}_r^{4n+1}$,

$D_j := \sum_{L=1}^{n-1} v_L C_{(j-1)n+L}$ para $j = 1, \ldots, 4$,

$F := e(C_0, K_0^*) \cdot \prod_{j=1}^{4} \left(e(D_j, K_{1,j}^*) \cdot e(C_{jn}, K_{2,j}^*) \right)$,

devolver $m' := c_3 / F$.

Señalar que B* := (b^*_0, …, b^*_{4n}) se especifica por $\{B^*_{0,0}, B^*_{0,j}, B^*_{i,0,L}, B^*_{i,j}, B'^*_{i,j,L}\}_{i=1,\ldots,4;L=1,\ldots,n}$. También, $\{B^*_{0,0}, B^*_{0,j}, B^*_{i,0,L}, B^*_{i,j}, B'^*_{i,j,L}\}_{i=1,3;j=1,\ldots,4;L=1,\ldots,n}$ incluidos en una salida del algortimo Setup se especifica por B^* := (b^*_0, …, b^*_n, b^*_{2n+1}, …, b^*_{3n}).

El algoritmo Dec se puede describir como el algoritmo Dec' indicado por la Fórmula 192.

[Fórmula 192]

$$\mathsf{Dec}'(\mathsf{pk}, \mathsf{sk}_{\vec{v}} := (\vec{v}, K_0^*, \{K_{1,j}^*, K_{2,j}^*\}_{j=1,\ldots,4}),\ \mathsf{ct}_{\vec{x}} := (\vec{x}, c, c_3)):$$

$$k^* := (K_0^*, \overbrace{v_1 K_{1,1}^*, \ldots, v_{n-1} K_{1,1}^*, K_{2,1}^*}^{n}, \quad \ldots, \overbrace{v_1 K_{1,4}^*, \ldots, v_{n-1} K_{1,4}^*, K_{2,4}^*}^{n}),$$

es decir, $k^* = (1, \overbrace{\delta \vec{v}}^{n}, \overbrace{0^n}^{n}, \overbrace{\varphi \vec{v}}^{n}, \overbrace{,0^n}^{n})_{\mathbb{B}^*}$, $F := e(c, k^*)$,

devolver $m' := c_3 / F$.

En el esquema de cifrado de producto interior cero explicado en la Realización 5, la clave de descifrado $sk_{v\rightarrow}$ incluye un total de 9 elementos de G, es decir, 1 por el elemento K^*_0 y 8 por los elementos $K^*_{1,j}$ y $K^*_{2,j}$ para cada entero j de j = 1, …, 4 indicado por la Fórmula 185. En fin, la clave de descifrado $sk_{v\rightarrow}$ tiene un tamaño constante en n.

También, en el esquema de cifrado de producto interior cero explicado en la Realización 5, el proceso de descifrado (algoritmo Dec) ejecuta un total de solamente 9 operaciones de emparejamiento, es decir, 1 por $e(C_0, K^*_0)$ y 8 por $\Pi_{j=1}^{4}(e(D_j, K^*_{1,j}) \cdot e(C_{jn}, K^*_{2,j}))$ indicado por la Fórmula 190. En fin, el proceso de descifrado requiere solamente un pequeño número de operaciones de emparejamiento.

Las realizaciones anteriores emplean la transformación lineal X mostrada en (b) de la Fig. 2. No obstante, la transformación lineal X no se limita a la mostrada en (b) de la Fig. 2. Por ejemplo, en (b) de la Fig. 2, los cuadrados sombreados pueden tener valores diferentes unos de otros. En (b) de la Fig. 2, todos los componentes en una columna N tienen valores aleatorios distintos del valor constante 0. No obstante, alternativamente, en lugar de la columna N, todos los componentes en al menos una de las otras columnas podría tener también valores aleatorios distintos del valor constante 0.

Más generalmente, la transformación lineal X es suficiente si es una matriz dispersa en la cual cada fila y cada columna tienen al menos un valor que es distinto del valor constante 0. Además, en caso de una matriz de n filas, n columnas, la transformación lineal X preferiblemente tiene al menos n valores diferentes como valores distintos del valor constante 0. Además, la transformación lineal X es preferiblemente de manera que todos los componentes en al menos una columna tienen valores distintos del valor constante 0. Además, la transformación lineal X es preferiblemente X es preferiblemente de manera que sus componentes diagonales y todos los componentes en al menos una columna tienen valores distintos del valor constante 0. Además, la transformación lineal X es preferiblemente de manera que sus componentes diagonales tienen el mismo valor excepto para las columnas en las cuales todos los componentes tienen valores distintos del valor constante 0.

Incluso con tal transformación lineal X, los tamaños de los parámetros públicos y la clave secreta son menores que en un caso donde se usa la transformación lineal X convencional. También, se acorta el tiempo tomado por el proceso de generación de la clave de usuario y el proceso de cifrado.

Dependiendo del tipo de transformación lineal X, no se puede disminuir el número de operaciones de emparejamiento.

En las realizaciones anteriores, el espacio de vector consta de cuatro subespacios ortogonales, es decir, parte de codificación, parte oculta, parte de aleatoriedad de clave secreta y parte de aleatoriedad de texto cifrado. A fin de hacer frente a esto, la transformación lineal X se constituye usando una matriz de n filas, n columnas $X_{i,j}$ (i, j = 1, …, 4), como se indica por la Fórmula 124. Esta estructura de la transformación lineal X descansa en una premisa que los subespacios de la parte oculta, parte de aleatoriedad de clave secreta y parte de aleatoriedad de texto cifrado son n dimensionales, como con el subespacio de la parte de codificación.

Alternativamente, los subespacios de la parte oculta, la parte de aleatoriedad de clave secreta y la parte de aleatoriedad de texto cifrado no necesitan ser n dimensionales a diferencia del subespacio de la parte de codificación. Por ejemplo, el subespacio de la parte oculta puede ser (n x u) dimensional, el subespacio de la parte de aleatoriedad de clave secreta puede ser (n x w) dimensional y el subespacio de la parte de aleatoriedad de texto cifrado puede ser (n x z) dimensional (u, w y z son cada uno un entero de 0 o más). En este caso, la transformación lineal X se puede constituir usando una matriz de n filas, n columnas $X_{i,j}$ (i, j = 1, …, 1 + u + w + z), como se indica por la Fórmula 193.

[Fórmula 193]

$$X := \begin{pmatrix} X_{1,1} & \cdots & X_{1,1+u+w+z} \\ \vdots & & \vdots \\ X_{1+u+w+z,1} & \cdots & X_{1+u+w+z,1+u+w+z} \end{pmatrix}$$

La revocación basada en ID (Identidad) (IBR) y el cifrado de difusión basado en ID (Identidad) (IBBE) constituyen una clase de cifrado funcional (ver las Literaturas No de Patente 1, 5, 6, 8, 19 y 12).

Según la revocación basada en ID, un texto cifrado se cifra para un conjunto de identidades S = (ID_1, …, ID_n). El texto cifrado se descifra por una clave secreta asociada con el ID que no satisface ID $\in$ S. Más específicamente, el descifrado requiere $R^{IBR}(ID, S) = 1$ si y sólo si ID $\in$ S no se establece.

Según el cifrado de difusión basado en ID, un texto cifrado se cifra para un conjunto de identidades S = (ID_1, …, ID_n). El texto cifrado se descifra mediante una clave secreta asociada con la ID que satisface ID $\in$ S. Más específicamente, el descifrado requiere $R^{IBBE}(ID, S) = 1$ si y sólo si ID $\in$ S se establece.

Supongamos $S(X) = \Sigma_{i=0}^{n} v_i X^i := \Pi_{i=1}^{n}(X - ID_i)$ donde S := {ID_1, …, ID_n}. También, supongamos un vector $\vec{v} := (v_0, v_1, \ldots, v_n)$ y un vector $\vec{x} := (1, ID, \ldots, ID^n)$.

Entonces, el esquema de cifrado de producto interior no cero explicado en las Realizaciones 2 y 3 se puede considerar como un esquema de revocación basado en ID y el esquema de cifrado de producto interior cero explicado en las Realizaciones 4 y 5 se pueden considerar como un esquema de cifrado de difusión basado en ID.

Más específicamente, los esquemas de cifrado de producto interior explicados en las realizaciones anteriores pueden implementar un esquema de revocación basado en ID y un esquema de cifrado de difusión basado en ID.

En este caso también, un texto cifrado o una clave de descifrado pueden tener un tamaño constante en n, de modo que el descifrado se puede dirigir por un número pequeño de las operaciones de emparejamiento.

Además, de los esquemas de cifrado prácticos explicados en las Realizaciones 2 a 4, si la transformación lineal X descrita anteriormente se aplica a los esquemas de cifrado explicados en las Literaturas No de Patente 13, 15, 16, 17 y similares, los tamaños de los parámetros públicos y la clave secreta disminuyen. También, se acorta el tiempo que lleva el proceso de generación de la clave de usuario y el proceso de cifrado.

La Fig. 22 muestra la comparación de los esquemas de cifrado de producto interior no cero y los esquemas de cifrado de producto interior cero explicados en las Realizaciones 2 a 4 con el esquema de cifrado de producto interior no cero y el esquema de cifrado de producto interior cero descritos en la Literatura No de Patente 2.

En la Fig. 22, $|G|$, $|G_T|$, $|F_q|$, P y M representan el tamaño de G, tamaño de G_T, tamaño de F_q, operación de emparejamiento y multiplicación escalar en G, respectivamente. También, CT, SK, IP y DBDH representan el texto cifrado, la clave secreta (clave de descifrado), el producto interior y Diffie-Hellman bilineal decisional, respectivamente.

Realización 6.

En las anteriores realizaciones, se ha descrito el método de implementación del proceso criptográfico en los espacios de vector dual. En la Realización 6, se describirá un método de implementación de un proceso criptográfico en grupos aditivos duales.

Más específicamente, en las realizaciones anteriores, el proceso criptográfico se implementa en el grupo cíclico del primo de orden q. Cuando un anillo R se expresa usando un número compuesto M como se indica por la Fórmula 194, el proceso criptográfico descrito en las realizaciones anteriores también se puede aplicar a un grupo aditivo que tiene un anillo R como coeficiente.

[Fórmula 194]

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

donde

$\mathbb{Z}$: un entero; y

M : un número compuesto

Si F_q en el algoritmo explicado en las realizaciones anteriores se cambia a R, se puede implementar el proceso criptográfico en un grupo aditivo dual.

La configuración hardware de un sistema de procesamiento criptográfico 10 (un dispositivo de generación de clave 100, un dispositivo de cifrado 200 y un dispositivo de descifrado 300) se describirá en una realización.

La Fig. 23 es un diagrama que muestra un ejemplo de la configuración hardware de cada uno del dispositivo de generación de clave 100, el dispositivo de cifrado 200, el dispositivo de descifrado 300 y un dispositivo de delegación de clave 400.

Como se muestra en la Fig. 23, cada uno del dispositivo de generación de clave 100, dispositivo de cifrado 200, dispositivo de descifrado 300 y el dispositivo de delegación de clave 400 incluye una CPU 911 (Unidad Central de Proceso; también conocida como dispositivo central de proceso, dispositivo de procesamiento, dispositivo de computación, microprocesador, microordenador o procesador) que ejecuta programas. La CPU 911 se conecta a una ROM 913, una RAM 914, un LCD 901 (Visualizador de Cristal Líquido), un teclado 902 (K/B), una placa de comunicación 915 y un dispositivo de disco magnético 920 a través de un bus 912 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 del dispositivo de almacenamiento (memoria). El teclado 902 y la placa de comunicación 915 son ejemplos de un dispositivo de entrada. La placa de comunicación 915 es un ejemplo de un dispositivo de comunicación. Además, 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. La CPU 911, el sistema operativo 921 y el sistema de ventanas 922 ejecutan cada programa de los programas 923.

Los programas 923 almacenan software y programas que ejecutan las funciones descritas como la “parte de generación de clave maestra 110”, la “parte de almacenamiento de clave maestra 120”, la “parte de entrada de información 130”, la “parte de generación de clave de descifrado 140”, la “parte de distribución de clave 150”, la “parte de adquisición de parámetro público 210”, la “parte de entrada de información 220”, la “parte de generación de texto cifrado 230”, la “parte de transmisión de datos 240”, la “parte de adquisición de clave de descifrado 310”, la “parte de recepción de datos 320”, la “parte de operación de emparejamiento 330”, la “parte de cálculo de mensaje 340” y similares en la descripción anterior. 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 los “parámetros públicos pk”, la “clave secreta maestra sk”, las “clave de descifrado $sk_{v\rightarrow}$”, el “texto cifrado $ct_{x\rightarrow}$” y similares de la explicación anterior, 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, los datos, los valores de señal, los valores de variables y los parámetros almacenados en el medio de grabación tal como el disco o la memoria se leen para la memoria principal o memoria caché por la CPU 911 a través de un circuito de lectura/escritura y se usan para las operaciones de la CPU 911 tales como extracción, búsqueda, revisión, comparación, computación, cálculo, proceso, salida, impresión y visualización. La información, los datos, los valores de señal, los valores de variable y los parámetros se almacenan temporalmente en la memoria principal, memoria caché o memoria de almacenador temporal durante las operaciones de la CPU 911 que incluyen extracción, búsqueda, revisión, comparación, computación, cálculo, proceso, salida, impresión y visualización.

Las flechas de los diagramas de flujo en la descripción anterior indican principalmente la entrada/salida de datos y señales. Los datos y valores de señal se graban 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; u ondas eléctricas.

La “parte” en la explicación anterior puede ser un “circuito”, “dispositivo”, “equipo”, “medios” o “función”; o un “paso”, “procedimiento” o “proceso”. El “dispositivo” puede ser “circuito”, “equipo”, “medios” o “función”; o un “paso”, “procedimiento” o “proceso”. El “proceso” puede ser un “paso”. Es decir, la “parte” se puede implementar como microprograma almacenado en la ROM 913. Alternativamente, la “parte” se puede implementar solamente por software; solamente por hardware tal como un elemento, un dispositivo, un sustrato o una línea de cableado; mediante una combinación de software y hardware; o además por una combinación de software, hardware y microprograma. El microprograma y software se almacenan, como un programa, en el medio de grabación tal como la ROM 913. El programa se lee por la CPU 911 y se ejecuta por la CPU 911. Es decir, el programa hace al ordenador o similar funcionar como una “parte” descrita anteriormente. Alternativamente, el programa hace al ordenador o similar ejecutar el procedimiento y método de la “parte” descrita anteriormente.

