(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 645 463**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.07.2013 PCT/JP2013/069368**

(87) Fecha y número de publicación internacional: **06.02.2014 WO14021102**

(96) Fecha de presentación y número de la solicitud europea: **17.07.2013 E 13824763 (0)**

(97) Fecha y número de publicación de la concesión europea: **27.09.2017 EP 2881930**

(54) Título: **Sistema criptográfico, método criptográfico, programa criptográfico y dispositivo de desencriptación**

(30) Prioridad:

31.07.2012 JP 2012170001

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.12.2017

(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:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema criptográfico, método criptográfico, programa criptográfico y dispositivo de desencriptación

Campo técnico

La presente invención a un esquema de encriptación funcional que utiliza la noción de programa de amplitud cuadrática.

Antecedentes

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

Según el esquema de encriptación funcional, un parámetro Φ y un parámetro Ψ se configuran respectivamente en la clave de encriptación ek y la clave de desencriptación dk. La clave de desencriptación dk puede desencriptar un texto cifrado mediante la clave de encriptación ek si y solo si se mantiene una relación R (Φ, Ψ).

La bibliografía no de patente 3 describe el esquema de encriptación funcional.

La bibliografía no de patente 6 describe el programa de amplitud cuadrática. La patente US 2009/080658 A1 se refiere a un método y aparato para encriptar datos para un control riguroso de acceso. El método para encriptar datos incluye encriptar los datos como un texto cifrado, etiquetar el texto cifrado con un conjunto de uno o más atributos descriptivos, generar una clave de desencriptación para desencriptar el texto cifrado, asociar una estructura de acceso con la clave de desencriptación, de manera que los datos sean recuperables del texto cifrado utilizando la clave de desencriptación solo si el conjunto de uno o más atributos descriptivos satisface la estructura de acceso y emite el texto cifrado y la clave de desencriptación.

Lista de citas

Bibliografía no de patente

Bibliografía no de patente 1: T. Okamoto, K. Takashima: Homomorphic encryption and signatures from vector decomposition. En: S.D. Galbraith, K.G. Paterson, (eds.) Pairing 2008. LNCS, vol. 5209, páginas 57 a 74, Springer Heidelberg (2008).

Bibliografía no de patente 2: T. Okamoto, K. Takashima: Hierarchical predicate encryption for inner-products. En: ASIACRYPT 2009, Springer Heidelberg (2009).

Bibliografía no de patente 3: T. Okamoto, K. Takashima: Fully secure functional encryption with general relations from the decisional linear assumption. En: T. Rabin, (ed.) CRYPTO 2010. LNCS, vol. 6223, páginas 191 a 208. Springer Heidelberg (2010). La versión completa está disponible en http://eprint.iacr.org/2010/563.

Bibliografía no de patente 4: T. Okamoto, K. Takashima: Efficient attribute-based signatures for non-monotone predicates in the standard model. En: PKC 2011, Springer Heidelberg (2011).

Bibliografía no de patente 5: T. Okamoto, K. Takashima: Decentralized Attribute-Based Signatures http://eprintiacr.org/2011/701.

Bibliografía no de patente 6: Rosario Gennaro y Craig Gentry y Bryan Parno y Mariana Raykova: Quadratic Span Programs and Succinct NIZKs without PCPs http://eprintiacr.org/2012/215.

Compendio de la invención

Problema técnico

El esquema de encriptación funcional descrito en la Bibliografía no patente 3 es un esquema que utiliza un programa de amplitud lineal. Este esquema de encriptación funcional solo puede expresar un rango limitado como una relación R.

Un objeto de la presente invención es proporcionar un esquema de encriptación funcional que, mediante la utilización de la noción de programa de amplitud cuadrática, puede expresar un rango más amplio como la relación R.

Solución al problema

Un sistema criptográfico según la presente invención incluye:

un dispositivo de encriptación que genera una de la primera información que incluye un programa de amplitud cuadrática y una segunda información que incluye información de atributos, como un texto cifrado; y

un dispositivo de desencriptación que, tratando una restante de la primera información y la segunda información, como clave de desencriptación, si el programa de amplitud cuadrática acepta la información de atributos, desencripta el texto cifrado en base a la información obtenida del programa de amplitud cuadrática y a la información de atributos.