Lista de signos de referencia

10: sistema de procesamiento criptográfico; 100: dispositivo de generación de clave; 110: parte de generación de clave maestra; 111: parte de generación de espacio; 112: parte de generación de matriz; 113: parte de generación de base; 114: parte de generación de clave; 120: parte de almacenamiento de clave maestra; 130: parte de entrada de información; 140: parte de generación de clave de descifrado; 141: parte de generación de número aleatorio; 142: parte de generación de elemento de clave; parte de distribución de clave; 200: dispositivo de cifrado; 210: parte de adquisición de parámetro público; 220: parte de entrada de información; 230: parte de generación de texto cifrado; 231: parte de generación de número aleatorio; 232: parte de generación de elemento de cifrado; 240: parte de transmisión de datos; 300: dispositivo de descifrado; 310: parte de adquisición de clave de descifrado; 320: parte de recepción de datos; 330: parte de operación de emparejamiento; 340: parte de cálculo de mensaje.

REIVINDICACIONES

1. Un sistema de procesamiento criptográfico (10) configurado para utilizar una base B y una base B* generadas transformando una base A predeterminada usando una matriz en la cual cada fila y cada columna tienen al menos un valor que es distinto del valor constante 0, para dirigir un proceso criptográfico, el sistema de procesamiento criptográfico que comprende:

un dispositivo de cifrado (200) que genera un vector en la base B, el vector que se integra con información predeterminada, como un vector de cifrado; y

un dispositivo de descifrado (300) que, tratando un vector predeterminado en la base B* como un vector de clave, dirige una operación de emparejamiento para el vector de clave y el vector de cifrado que se genera por el dispositivo de cifrado, para descifrar el vector de cifrado y extrae información en la información predeterminada,

en donde la matriz es una matriz de n filas, n columnas (n es un entero de 2 o más) y tiene al menos n valores diferentes como un valor distinto del valor constante 0,

en donde la matriz es de manera que todos los componentes en al menos una columna tienen valores distintos del valor constante 0 y

en donde la matriz es de manera que solamente componentes diagonales de la misma y todos los componentes en una columna tienen valores distintos del valor constante 0.

2. El sistema de procesamiento criptográfico según la reivindicación 1,

en donde la matriz es de manera que los componentes diagonales tienen el mismo valor excepto para la columna en la que todos los componentes tienen valores distintos del valor constante 0.

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

en donde la matriz es una matriz indicada por la Fórmula 1:

[Fórmula 1]

$$\begin{pmatrix} \mu & & \mu'_1 \\ & \ddots & \vdots \\ & \mu & \mu'_{n-1} \\ & & \mu'_n \end{pmatrix}$$

en donde $\mu, \mu'_1, \ldots, \mu'_n$ son cada uno un valor predeterminado distinto del valor constante 0 y las partes en blanco representan el valor constante 0.

4. El sistema de procesamiento criptográfico según la reivindicación 1,

que utiliza una base B y una base B* generadas a partir de una base A como se indica por la Fórmula 3 usando una transformación lineal X de N filas, N columnas (N es un entero de n o más) que constituye una matriz en la que un valor de la 1ª fila, 1ª columna a un valor de la fila de orden n, la columna de orden n son como se indica por la Fórmula 2,

en donde el dispositivo de cifrado genera un vector que incluye la Fórmula 4, como el vector de cifrado y

en donde el dispositivo de descifrado, tratando un vector k* que incluye la Fórmula 5, como el vector de clave, descifra el vector de cifrado:

[Fórmula 2]

$$\begin{pmatrix} \mu_1 & & \mu'_1 \\ & \ddots & \vdots \\ & \mu_{n-1} & \mu'_{n-1} \\ & & \mu'_n \end{pmatrix}$$

en donde $\mu_1, \ldots, \mu_{n-1}, \mu'_1, \ldots, \mu'_n$ son cada uno un valor predeterminado distinto del valor constante 0 y las partes en blanco representan el valor constante 0,

[Fórmula 3]

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

$$\vartheta_{i,j} := \psi \cdot (X^T)^{-1},$$

$$b_i^* := \sum_{j=1}^{N} \vartheta_{i,j} a_j \quad \text{para } i = 1,\ldots,N, \; \mathrm{B}^* := (b_1^*,\ldots,b_N^*)$$

donde $\chi_{i,j}$ es un componente de la fila de orden i, columna de orden j de la transformación lineal X, Ψ es un valor predeterminado y a_j es un vector de base de orden j de la base A,

[Fórmula 4]

$$\sum_{i=1}^{n} \omega x_i b_i$$

donde ω y $x_1, \ldots, x_n$ son cada uno un valor predeterminado y

[Fórmula 5]

$$\sum_{i=1}^{n} \delta v_i b_i^*$$

donde δ y $v_1, \ldots, v_n$ son cada uno un valor predeterminado.

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

en donde la matriz indicada por la Fórmula 2 tiene valores μ_i (i = 1, …, n-1) que son el mismo valor μ,

en donde el dispositivo de cifrado genera un vector que incluye un vector C_1 y un vector C_2, como el vector de cifrado, el vector C_1 que incluye la Fórmula 6, el vector C_2 que incluye la Fórmula 7 y

en donde el dispositivo de cifrado calcula D* indicado por la Fórmula 8, para dirigir la operación de emparejamiento indicada por la Fórmula 9:

[Fórmula 6]

$$C_1 := \omega B_1$$

[Fórmula 7]

$$C_2 := \sum_{i=1}^{n} x_i (\omega B_i')$$

[Fórmula 8]

$$D^* := \sum_{i=1}^{n-1} ((\vec{x} \cdot \vec{v})^{-1} x_i) K_i^*$$

donde $K^*_1, \ldots, K^*_{n-1}$ son cada uno un componente de vectores de base $b^*_1, \ldots, b^*_{n-1}$ para un caso donde el vector k* se descompone en componentes para los vectores de base respectivos,

[Fórmula 9]

$$e(C_1, D^*) \cdot e(C_2, K_n^*)$$

donde K^*_n es un componente de un vector de base b^*_n para un caso donde el vector k* se descompone en componentes para los vectores de base respectivos.

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

en donde la matriz indicada por la Fórmula 2 tiene valores μ_i (i = 1, …, n-1) que son el mismo valor μ,

en donde el dispositivo de cifrado genera un vector que incluye un vector C_1 y un vector C_2, como el vector de cifrado, el vector C_1 que incluye la Fórmula 10, el vector C_2 que incluye la Fórmula 11 y

en donde el dispositivo de cifrado calcula D* indicado por la Fórmula 12, para dirigir la operación de emparejamiento indicada por la Fórmula 13:

[Fórmula 10]

$$C_1 := \omega B_1$$

[Fórmula 11]

$$C_2 := \sum_{i=1}^{n} x_i(\omega B_i')$$

[Fórmula 12]

$$D^* := \sum_{i=1}^{n-1} x_i K_i^*$$

donde K^*_1, …, K^*_{n-1} son cada uno un componente de los vectores de base b^*_1, …, b^*_{n-1} para un caso donde el vector k* se descompone en componentes para los vectores de base respectivos y

[Fórmula 13]

$$e(C_1, D^*) \cdot e(C_2, K_n^*)$$

donde K^*_n es un componente de un vector de base b^*_n para un caso donde el vector k* se descompone en componentes para los vectores de base respectivos.

7. El sistema de procesamiento criptográfico según la reivindicación 1,

que utiliza una base B y una base B* generadas a partir de la base A como se indica por la Fórmula 15 usando una transformación lineal X de N filas, N columnas (N es un entero de n o más) que constituye una matriz en la que un valor de la 1ª fila, 1ª columna a un valor de la fila de orden n, columna de orden n son como se indica por la Fórmula 14,

en donde el dispositivo de cifrado genera un vector c que incluye la Fórmula 16, como el vector de cifrado y

en donde el dispositivo de descifrado, tratando un vector que incluye la Fórmula 17, como el vector de clave, descifra el vector de cifrado:

[Fórmula 14]

$$\begin{pmatrix} \mu_1 & & \mu_1' \\ & \ddots & \vdots \\ & \mu_{n-1} & \mu_{n-1}' \\ & & \mu_n' \end{pmatrix}$$

en donde μ_1, …, μ_{n-1}, μ'_1, …, μ'_n son cada uno un valor predeterminado distinto del valor constante 0 y las partes en blanco representan el valor constante 0,

[Fórmula 15]

$$b_i^* := \sum_{j=1}^{N} \chi_{i,j} a_j \quad \text{para } i = 1,\ldots,N, \quad \mathrm{B}^* := (b_1^*,\ldots,b_N^*),$$

$$\vartheta_{i,j} := \psi \cdot (X^T)^{-1},$$

$$b_i := \sum_{j=1}^{N} \vartheta_{i,j} a_j \quad \text{para } i = 1,\ldots,N, \quad \mathrm{B} := (b_1,\ldots,b_N)$$

donde $\chi_{i,j}$ es un componente de la fila de orden i, columna de orden j de la transformación lineal X, Ψ es un valor predeterminado y a_j es un vector de base de orden j de la base A,

[Fórmula 16]

$$\sum_{i=1}^{n} \omega x_i b_i$$

donde ω y $x_1, \ldots, x_n$ son cada uno un valor predeterminado y

[Fórmula 17]

$$\sum_{i=1}^{n} \delta v_i b_i^*$$

donde δ y $v_1, \ldots, v_n$ son cada uno un valor predeterminado.

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

en donde la matriz indicada por la Fórmula 14 tiene valores μ_i (i = 1, …, n-1) que son el mismo valor μ y

en donde el dispositivo de descifrado, tratando un vector que incluye un vector K^*_1 y un vector K^*_2, como el vector de clave, el vector K^*_1 que incluye la Fórmula 18, el vector K^*_2 que incluye la Fórmula 19, calcula D* indicado por la Fórmula 20, para dirigir una operación de emparejamiento indicada por la Fórmula 21:

[Fórmula 18]

$$K_1^* := \delta B_1$$

[Fórmula 19]

$$K_2^* := \sum_{i=1}^{n} v_i (\delta B_i')$$

[Fórmula 20]

$$D := \sum_{i=1}^{n-1} ((\vec{x} \cdot \vec{v})^{-1} v_i) C_i$$

donde $C_1, \ldots, C_{n-1}$ son cada uno un componente de los vectores de base $b_1, \ldots, b_{n-1}$ para un caso donde el vector c se descompone en componentes para los vectores de base respectivos y

[Fórmula 21]

$$e(D, K_1^*) \cdot e(C_n, K_2^*)$$

donde C_n es un componente de un vector de base b_n para un caso donde el vector c se descompone en componentes para los vectores de base respectivos.

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

en donde la matriz dispersa indicada por la Fórmula 14 tiene valores μ_i (i = 1, …, n-1) que son el mismo valor μ y

en donde el dispositivo de descifrado, tratando un vector que incluye un vector K^*_1 y un vector K^*_2, como el vector de clave, el vector K^*_1 que incluye la Fórmula 22, el vector K^*_2 que incluye la Fórmula 23, calcula D* indicado por la Fórmula 24, para dirigir una operación de emparejamiento indicada por la Fórmula 25:

[Fórmula 22]

$$K_1^* := \delta B_1$$

[Fórmula 23]

$$K_2^* := \sum_{i=1}^{n} v_i (\delta B_i')$$

[Fórmula 24]

$$D := \sum_{i=1}^{n-1} v_i C_i$$

donde $C_1, \ldots, C_{n-1}$ son cada uno un componente de los vectores de base $b_1, \ldots, b_{n-1}$ para un caso donde el vector c se descompone en componentes para los vectores de base respectivos y

[Fórmula 25]

$$e(D, K_1^*) \cdot e(C_n, K_2^*)$$

donde C_n es un componente del vector de base b_n para un caso donde el vector c se descompone en componentes para los vectores de base respectivos.

10. Un método de procesamiento criptográfico configurado para utilizar una base B y una base B* generadas transformando una base A predeterminada usando una matriz en la cual cada fila y cada columna tienen al menos un valor distinto de 0, en el que la matriz es una matriz de n filas, n columnas (n es un entero de 2 o más) y tiene al menos n valores diferentes como un valor distinto del valor constante 0 y en el que solamente los componentes diagonales y todos los componentes en una columna tienen valores distintos del valor constante 0, para dirigir un proceso criptográfico, el método de procesamiento criptográfico que comprende:

con un dispositivo de cifrado (200), generar un vector en la base B, el vector que se integra con información predeterminada, como un vector de cifrado; y

con un dispositivo de descifrado (300), tratando un vector predeterminado en la base B* como un vector de clave, dirigir una operación de emparejamiento para el vector de clave y el vector de cifrado que se genera por el dispositivo de cifrado, para descifrar el vector de cifrado y extraer información en la información predeterminada.

11. Un programa de procesamiento criptográfico configurado para utilizar una base B y una base B* generadas transformando una base A predeterminada usando una matriz en la cual cada fila y cada columna tienen al menos un valor distinto de 0, en el que la matriz es una matriz de n filas, n columnas (n es un entero de 2 o más) y tiene al menos n valores diferentes como un valor distinto del valor constante 0 y en el que solamente los componentes diagonales y todos los componentes en una columna tienen valores distintos del valor constante 0, para dirigir un proceso criptográfico, el programa de procesamiento criptográfico que comprende:

un proceso de cifrado de generación de un vector en la base B, el vector que se integra con información predeterminada, como un vector de cifrado; y

un proceso de descifrado de, tratando un vector predeterminado en la base B* como un vector de clave, dirigir una operación de emparejamiento para el vector de clave y el vector de cifrado que se genera por el proceso de cifrado, para descifrar el vector de cifrado y extraer información en la información predeterminada.

12. Un dispositivo de generación de clave (100) para generar un parámetro público y una clave secreta en cifrado de clave pública, que comprende:

una parte de generación de matriz (112) que genera una transformación lineal X que incluye una matriz en la que cada fila y cada columna tienen al menos un valor distinto de 0, en el que la matriz es una matriz de n filas, n columnas (n es un entero de 2 o más) y tiene al menos n valores diferentes como un valor distinto del valor constante 0 y en el que solamente los componentes diagonales y todos los componentes en una columna tienen valores distintos del valor constante 0;

una parte de generación de base (113) que genera una base D y una base D* a partir de una base A predeterminada como se indica por la Fórmula 26 usando la transformación lineal X generada por la parte de generación de matriz; y

una parte de generación de clave maestra (110) que, tratando al menos parte de los vectores de base de una de la base D y la base D* generadas por la parte de generación de base, como un parámetro público, genera al menos parte de los vectores de base de una restante de la base D y la base D*, como una clave secreta:

[Fórmula 26]

$$b_i := \sum_{j=1}^{N} \chi_{i,j} a_j \quad \text{para } i = 1, \ldots, N, \quad \mathbf{D} := (b_1, \ldots, b_N),$$

$$\vartheta_{i,j} := \psi \cdot (X^T)^{-1},$$

$$b_i^* := \sum_{j=1}^{N} \vartheta_{i,j} a_j \quad \text{para } i = 1, \ldots, N, \quad \mathrm{D}^* := (b_1^*, \ldots, b_N^*)$$

donde $\chi_{i,j}$ es un componente de la fila de orden i, columna de orden j de la transformación lineal X, Ψ es un valor predeterminado y a_j es un vector de base de orden j de la base A.

Fig. 1

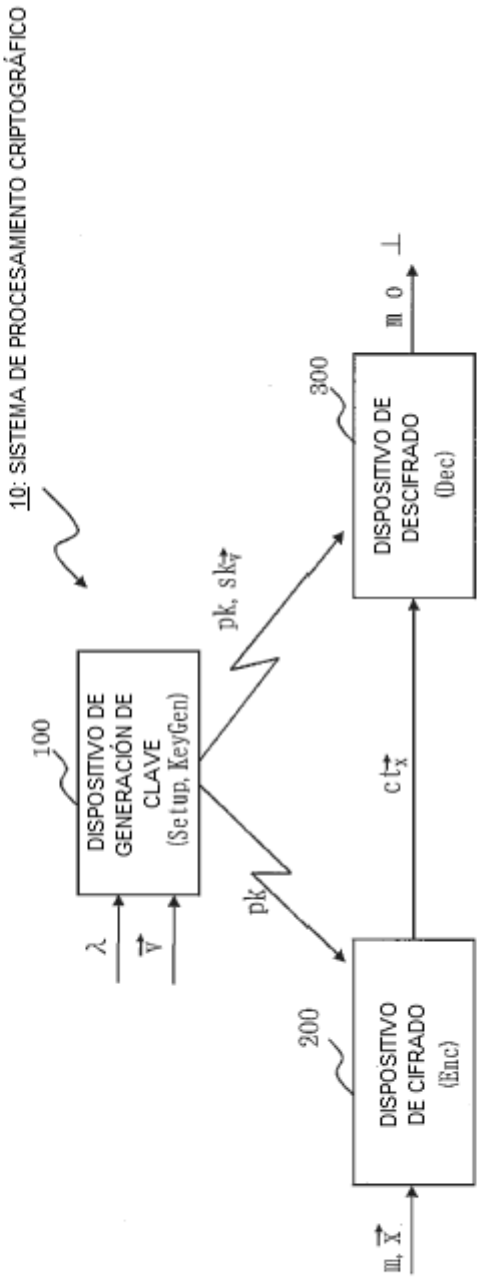

10: SISTEMA DE PROCESAMIENTO CRIPTOGRÁFICO
DISPOSITIVO DE GENERACIÓN DE CLAVE (Setup, KeyGen)
100
DISPOSITIVO DE CIFRADO (Enc)
200
DISPOSITIVO DE DESCIFRADO (Dec)
300
λ
pk, sk
pk
ct
m, x
m 0 ⊥

Fig. 2

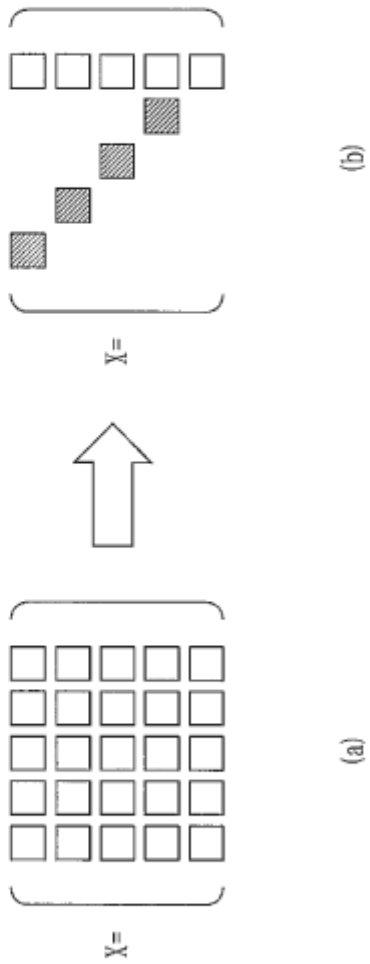


Fig. 3

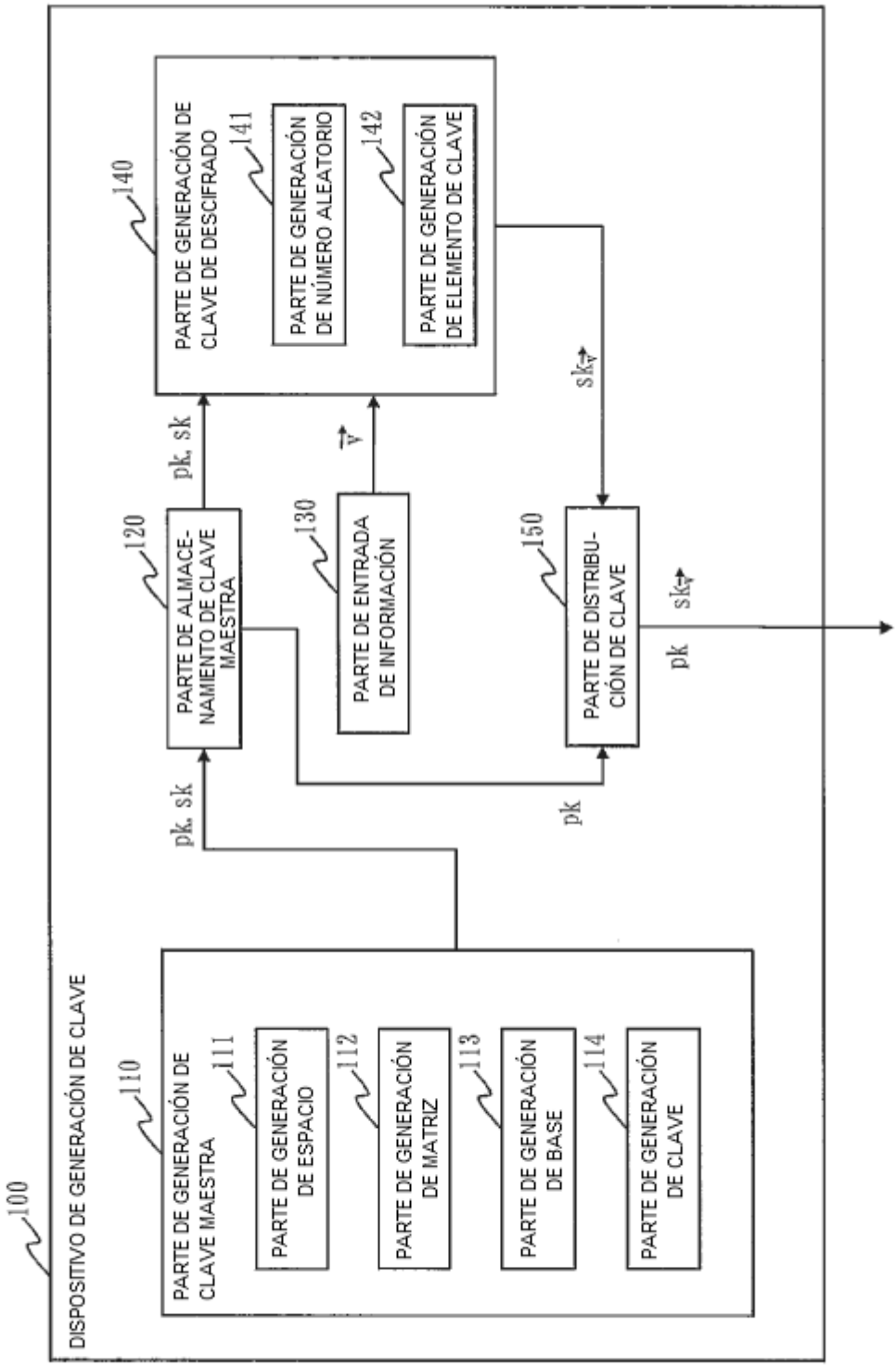

100
DISPOSITIVO DE GENERACIÓN DE CLAVE
110
PARTE DE GENERACIÓN DE CLAVE MAESTRA
111
PARTE DE GENERACIÓN DE ESPACIO
112
PARTE DE GENERACIÓN DE MATRIZ
113
PARTE DE GENERACIÓN DE BASE
114
PARTE DE GENERACIÓN DE CLAVE
120
PARTE DE ALMACENAMIENTO DE CLAVE MAESTRA
130
PARTE DE ENTRADA DE INFORMACIÓN
140
PARTE DE GENERACIÓN DE CLAVE DE DESCIFRADO
141
PARTE DE GENERACIÓN DE NÚMERO ALEATORIO
142
PARTE DE GENERACIÓN DE ELEMENTO DE CLAVE
150
PARTE DE DISTRIBUCIÓN DE CLAVE
pk, sk
pk, sk
pk
pk
sk

Fig. 4

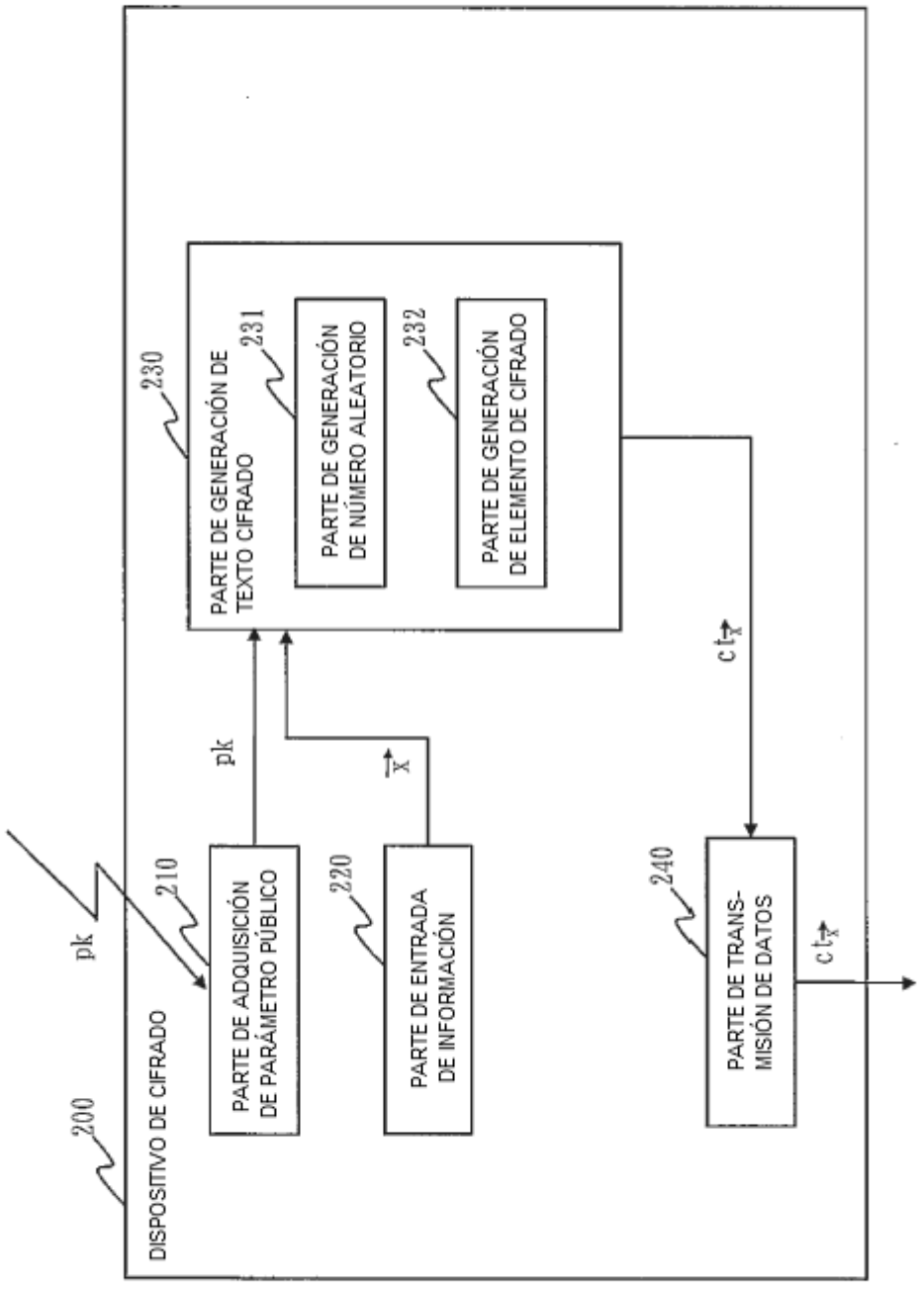

200
DISPOSITIVO DE CIFRADO
pk
210
PARTE DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
pk
220
PARTE DE ENTRADA DE INFORMACIÓN
x
230
PARTE DE GENERACIÓN DE TEXTO CIFRADO
231
PARTE DE GENERACIÓN DE NÚMERO ALEATORIO
232
PARTE DE GENERACIÓN DE ELEMENTO DE CIFRADO
240
PARTE DE TRANSMISIÓN DE DATOS
ct
ct