Efectos ventajosos de la invención

El sistema criptográfico según la presente invención utiliza la noción de programa de amplitud cuadrática, de manera que un rango ideal puede expresarse como la relación R.

Breve descripción de los dibujos

La figura 1 es un dibujo explicativo de un programa de amplitud cuadrática.

La figura 2 es un dibujo explicativo de un subconjunto I_u.

La figura 3 es un diagrama de configuración de un sistema criptográfico 10 que ejecuta un esquema KP-FE.

La figura 4 es un diagrama de configuración de un sistema criptográfico 10 que ejecuta un esquema CP-FE.

La figura 5 es un diagrama de configuración de un dispositivo de generación de claves 100 según la realización 2.

La figura 6 es un diagrama de configuración de un dispositivo de encriptación 200 según la realización 2.

La figura 7 es un diagrama de configuración de un dispositivo de desencriptación 300 según la realización 2.

La figura 8 es un diagrama de flujo que muestra el proceso del algoritmo de Setup (Configuración) según la realización 2.

La figura 9 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen (Generación de claves) según la realización 2.

La figura 10 es un diagrama de flujo que muestra el proceso del algoritmo Enc (Encriptación) según la realización 2.

La figura 11 es un diagrama de flujo que muestra el proceso del algoritmo Dec (Desencriptación) según la realización 2.

La figura 12 es un diagrama de flujo que muestra el proceso del algoritmo de KeyGen según la realización 4.

La figura 13 es un diagrama que muestra un ejemplo de la configuración de hardware del dispositivo de generación de claves 100, el dispositivo de encriptación 200 y el dispositivo de desencriptación 300.

Descripción de las realizaciones

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

En la siguiente descripción, un dispositivo de procesamiento es una CPU 911 (que se describirá más adelante) y similares. Un dispositivo de almacenamiento es una ROM 913, una RAM 914, un disco magnético 920 (que se describirán cada uno más adelante), y similares. Un dispositivo de comunicación es una tarjeta de comunicación 915 (que se describirá más adelante) y similares. Un dispositivo de entrada es un teclado 902, la placa de comunicación 915 (que se describirán cada uno más adelante), y similares. Concretamente, el dispositivo de procesamiento, el dispositivo de almacenamiento, el dispositivo de comunicación y el dispositivo de entrada son hardware.

La notación se explicará en la siguiente descripción.

Cuando A es una variable o distribución aleatoria, la fórmula 101 indica que y se elige aleatoriamente a partir de A según la distribución de A. Concretamente, en la fórmula 101 y es un número aleatorio.

[Fórmula 101]

$$y \xleftarrow{R} A$$

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

[Fórmula 102]

$$y \xleftarrow{U} A$$

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

[Fórmula 103]

$$y := z$$

Cuando a es un valor fijo, la fórmula 104 indica un evento de que una máquina (algoritmo) A devuelve a para la entrada x.

[Fórmula 104]

$$A(x) \to a$$

Por ejemplo,

$$A(x) \to 1$$

La fórmula 105, concretamente, F_q, indica un campo finito de orden q.

[Fórmula 105]

$$\mathbb{F}_q$$

El símbolo de vector indica una representación vectorial sobre el campo finito F_q. Concretamente, se establece la fórmula 106.

[Fórmula 106]

$\vec{x}$ indica

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

La fórmula 107 indica el producto interno, indicado por la fórmula 109, de dos vectores $\mathbf{x}^{\rightarrow}$ y $\mathbf{v}^{\rightarrow}$ indicados en la fórmula 108.

[Fórmula 107]

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

[Fórmula 108]

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

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

[Fórmula 109]

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

Se debe observar que X^T indica la traspuesta de la matriz M.

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

[Fórmula 110]

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

[Fórmula 111]

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

[Fórmula 112]

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

Se debe observar que para las bases B y B* indicadas en la fórmula 113, se establece la fórmula 114.

[Fórmula 113]

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

[Fórmula 114]

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

En la siguiente descripción, cuando "Vt" se indica como un subíndice o un superíndice, Vt es V_t. Del mismo modo, cuando "δi,j" se indica como superíndice, δi,j es $\delta_{i,j}$. De igual manera, cuando "fт" y "kт" se indican como superíndices, fт es $f_т$, y kт es $k_т$.

Cuando "→" indica que un vector está unido a un subíndice o un superíndice, "→" está unido como un superíndice al subíndice o superíndice.

En la siguiente descripción, un proceso criptográfico incluye un proceso de generación de claves, un proceso de encriptación y un proceso de desencriptación.

Realización 1

Esta realización describe un concepto básico del esquema de encriptación funcional que utiliza el programa de amplitud cuadrática y el esquema del esquema de encriptación funcional que utiliza el programa de amplitud cuadrática.

En primer lugar, se describirá un espacio que tiene una rica estructura matemática llamada "espacios vectoriales de emparejamientos dobles (DPVS – Dual Pairing Vector Spaces, en inglés)" que es un espacio para implementar el esquema de encriptación funcional.

En segundo lugar, se describirá un concepto para implementar el esquema de encriptación funcional. Aquí se describirán el "programa de amplitud cuadrática", las "igualdades de información de atributos y el programa de amplitud cuadrática" y el "esquema de distribución secreta".

En tercer lugar, se describirá el esquema del esquema de encriptación funcional que utiliza el programa de amplitud cuadrática.

<2. Espacios vectoriales de emparejamientos dobles>

En primer lugar, los grupos de emparejamientos bilineales simétricos (q, G, G_T, g, e) son una tupla de un q primo, un grupo aditivo cíclico G de orden q, un grupo multiplicativo cíclico G_T de orden q, g ≠ 0 ∈ G y un emparejamiento bilineal no degenerado calculable en el tiempo polinomial e : G x G → G_T. El emparejamiento bilineal no degenerado significa e (sg, tg) = e (g, g)st donde e (g, g) ≠ 1.

En la descripción siguiente, sea G_{bpg} un algoritmo que toma como entrada l^{λ} y devuelve el valor de un parámetro $param_G := (q, G, G_T, g, e)$ de grupos de emparejamientos bilineales con un parámetro de seguridad λ.

A continuación, se describirán espacios vectoriales de emparejamiento doble.

Los espacios vectoriales de emparejamiento doble (q, V, G_T, A, e) pueden estar constituidos por un producto directo de grupos de emparejamientos bilineales simétricos ($param_G := (q, G, G_T, g, e)$). Los espacios vectoriales de emparejamientos dobles (q, V, G_T, A, e) son una tupla de un q primo, un espacio vectorial N-dimensional V sobre F_q indicado en la fórmula 115, un grupo cíclico G_T del orden q y una base canónica $A := (a_1, \ldots, a_N)$ de un espacio V, y tienen las siguientes operaciones (1) y (2), donde a_i es como se indica mediante la fórmula 116.

[Fórmula 115]

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

[Fórmula 116]

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

Operación (1): Emparejamiento bilineal no degenerado

El emparejamiento en el espacio V está definido por la fórmula 117.

[Fórmula 117]

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

donde

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

Esto 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)$^{\delta ij}$, donde δ_{ij} = 1 si i = j, y δ_{ij} = 0 si i ≠ j. Asimismo e (g, g) ≠ 1 ∈ G_T.

Operación (2): Mapas de Distorsión

La transformación lineal Φi,j en el espacio V indicado en la fórmula 118 puede llegar a la fórmula 119.

[Fórmula 118]

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

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

[Fórmula 119]

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

Se debe observar que

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

La transformación lineal Φi,j se llamará mapas de distorsión.

En la siguiente descripción, sea G_{dpvs} un algoritmo que toma como entrada, l^{λ} (λ ∈ números naturales), N ∈ números naturales, y los valores del parámetro $param_G := (q, G, G_T, g, e)$ de los grupos de emparejamientos bilineales, y devuelve el valor de un parámetro $param_v := (q, V, G_T, A, e)$ de pares de vectores de emparejamientos dobles que tienen un parámetro de seguridad λ, y que forman un espacio N-dimensional V.

Se describirá un caso en el que los espacios vectoriales de emparejamientos dobles se construyen a partir de los grupos de emparejamientos bilineales simétricos descritos anteriormente. También se pueden construir espacios vectoriales de emparejamientos dobles a partir de grupos de emparejamientos bilineales asimétricos. La siguiente descripción se puede aplicar fácilmente a un caso en el que los espacios vectoriales de emparejamientos dobles se construyen a partir de grupos de emparejamientos bilineales asimétricos.

<2. Concepto para implementar la encriptación funcional>

<2-1. Programa de amplitud cuadrática>

La figura 1 es un dibujo explicativo de un programa de amplitud cuadrática.