Fig. 5

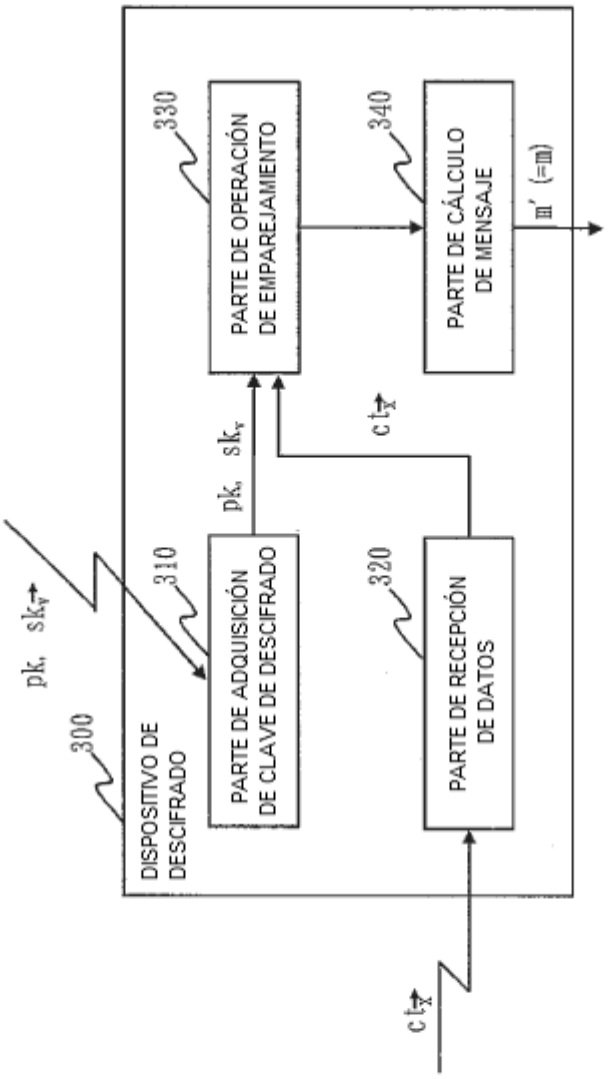

pk, sk$_r$
300
DISPOSITIVO DE DESCIFRADO
310
PARTE DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
pk, sk$_r$
320
PARTE DE RECEPCIÓN DE DATOS
c t$_x$
330
PARTE DE OPERACIÓN DE EMPAREJAMIENTO
c t$_x$
340
PARTE DE CÁLCULO DE MENSAJE
m' (=m)
c t$_x$

Fig. 6

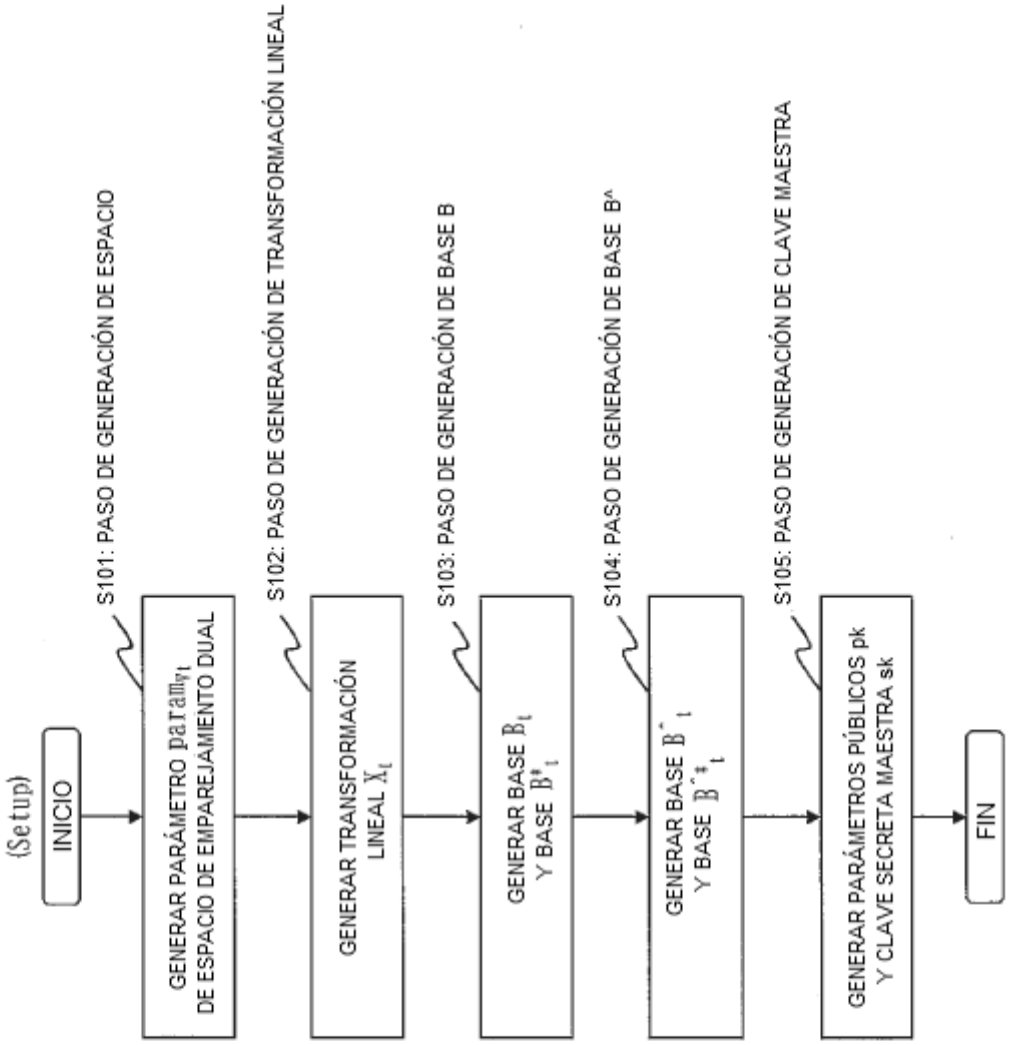

(Setup)
INICIO
S101: PASO DE GENERACIÓN DE ESPACIO
GENERAR PARÁMETRO $param_t$ DE ESPACIO DE EMPAREJAMIENTO DUAL
S102: PASO DE GENERACIÓN DE TRANSFORMACIÓN LINEAL
GENERAR TRANSFORMACIÓN LINEAL X_t
S103: PASO DE GENERACIÓN DE BASE B
GENERAR BASE B_t Y BASE B^*_t
S104: PASO DE GENERACIÓN DE BASE B^
GENERAR BASE $\hat{B}_t$ Y BASE $\hat{B}^*_t$
S105: PASO DE GENERACIÓN DE CLAVE MAESTRA
GENERAR PARÁMETROS PÚBLICOS pk Y CLAVE SECRETA MAESTRA sk
FIN

Fig. 7

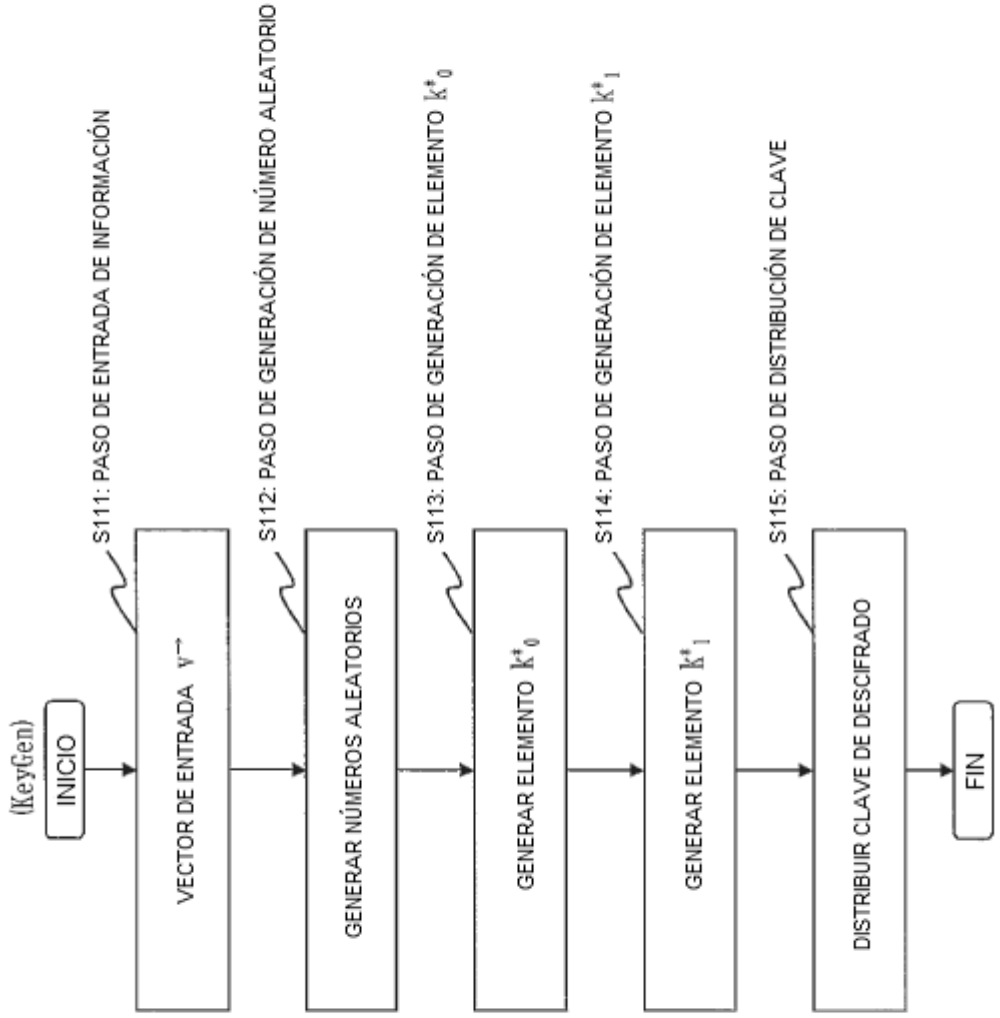

(KeyGen)
INICIO
S111: PASO DE ENTRADA DE INFORMACIÓN
VECTOR DE ENTRADA $\vec{v}$
S112: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S113: PASO DE GENERACIÓN DE ELEMENTO k^*_0
GENERAR ELEMENTO k^*_0
S114: PASO DE GENERACIÓN DE ELEMENTO k^*_1
GENERAR ELEMENTO k^*_1
S115: PASO DE DISTRIBUCIÓN DE CLAVE
DISTRIBUIR CLAVE DE DESCIFRADO
FIN

Fig. 8

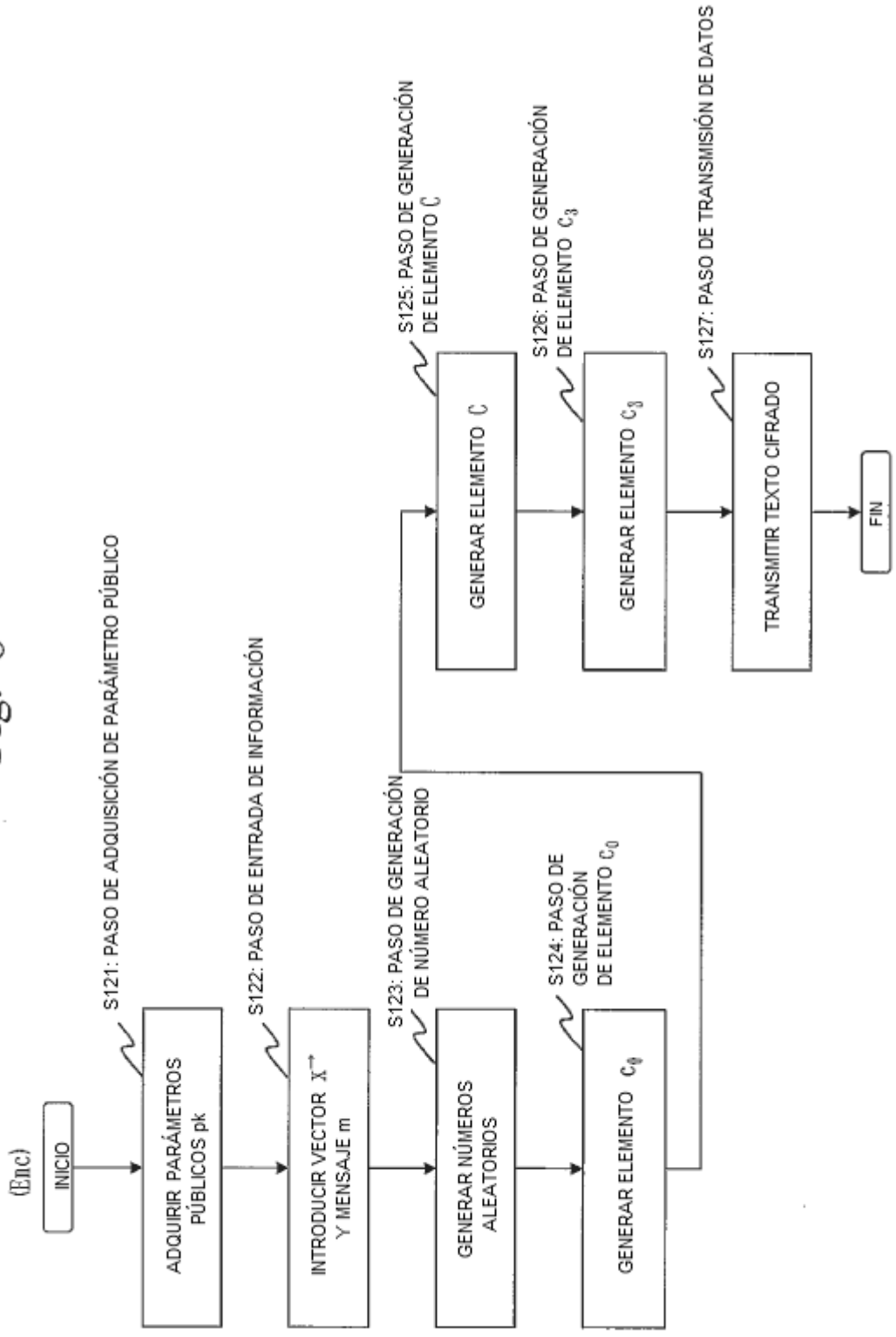

(Enc)
INICIO
S121: PASO DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
ADQUIRIR PARÁMETROS PÚBLICOS pk
S122: PASO DE ENTRADA DE INFORMACIÓN
INTRODUCIR VECTOR $\vec{X}$ Y MENSAJE m
S123: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S124: PASO DE GENERACIÓN DE ELEMENTO c_0
GENERAR ELEMENTO c_θ
S125: PASO DE GENERACIÓN DE ELEMENTO C
GENERAR ELEMENTO C
S126: PASO DE GENERACIÓN DE ELEMENTO c_3
GENERAR ELEMENTO c_3
S127: PASO DE TRANSMISIÓN DE DATOS
TRANSMITIR TEXTO CIFRADO
FIN