El programa de amplitud cuadrática sobre el campo F_q incluye dos conjuntos de polinomios, es decir, un conjunto A = $\{a_i(x) \mid i \in \{0, ..., L\}\}$ y un conjunto B = $\{b_i(x) \mid i \in \{0, ..., L\}\}$, y un polinomio objetivo d(x). El programa de amplitud cuadrática incluye una etiqueta ρ de un conjunto I := {1, ..., L}. Todas las etiquetas ρ_i (i = 1, …, L) están relacionadas cada una con un literal de $\{p_0, p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$ concretamente, $\rho : I \rightarrow \{p_0, p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$.

Para una entrada $u := (u_1, ..., u_n) \in \{0, 1\}^r$, se establece un valor verdadero T del literal a partir de $T(p_j) := u_j$ y $T(\neg p_j) := \neg u_j$ relativo a cada entero j de j = 1, …, n. Para cualquier entrada u, 1 se configura como el valor verdadero T de p_0, concretamente, T (p_0) := 1.

Un subconjunto I_u del conjunto I se construye a partir de los elementos de una etiqueta para la cual se configura 1 sobre la entrada u. Concretamente $I_u := \{i \in I \mid T(p(i) = 1)\}$. Alternativamente, $I_u := \{i \in I \mid [\rho(i) = p_j \wedge u_j = 1] \vee [\rho(i) = \neg p_j \wedge u_j = 0] \vee [\rho(i) = p_0]\}$.

La figura 2 es un dibujo explicativo del subconjunto I_u.

Se debe observar que en la figura 2, n = 7 y L = 6. Asimismo, en la figura 2, supóngase que las etiquetas ρ están relacionadas de tal manera que forma que ρ_1 corresponde a $\neg p_2$, ρ_2 a p_1, ρ_3 a p_4, ρ_4 a $\neg p_5$, ρ_5 a $\neg p_3$ y ρ_6 a p_5.

Mirando la entrada $u := (u_1, ..., u_7) \in \{0, 1\}^7$, supóngase que $u_1 = 1$, $u_2 = 0$, $u_3 = 1$, $u_4 = 0$, $u_5 = 0$, $u_6 = 1$, y $u_7 = 1$. En este caso, el subconjunto I_u consta de elementos i de etiquetas ρ_i relacionados con los literales $(p_1, p_3, p_6, p_7, \neg p_2, \neg p_4, \neg p_5)$ rodeados por líneas discontinuas. Es decir, el subconjunto I_u consta de los elementos i de las etiquetas ρ_1, ρ_2 y ρ_4, de manera que el subconjunto I_u := {i = 1, 2, 4}

El programa de amplitud cuadrática acepta la entrada u ∈ $\{1, 0\}^n$ (o acepta el subconjunto I_u) si y solo si existe una tupla de (α_1, ..., α_L) y (β_1, …, β_L) donde $\alpha_i = 0 = \beta_i$ relativo a cada i no está incluido en el subconjunto I_u, siendo la tupla de (α_1, ..., α_L) y (β_1, …, β_L) una tupla sobre un campo F_q^L en el que el polinomio d(x) divide la fórmula 120.

De lo contrario, el programa de amplitud cuadrática rechaza la entrada u ∈ $\{1, 0\}^n$.

[Fórmula 120]

$$\left(a_0(x) + \sum_{i=1}^{L} \alpha_i \cdot a_i(x)\right) \cdot \left(b_0(x) + \sum_{i=1}^{L} \beta_i \cdot b_i(x)\right)$$

Es decir, el programa de amplitud cuadrática acepta la entrada u ∈ $\{1, 0\}^n$ si y solo si existe una tupla de α_i y β_i relativa a i ∈ I_u en la que el polinomio objetivo d(x) divide la fórmula 121.

[Fórmula 121]

$$\left(a_0(x) + \sum_{i \in \mathcal{I}} \alpha_i \cdot a_i(x)\right) \cdot \left(b_0(x) + \sum_{i \in \mathcal{I}} \beta_i \cdot b_i(x)\right)$$

Si el programa de amplitud cuadrática acepta la entrada $u \in \{1, 0\}^n$, la tupla de α_i y β_i relativa a $i \in I_u$ es calculable en tiempo polinomial (véase la Bibliografía no de Patente 6).