Fig. 9

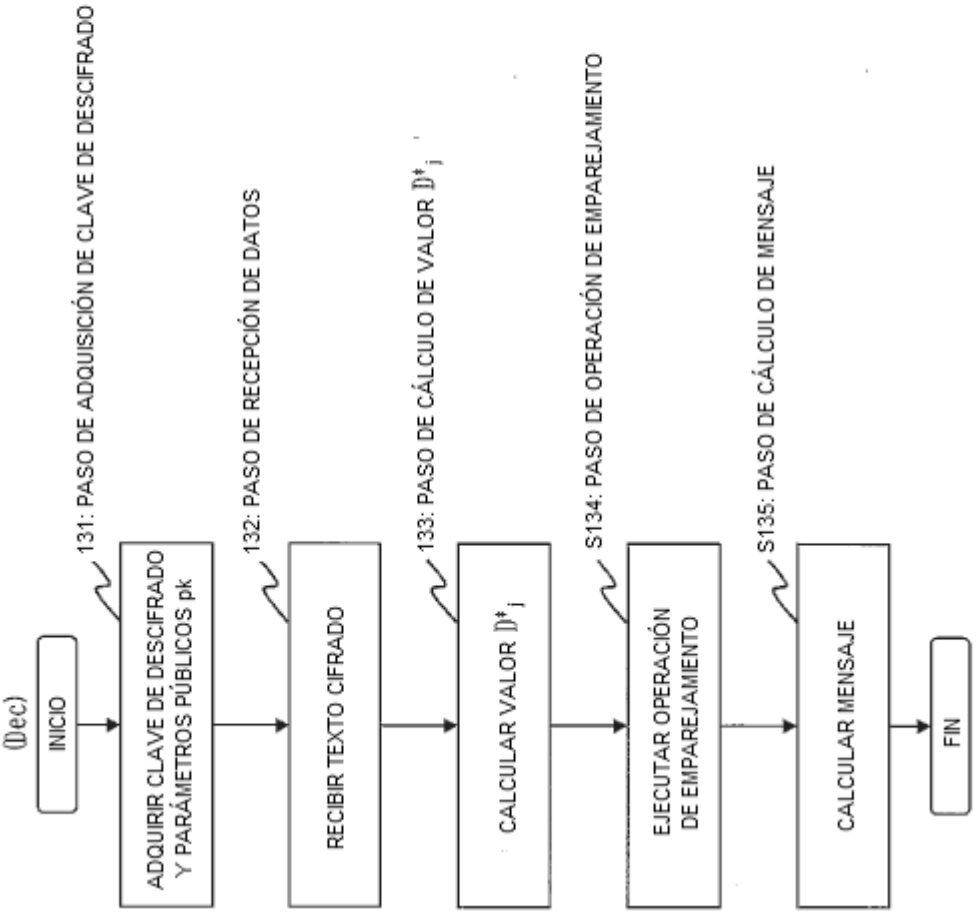

(Dec)
INICIO
131: PASO DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
ADQUIRIR CLAVE DE DESCIFRADO Y PARÁMETROS PÚBLICOS pk
132: PASO DE RECEPCIÓN DE DATOS
RECIBIR TEXTO CIFRADO
133: PASO DE CÁLCULO DE VALOR $D^{\dagger}_{j}$
CALCULAR VALOR $D^{\dagger}_{j}$
S134: PASO DE OPERACIÓN DE EMPAREJAMIENTO
EJECUTAR OPERACIÓN DE EMPAREJAMIENTO
S135: PASO DE CÁLCULO DE MENSAJE
CALCULAR MENSAJE
FIN

Fig. 10

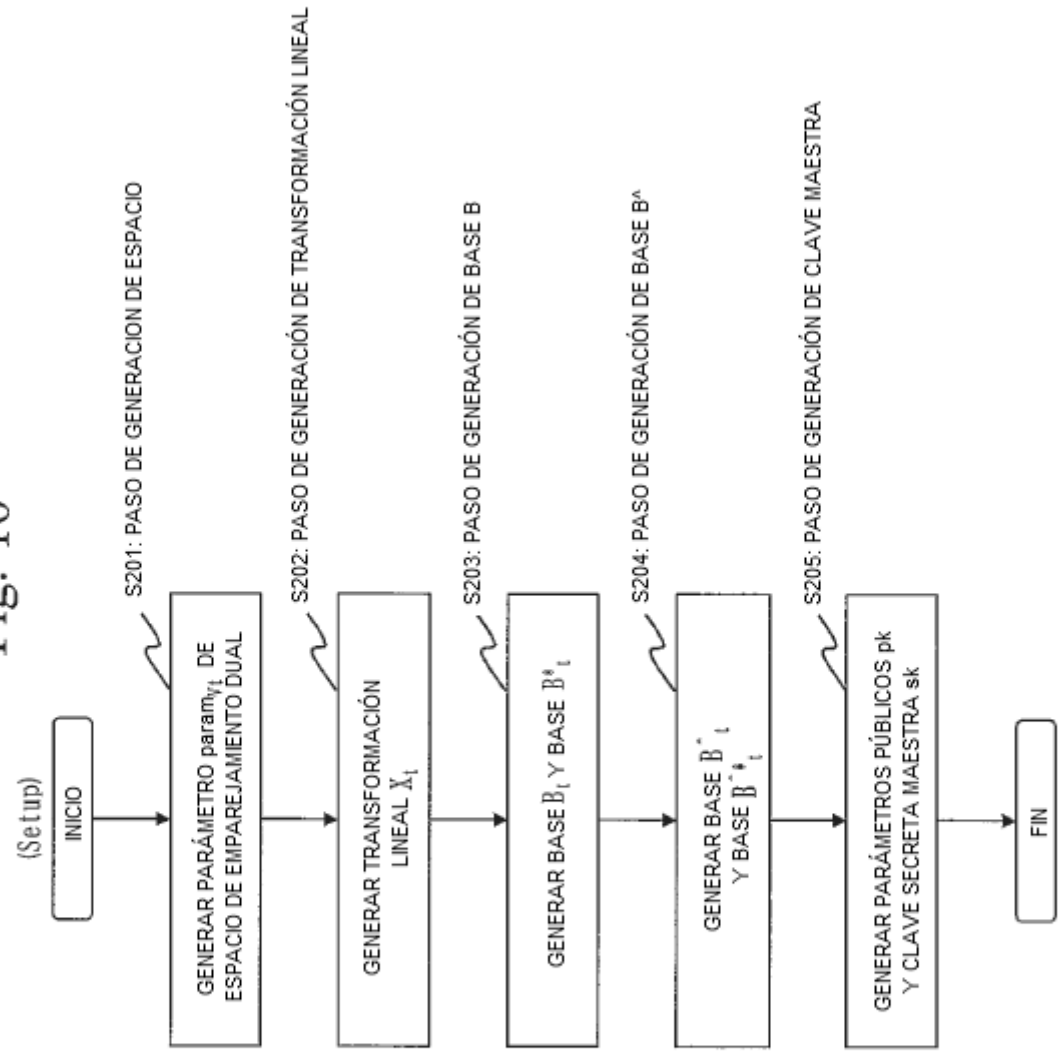

(Setup)
INICIO
S201: PASO DE GENERACION DE ESPACIO
GENERAR PARÁMETRO param$_{\gamma t}$ DE ESPACIO DE EMPAREJAMIENTO DUAL
S202: PASO DE GENERACIÓN DE TRANSFORMACIÓN LINEAL
GENERAR TRANSFORMACIÓN LINEAL X_t
S203: PASO DE GENERACIÓN DE BASE B
GENERAR BASE B_t Y BASE B^*_t
S204: PASO DE GENERACIÓN DE BASE B^
GENERAR BASE $\hat{B}_t$ Y BASE $\hat{B}^*_t$
S205: PASO DE GENERACIÓN DE CLAVE MAESTRA
GENERAR PARÁMETROS PÚBLICOS pk Y CLAVE SECRETA MAESTRA sk
FIN

Fig. 11

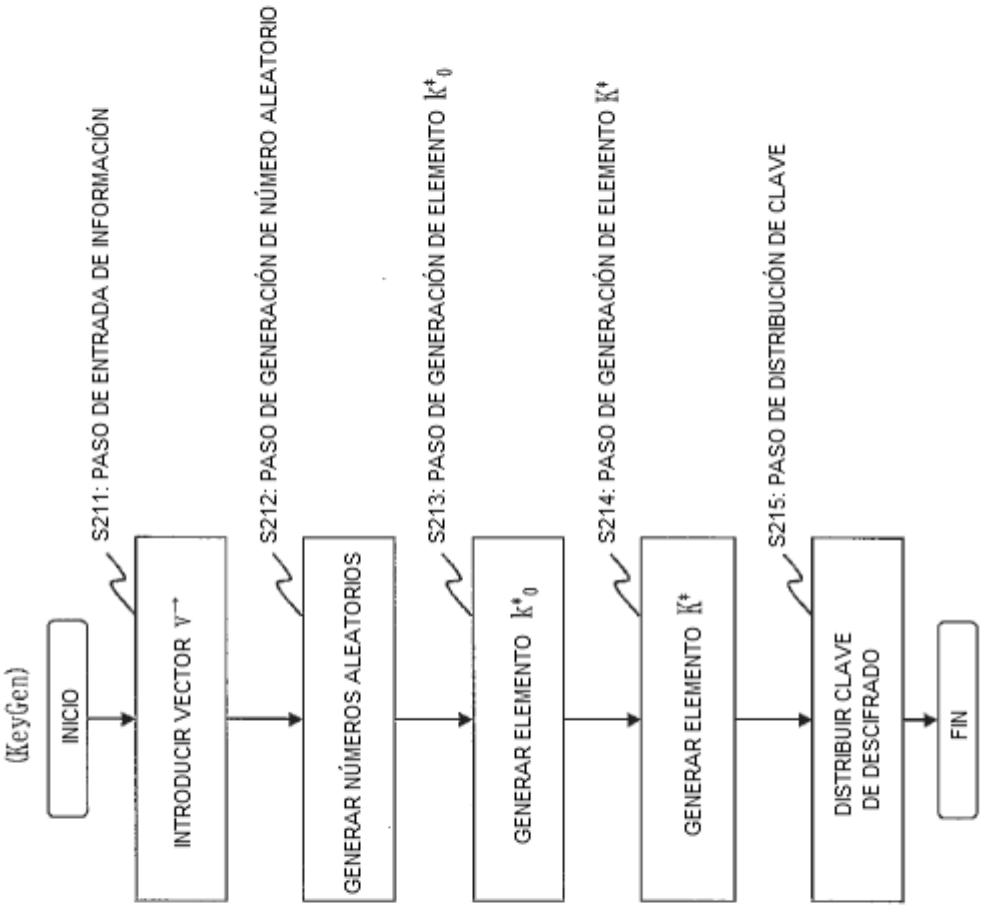

(KeyGen)
INICIO
S211: PASO DE ENTRADA DE INFORMACIÓN
INTRODUCIR VECTOR v^*
S212: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S213: PASO DE GENERACIÓN DE ELEMENTO k^*_0
GENERAR ELEMENTO k^*_0
S214: PASO DE GENERACIÓN DE ELEMENTO K^*
GENERAR ELEMENTO K^*
S215: PASO DE DISTRIBUCIÓN DE CLAVE
DISTRIBUIR CLAVE DE DESCIFRADO
FIN

Fig. 12

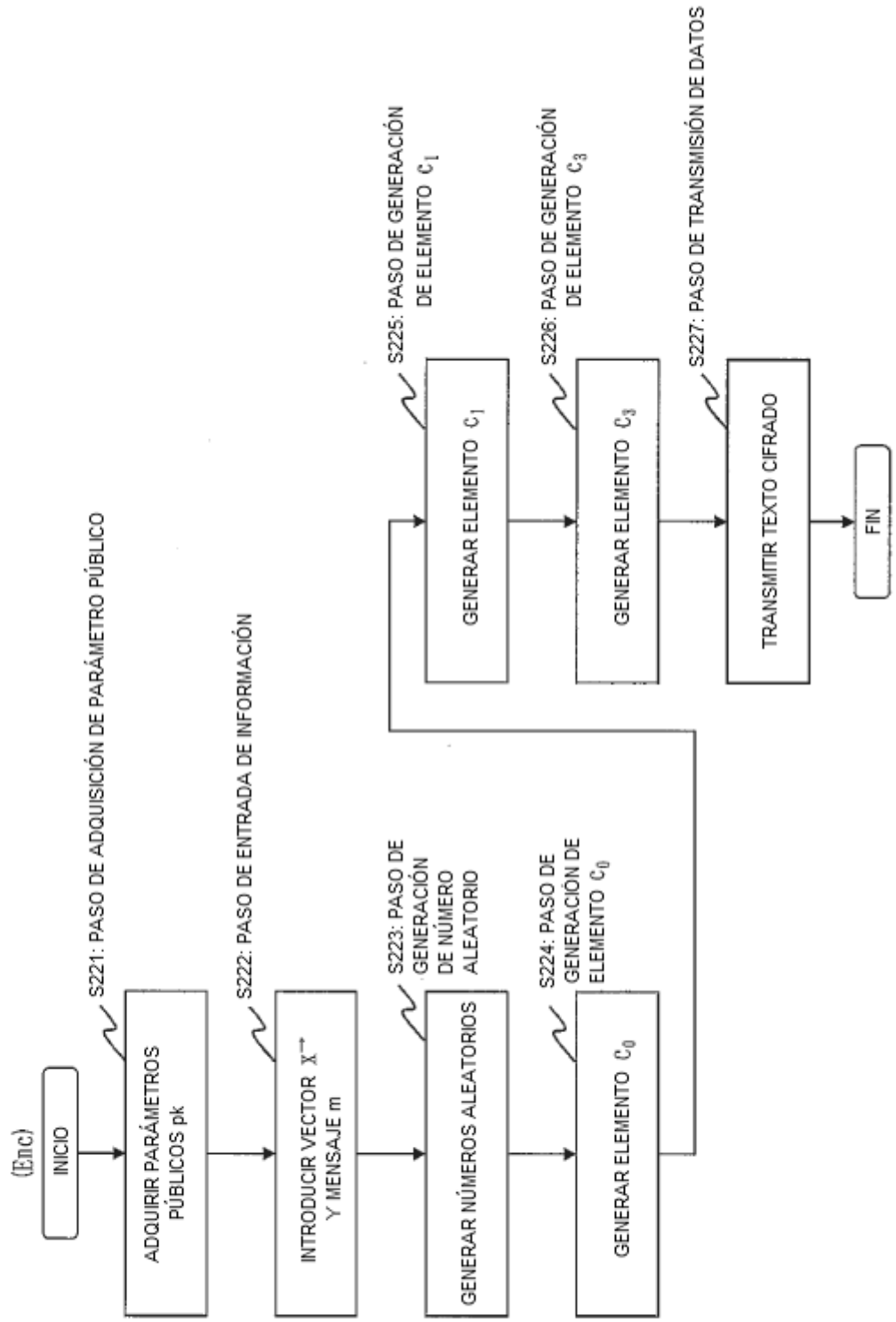

(Enc)
INICIO
S221: PASO DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
ADQUIRIR PARÁMETROS PÚBLICOS pk
S222: PASO DE ENTRADA DE INFORMACIÓN
INTRODUCIR VECTOR $\vec{X}$ Y MENSAJE m
S223: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S224: PASO DE GENERACIÓN DE ELEMENTO c_0
GENERAR ELEMENTO c_0
S225: PASO DE GENERACIÓN DE ELEMENTO c_1
GENERAR ELEMENTO c_1
S226: PASO DE GENERACIÓN DE ELEMENTO c_3
GENERAR ELEMENTO c_3
S227: PASO DE TRANSMISIÓN DE DATOS
TRANSMITIR TEXTO CIFRADO
FIN