Con el ejemplo mostrado en la figura 2, el programa de amplitud cuadrática acepta la entrada $u \in \{1, 0\}^n$ si y solo si existe una tupla de α_i y β_i relativa a $i \in I_u := \{i = 1, 2, 4\}$ en la que el polinomio objetivo d(x) divide la fórmula 121.

[Fórmula 122]

$$\left(a_0(x) + \sum_{i \in \{1,2,4\}} \alpha_i \cdot a_i(x)\right) \cdot \left(b_0(x) + \sum_{i \in \{1,2,4\}} \beta_i \cdot b_i(x)\right)$$

<2-2. Producto interior de atributos y programa de amplitud cuadrática>

U_t (t = 1, …, d y $U_t \subset \{0, 1\}^*$) es un sub-universo y un conjunto de atributos. Each U_t incluye información de identificación (t) del sub-universo y la información de atributos $(\vec{v})$ expresada como un vector n-dimensional. Concretamente, U_t es $(t, \vec{v})$ donde $t \in \{1, ..., d\}$ y $\vec{v} \in F_q^n$.

Sea $U_t := (t, \vec{v})$ p, es decir $p := (t, \vec{v})$. Se dará una explicación sobre un método para determinar el subconjunto I_u, en un programa de amplitud cuadrática Q := (A, B, d(x), ρ) mediante $p_j := (t, \vec{v}_j)$ $(j = 1, ..., n; t \in \{1, \ldots, d\})$.

Sea una estructura de acceso S un programa de amplitud cuadrática Q := (A, B, d(x), ρ) que acompaña a p_0 y $\{p_j := (t, \vec{v}_j)\}_{j=1,...,n}$. Esto es, $\rho : \{1, \ldots, L\} \rightarrow \{p_0, (t, \vec{v}_1), ..., (t, \vec{v}_n), \neg(t, \vec{v}_1), ..., \neg(t, \vec{v}_n)\}$. Sea Γ un conjunto de atributos, es decir, que $\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in F_q^n, 1 \le t \le d\}$. Debe observarse que t es un subconjunto de {1, …, d} y no tiene que ser todos los índices.

Cuando un conjunto de atributos Γ es proporcionado a la estructura de acceso S, un valor verdadero T de los lectores $\{p_0, p_1, ..., p_n, \neg p_1, ..., \neg p_n\}$ se determina como sigue. $T(p_j) := 1$ si y solo si $p_j = (t, \vec{v}_j)$ y $(t, \vec{v}_t) \in \Gamma \quad \vec{v}_j \cdot \vec{x}_t \in 0.$ $T(\neg p_j) := 1$ si y solo si $p_j = \neg(t, \vec{v}_j)$ y $(t, \vec{x}_j) \in \Gamma$ $\vec{v}_j \cdot \vec{x}_t \neq 0.$ $T(p_0) := 1$. De lo contrario, el valor verdadero de T es 0.

Asimismo, $I_u (= I_{(\rho,\Gamma)} := \{i \in I \mid T(\rho(i)) = 1\}$ esto es $I_{(\rho,\Gamma)} := \{i \in I \mid [\rho(i) = (t, \vec{v}_j) \wedge (t, \vec{x}_t) \in \Gamma \wedge (\vec{v}_j \cdot \vec{x}_t) = 0] \vee [(\rho(i) = \neg(t, \vec{v}_j) \wedge (t, \vec{x}_j) \in \Gamma \wedge \vec{v}_j \cdot \vec{x}_t \neq 0] \vee [\rho(i) = p_0]\}$.

<3. Esquema del esquema de encriptación funcional>

Un esquema de encriptación funcional está constituido permitiendo que una de una clave de desencriptación y un texto cifrado tengan la estructura de acceso S descrita anteriormente, y la otra tenga el conjunto de atributos Γ.

Un esquema de encriptación funcional en el que una clave de desencriptación tiene una estructura de acceso S se denomina esquema de encriptación funcional de política de claves (KP-FE) y un esquema de encriptación en el que un texto cifrado tiene una estructura de acceso S se denomina esquema de encriptación funcional de política de texto cifrado (CP-FE).

Se describirán las estructuras del esquema KP-FE y del esquema CP-FE y las estructuras de los sistemas criptográficos 10 que ejecutan los respectivos esquemas.

<3-1. Esquema KP-FE>

El esquema KP-FE consiste en cuatro algoritmos: Setup, KeyGen, Enc y Dec.