Fig. 13

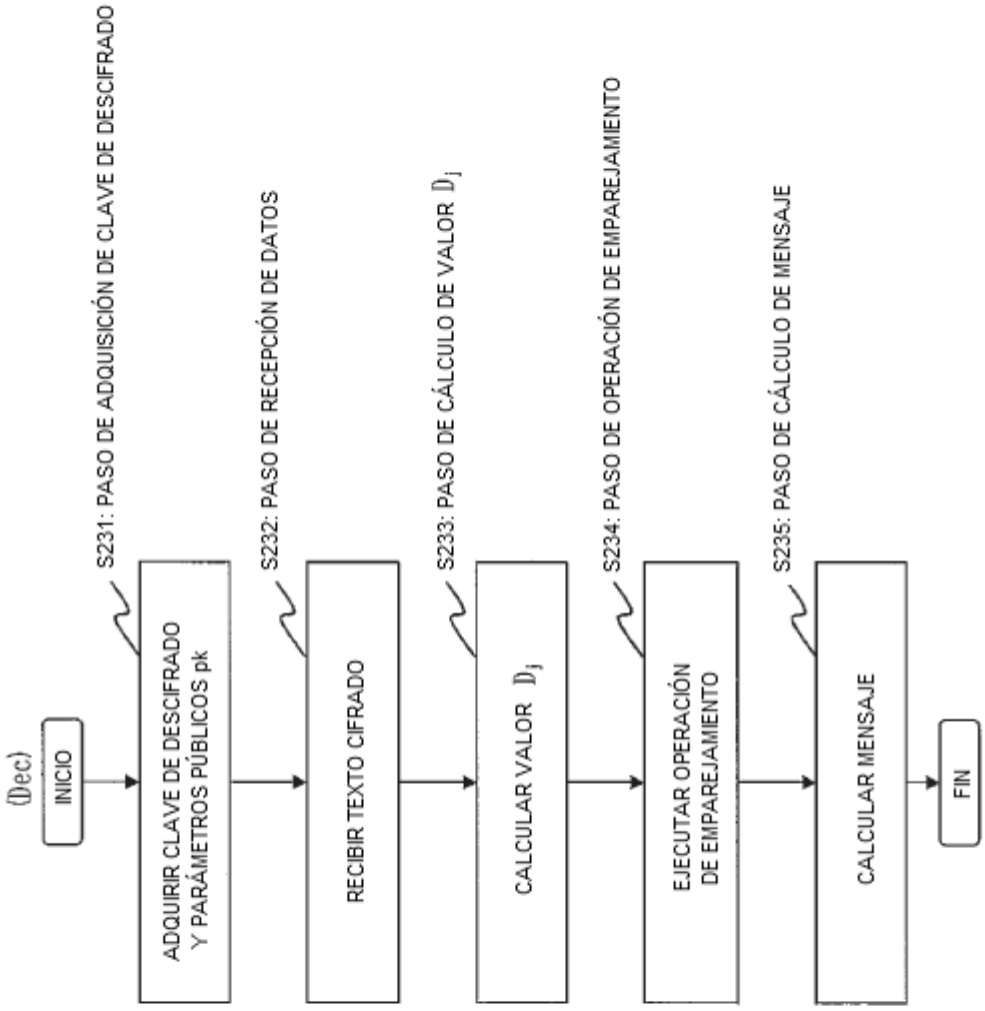

(Dec)
INICIO
S231: PASO DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
ADQUIRIR CLAVE DE DESCIFRADO Y PARÁMETROS PÚBLICOS pk
S232: PASO DE RECEPCIÓN DE DATOS
RECIBIR TEXTO CIFRADO
S233: PASO DE CÁLCULO DE VALOR D_j
CALCULAR VALOR D_j
S234: PASO DE OPERACIÓN DE EMPAREJAMIENTO
EJECUTAR OPERACIÓN DE EMPAREJAMIENTO
S235: PASO DE CÁLCULO DE MENSAJE
CALCULAR MENSAJE
FIN

Fig. 14

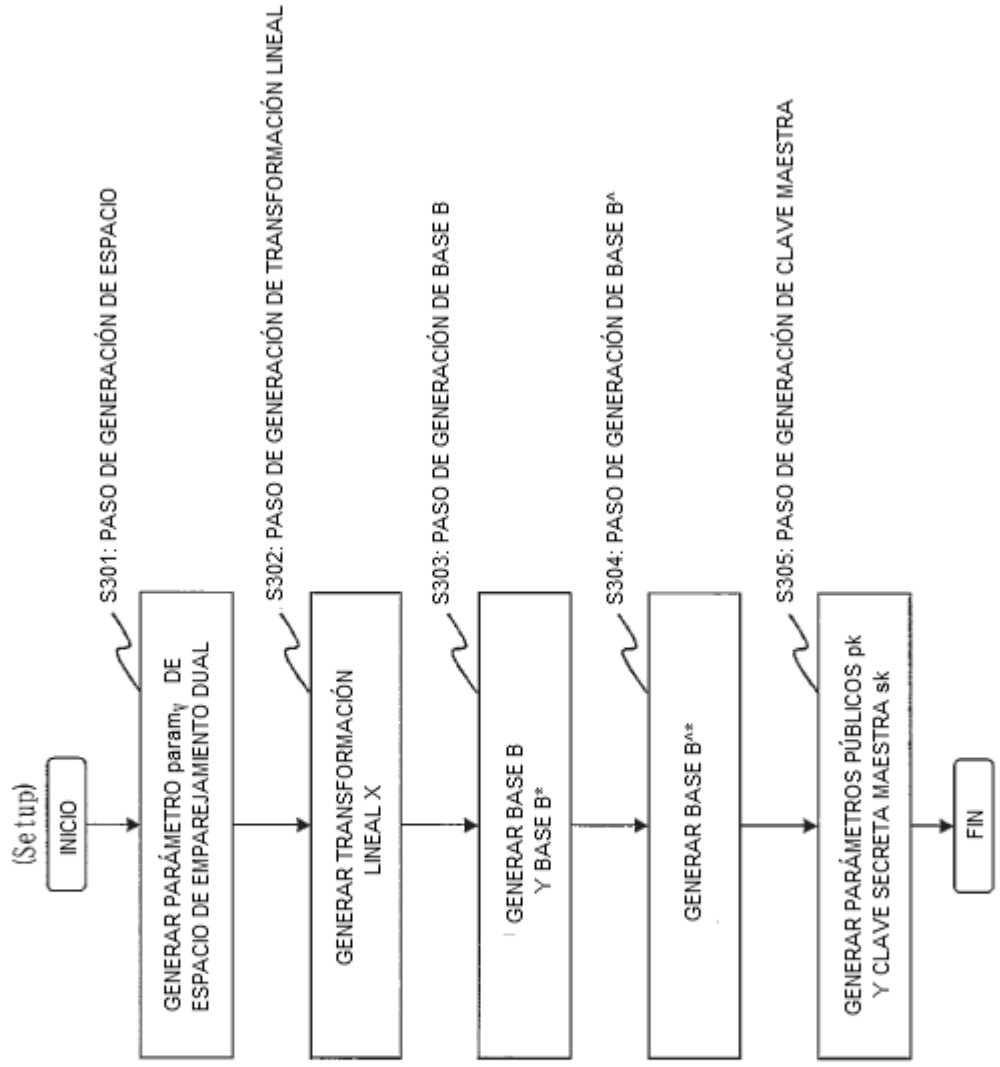

(Setup)
INICIO
S301: PASO DE GENERACIÓN DE ESPACIO
GENERAR PARÁMETRO $param_V$ DE ESPACIO DE EMPAREJAMIENTO DUAL
S302: PASO DE GENERACIÓN DE TRANSFORMACIÓN LINEAL
GENERAR TRANSFORMACIÓN LINEAL X
S303: PASO DE GENERACIÓN DE BASE B
GENERAR BASE B Y BASE B*
S304: PASO DE GENERACIÓN DE BASE B^
GENERAR BASE B^*
S305: PASO DE GENERACIÓN DE CLAVE MAESTRA
GENERAR PARÁMETROS PÚBLICOS pk Y CLAVE SECRETA MAESTRA sk
FIN

Fig. 15

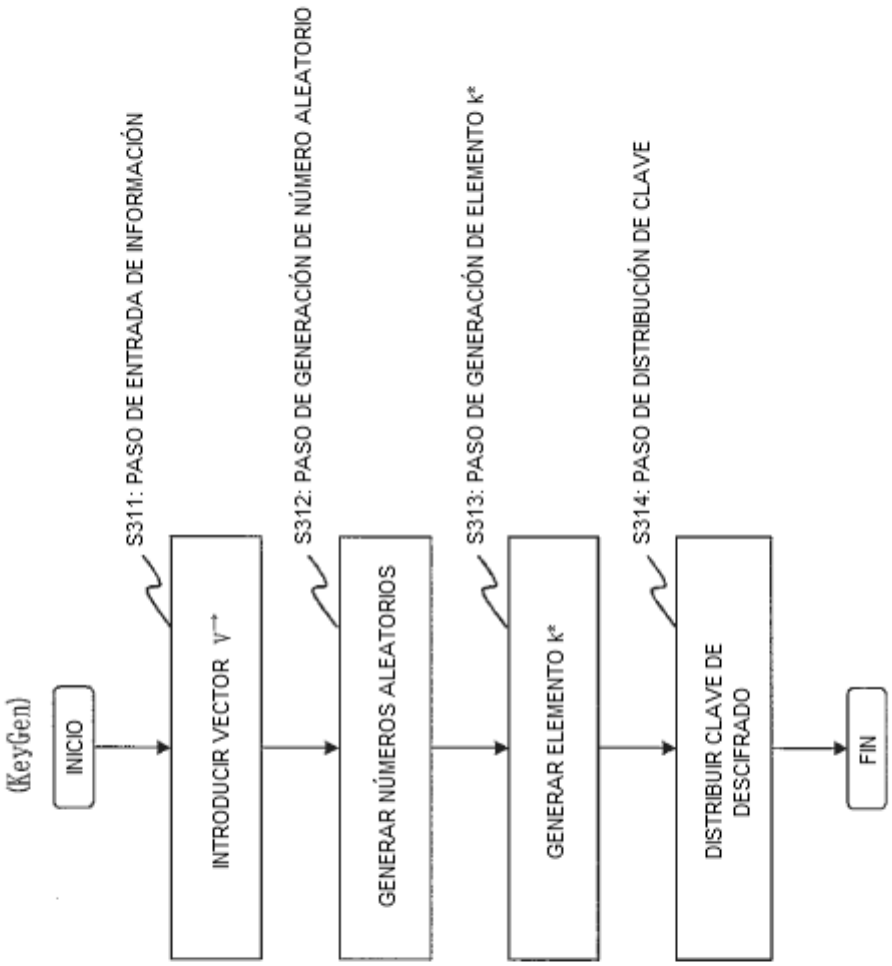

(KeyGen)
INICIO
S311: PASO DE ENTRADA DE INFORMACIÓN
INTRODUCIR VECTOR $\vec{V}$
S312: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S313: PASO DE GENERACIÓN DE ELEMENTO k*
GENERAR ELEMENTO k*
S314: PASO DE DISTRIBUCIÓN DE CLAVE
DISTRIBUIR CLAVE DE DESCIFRADO
FIN

Fig. 16

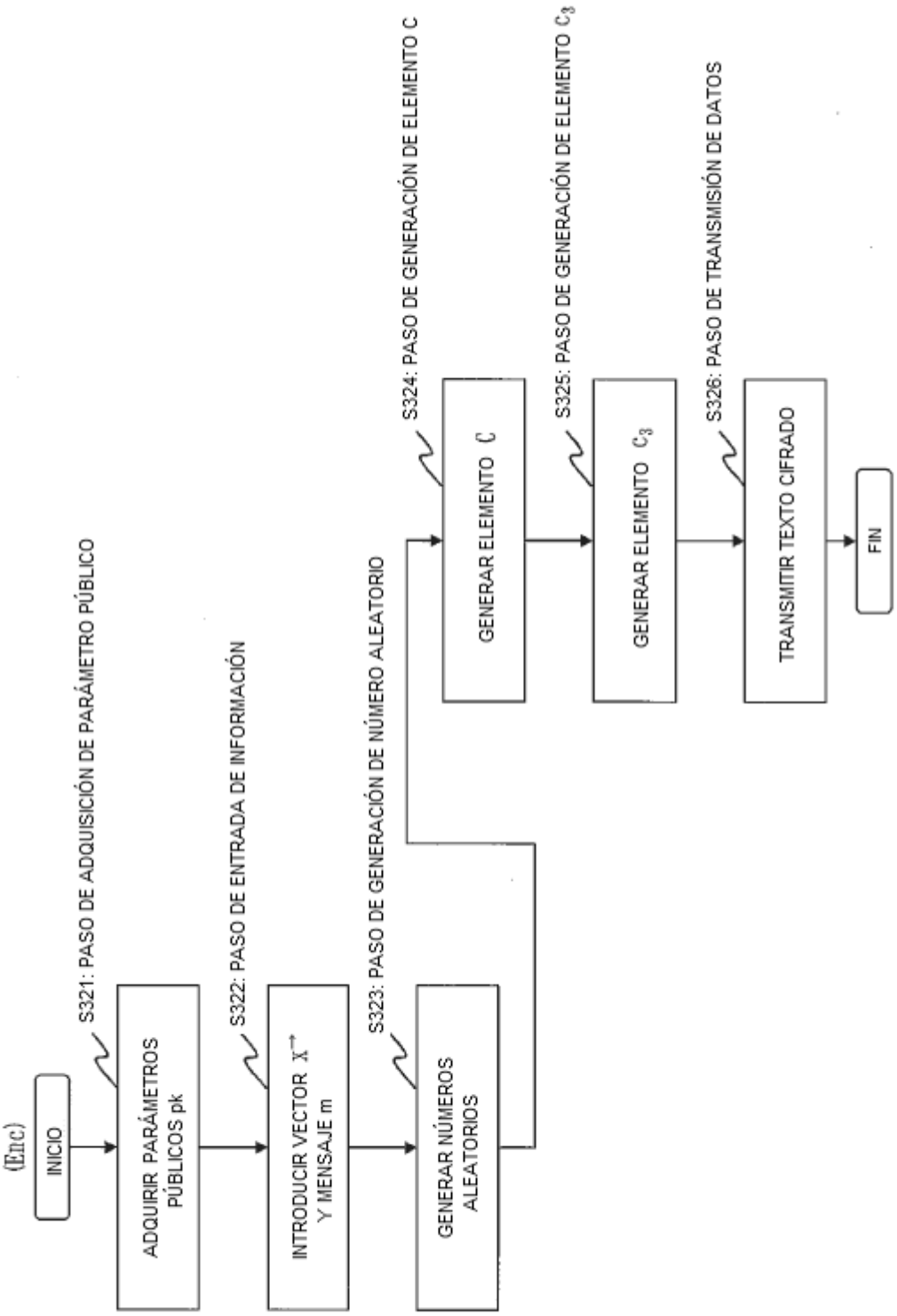

(Enc)
INICIO
S321: PASO DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
ADQUIRIR PARÁMETROS PÚBLICOS pk
S322: PASO DE ENTRADA DE INFORMACIÓN
INTRODUCIR VECTOR $\vec{X}$ Y MENSAJE m
S323: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S324: PASO DE GENERACIÓN DE ELEMENTO C
GENERAR ELEMENTO C
S325: PASO DE GENERACIÓN DE ELEMENTO C_3
GENERAR ELEMENTO C_3
S326: PASO DE TRANSMISIÓN DE DATOS
TRANSMITIR TEXTO CIFRADO
FIN

Fig. 17

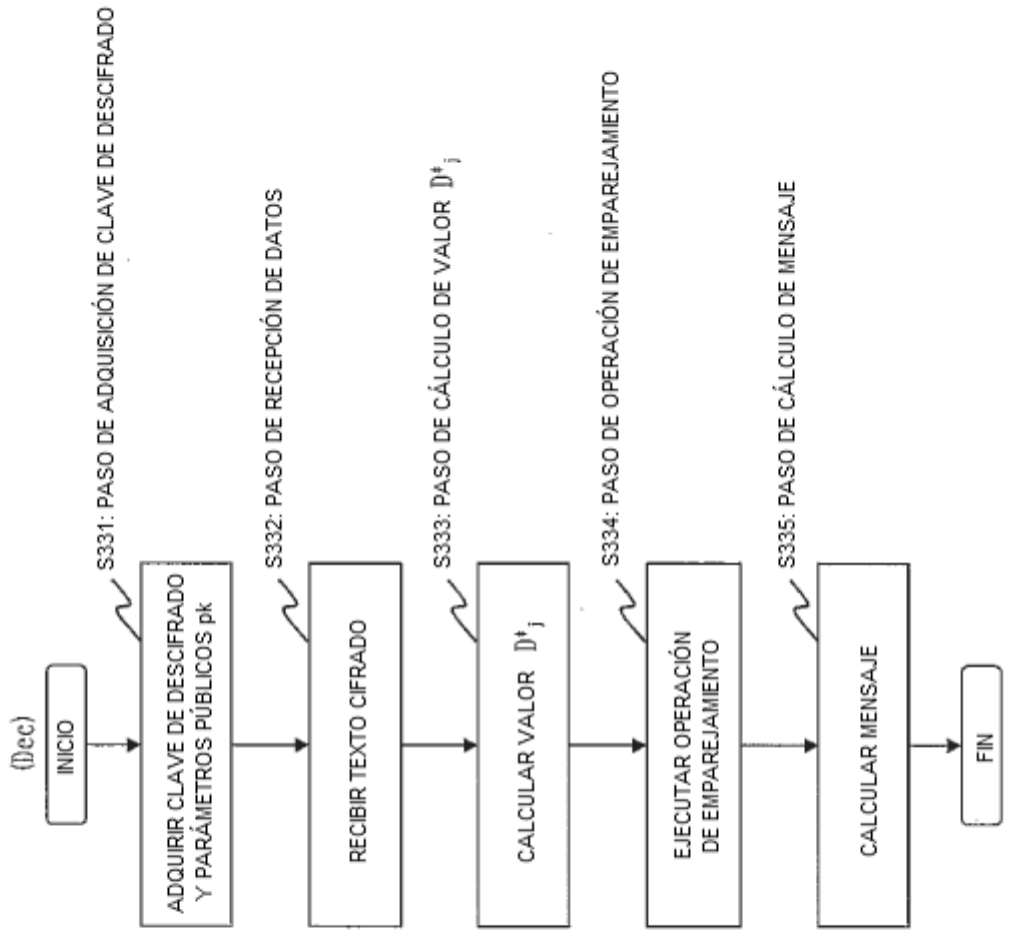

(Dec)
INICIO
S331: PASO DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
ADQUIRIR CLAVE DE DESCIFRADO Y PARÁMETROS PÚBLICOS pk
S332: PASO DE RECEPCIÓN DE DATOS
RECIBIR TEXTO CIFRADO
S333: PASO DE CÁLCULO DE VALOR D'_j
CALCULAR VALOR D'_j
S334: PASO DE OPERACIÓN DE EMPAREJAMIENTO
EJECUTAR OPERACIÓN DE EMPAREJAMIENTO
S335: PASO DE CÁLCULO DE MENSAJE
CALCULAR MENSAJE
FIN

Fig. 18

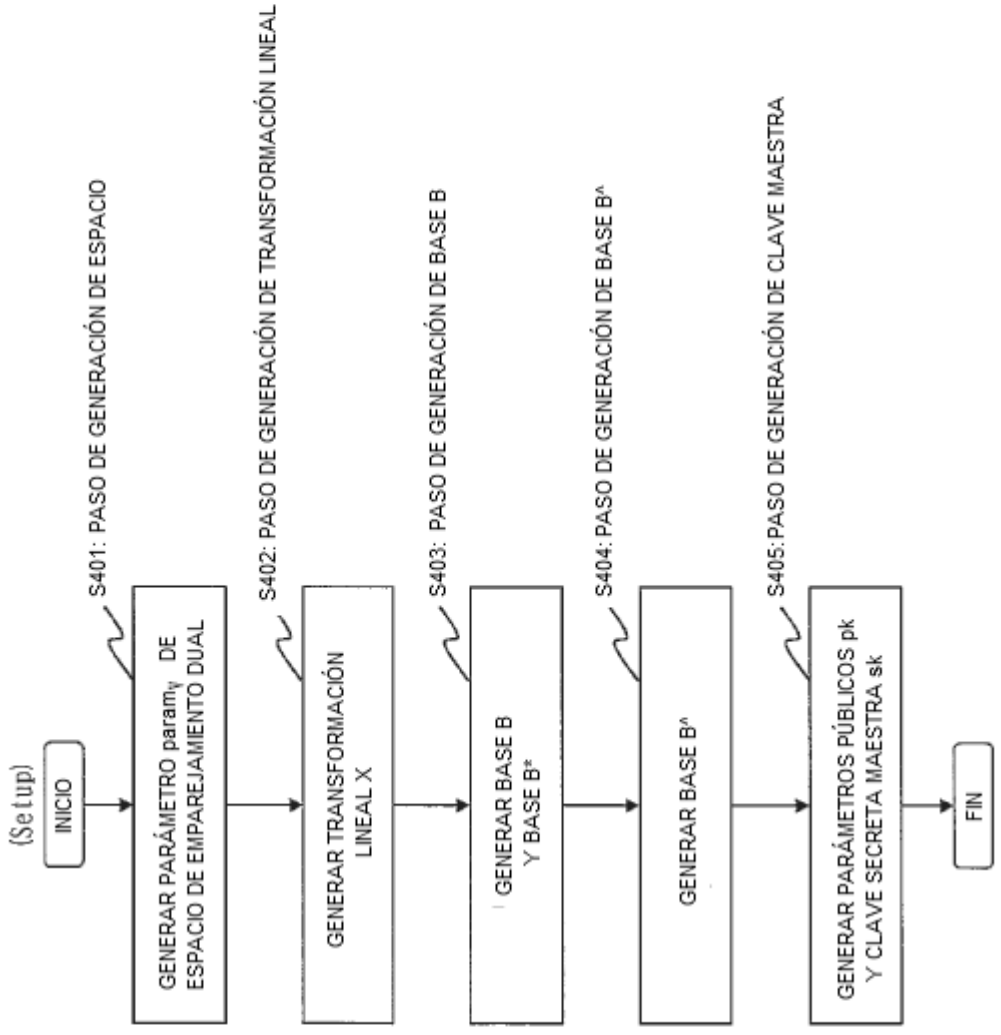

(Setup)
INICIO
S401: PASO DE GENERACIÓN DE ESPACIO
GENERAR PARÁMETRO param$_\Psi$ DE ESPACIO DE EMPAREJAMIENTO DUAL
S402: PASO DE GENERACIÓN DE TRANSFORMACIÓN LINEAL
GENERAR TRANSFORMACIÓN LINEAL X
S403: PASO DE GENERACIÓN DE BASE B
GENERAR BASE B Y BASE B*
S404: PASO DE GENERACIÓN DE BASE B^
GENERAR BASE B^
S405: PASO DE GENERACIÓN DE CLAVE MAESTRA
GENERAR PARÁMETROS PÚBLICOS pk Y CLAVE SECRETA MAESTRA sk
FIN

Fig. 19

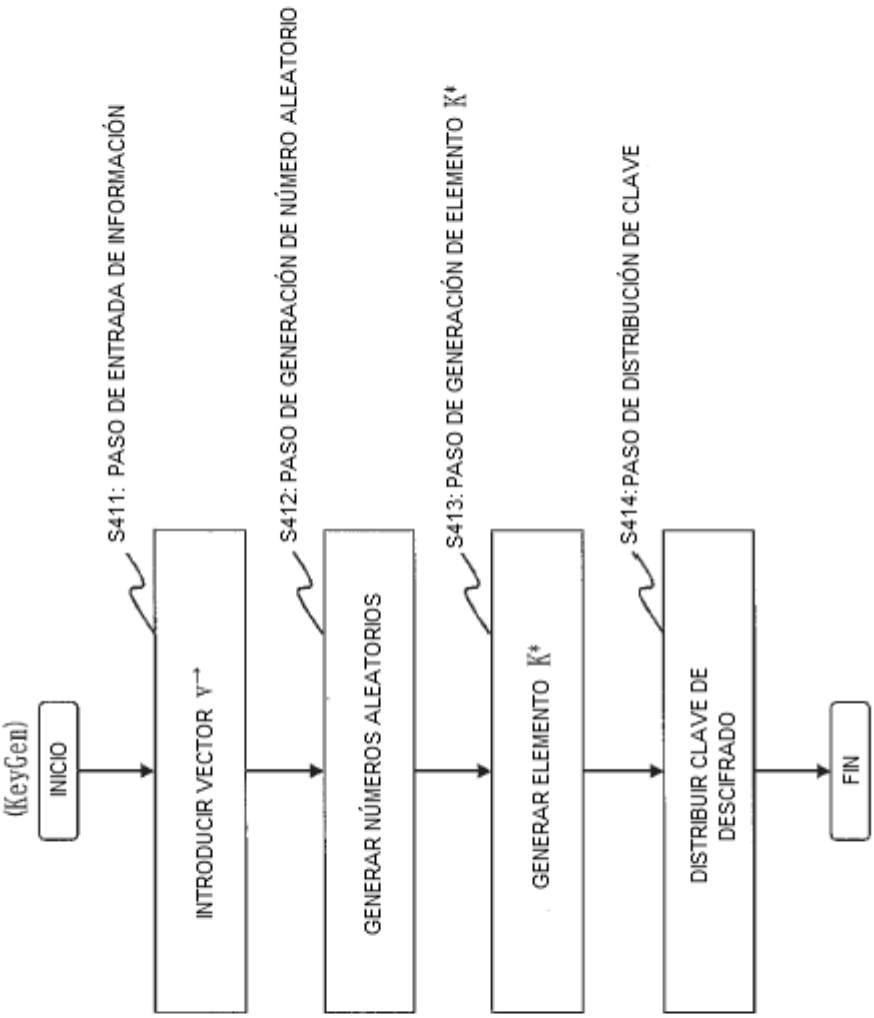

(KeyGen)
INICIO
S411: PASO DE ENTRADA DE INFORMACIÓN
INTRODUCIR VECTOR $\vec{v}$
S412: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S413: PASO DE GENERACIÓN DE ELEMENTO $\mathbb{K}^*$
GENERAR ELEMENTO $\mathbb{K}^*$
S414: PASO DE DISTRIBUCIÓN DE CLAVE
DISTRIBUIR CLAVE DE DESCIFRADO
FIN

Fig. 20

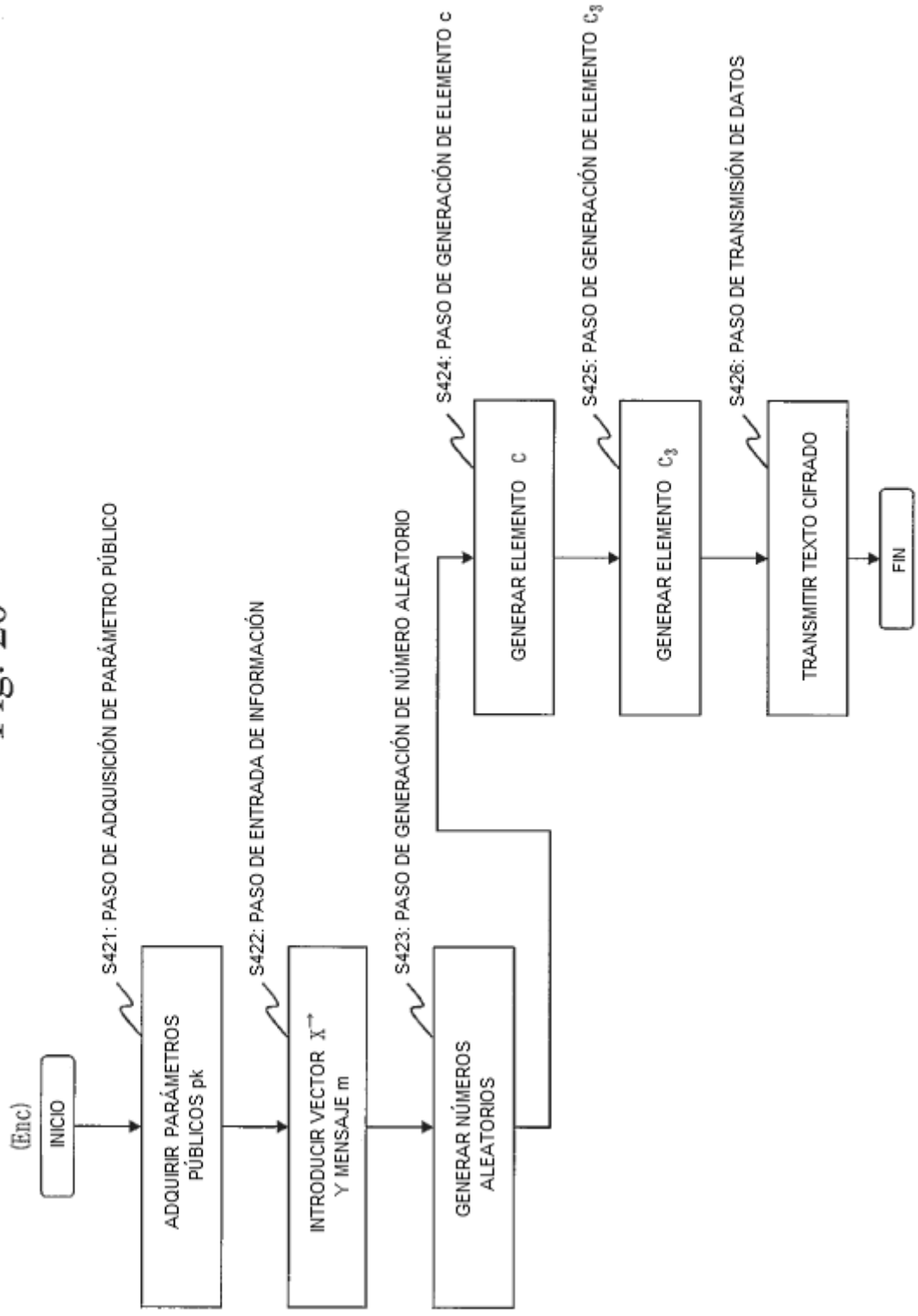

(Enc)
INICIO
S421: PASO DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
ADQUIRIR PARÁMETROS PÚBLICOS pk
S422: PASO DE ENTRADA DE INFORMACIÓN
INTRODUCIR VECTOR $\vec{X}$ Y MENSAJE m
S423: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMEROS ALEATORIOS
S424: PASO DE GENERACIÓN DE ELEMENTO c
GENERAR ELEMENTO c
S425: PASO DE GENERACIÓN DE ELEMENTO c_3
GENERAR ELEMENTO c_3
S426: PASO DE TRANSMISIÓN DE DATOS
TRANSMITIR TEXTO CIFRADO
FIN

Fig. 21

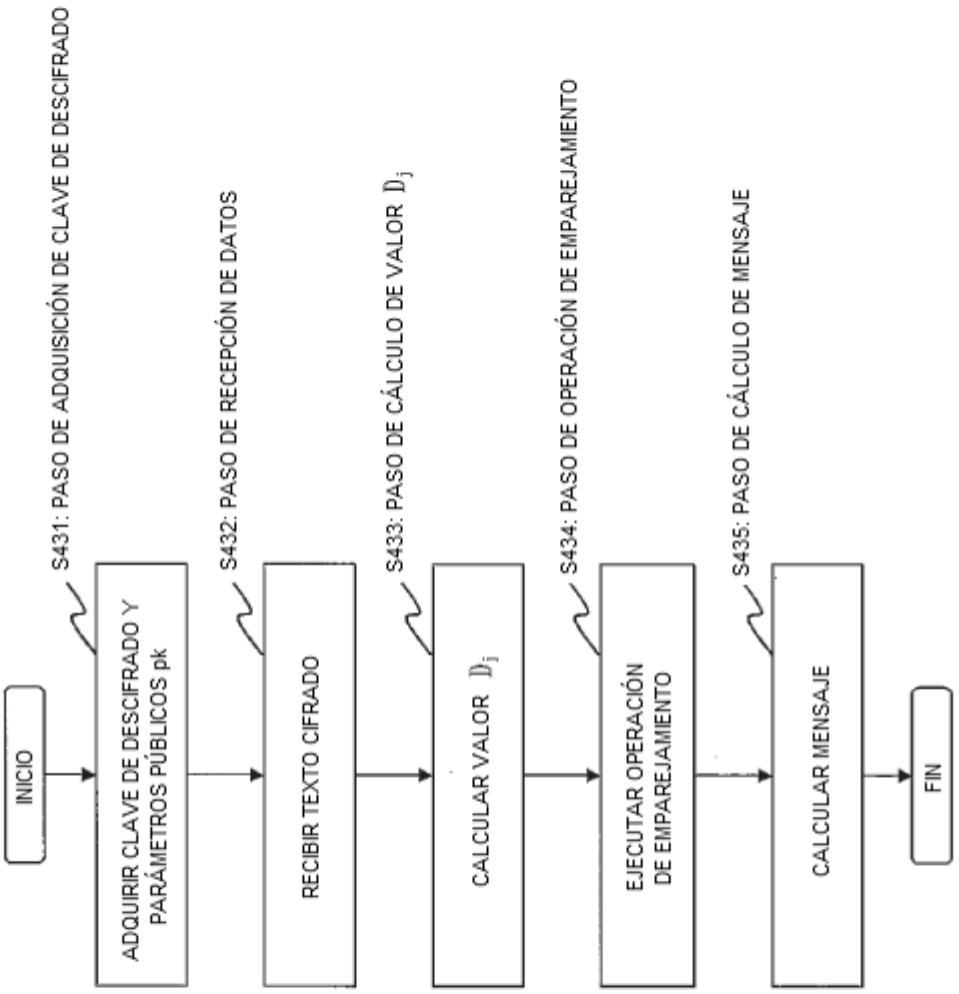
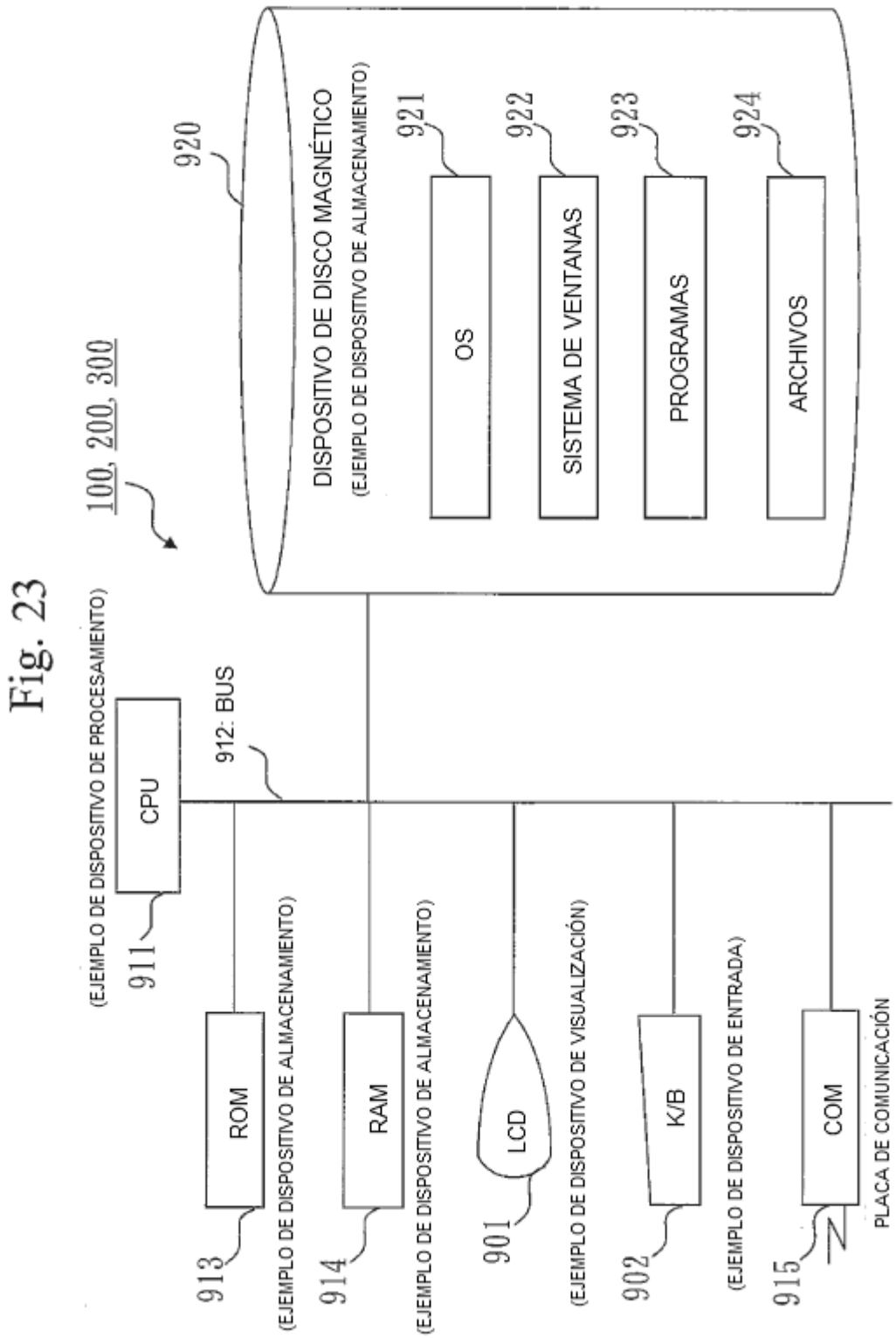

(Dec)
INICIO
S431: PASO DE ADQUISICIÓN DE CLAVE DE DESCIFRADO
ADQUIRIR CLAVE DE DESCIFRADO Y PARÁMETROS PÚBLICOS pk
S432: PASO DE RECEPCIÓN DE DATOS
RECIBIR TEXTO CIFRADO
S433: PASO DE CÁLCULO DE VALOR D_j
CALCULAR VALOR D_j
S434: PASO DE OPERACIÓN DE EMPAREJAMIENTO
EJECUTAR OPERACIÓN DE EMPAREJAMIENTO
S435: PASO DE CÁLCULO DE MENSAJE
CALCULAR MENSAJE
FIN

Fig. 22

	ESQUEMA DE LITERATURA NO DE PATENTE 2 ZIPE con CT cortos	ESQUEMA DE LITERATURA NO DE PATENTE 2 NIPE con CT cortos	ESQUEMA DE REALIZACIÓN 2 ZIPE con CT cortos	ESQUEMA DE REALIZACIÓN 4 NIPE con CT cortos	ESQUEMA DE REALIZACIÓN 3 ZIPE con SK cortas	ESQUEMA DE REALIZACIÓN 5 NIPE con SK cortas
Seguridad	Adaptativo	Co-selectivo	Adaptativo	Adaptativo	Adaptativo	Adaptativo
Suposic.	DLIN Y DBDH	DLIN Y DBDH	DLIN	DLIN	DLIN	DLIN
Rel. IP	Cero	No cero	Cero	No cero	Cero	No cero
Tamaño PK	$(n+11)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(n+11)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(10n+13)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(8n+23)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(10n+13)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(8n+23)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$
Tamaño SK	$(n+6)\lvert\mathbb{G}\rvert + (n+1)\lvert\mathbb{F}_q\rvert$	$(n+6)\lvert\mathbb{G}\rvert$	$(4n+1)\lvert\mathbb{G}\rvert$	$(4n+5)\lvert\mathbb{G}\rvert$	$9\lvert\mathbb{G}\rvert$	$13\lvert\mathbb{G}\rvert$
Tamaño CT	$9\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert + \lvert\mathbb{F}_q\rvert$	$9\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$9\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$13\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(4n+1)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(4n+5)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$
Tiempo Dec	9P+nM	9P+nM	9P+4(n−1)M	13P+4(n−1)M	9P+4(n−1)M	13P+4(n−1)M

ES 2 613 811 T3

Fig. 23


100, 200, 300
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)
CPU
911
ROM
913
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
RAM
914
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
LCD
901
(EJEMPLO DE DISPOSITIVO DE VISUALIZACIÓN)
K/B
902
(EJEMPLO DE DISPOSITIVO DE ENTRADA)
COM
915
PLACA DE COMUNICACIÓN