(Setup)

El algoritmo Setup es un algoritmo aleatorio que toma como entrada un parámetro de seguridad λ y devuelve los parámetros públicos pk y una clave principal sk.

(KeyGen)

El algoritmo KeyGen es un algoritmo aleatorio que toma como entrada una estructura de acceso S, los parámetros públicos pk y la clave principal sk, y devuelve una clave de desencriptación sk_s.

(Enc)

El algoritmo Enc es un algoritmo aleatorio que toma como entrada un mensaje msg, un conjunto de atributos $\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in \mathbf{F}_q^n, 1 \leq t \leq d\}$ y los parámetros públicos pk, y devuelve un texto cifrado ct_Γ.

(Dec)

El algoritmo Dec es un algoritmo que toma como entrada el texto cifrado ctr_Γ encriptado bajo el conjunto de atributos Γ, la clave de desencriptación sk_s para la estructura de acceso S y los parámetros públicos pk, y devuelve el mensaje msg o el símbolo distinguido $\perp$.

La figura 3 es un diagrama de configuración de un sistema criptográfico 10 que ejecuta el esquema KP-FE.

El sistema criptográfico 10 está provisto de un dispositivo de generación de claves 100, un dispositivo de encriptación 200 y un dispositivo de desencriptación 300.

El dispositivo de generación de claves 100 ejecuta el algoritmo Setup tomando como entrada un parámetro de seguridad λ, y genera parámetros públicos pk y una clave principal sk. El dispositivo de generación de claves 100 divulga los parámetros públicos pk generados. El dispositivo de generación de claves 100 ejecuta asimismo el algoritmo KeyGen tomando como entrada una estructura de acceso S, genera una clave de desencriptación sk_s y distribuye la clave de desencriptación sk_s al dispositivo de desencriptación 300 en secreto.

El dispositivo de encriptación 200 ejecuta el algoritmo Enc tomando como entrada un mensaje msg, un conjunto de atributos Γ, y los parámetros públicos pk, y genera un texto cifrado ct_Γ. El dispositivo de encriptación 200 transmite el ct_Γ del texto cifrado generado al dispositivo de desencriptación 300.

El dispositivo de desencriptación 300 ejecuta el algoritmo Dec tomando como entrada los parámetros públicos pk, la clave de desencriptación sk_s y el texto cifrado ct_Γ y emite un mensaje msg o símbolo distinguido $\perp$.

<3-2. Esquema CP-FE>

El esquema CP-FE consiste en cuatro algoritmos: Setup, KeyGen, Enc y Dec.

(Setup)

El algoritmo Setup es un algoritmo aleatorio que toma como entrada un parámetro de seguridad λ y devuelve parámetros públicos pk y una clave principal. sk.

(KeyGen)

El algoritmo KeyGen es un algoritmo aleatorio que toma como entrada un conjunto de atributos $\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in \mathbf{F}_q^n, 1 \leq t \leq d\}$, los parámetros públicos pk y la clave principal sk, y devuelve una clave de desencriptación sk_s.

(Enc)

El algoritmo Enc es un algoritmo aleatorio que toma como entrada un mensaje msg, una estructura de acceso S, y los parámetros públicos pk, y devuelve un texto cifrado ct_s.

(Dec)

El algoritmo Dec es un algoritmo que toma como entrada el texto cifrado ct_s encriptado bajo la estructura de acceso S, una clave de desencriptación sk_Γ para el conjunto de atributos Γ y los parámetros públicos pk, y devuelve un mensaje msg o un símbolo distinguido $\perp$.

La figura 4 es un diagrama de configuración de un sistema de procesamiento criptográfico 10 que ejecuta el esquema CP-FE.

El sistema de procesamiento criptográfico 10 está provisto de un dispositivo de generación de claves 100, un dispositivo de encriptación 200 y un dispositivo de desencriptación 300.

El dispositivo de generación de claves 100 ejecuta el algoritmo Setup tomando como entrada el parámetro de seguridad λ y genera parámetros públicos pk y una clave principal sk. El dispositivo de generación de claves 100 divulga los parámetros públicos pk generados. El dispositivo de generación de claves 100 ejecuta asimismo el algoritmo KeyGen tomando como entrada un conjunto de atributos Γ, genera una clave de desencriptación sk_Γ y distribuye la clave de desencriptación sk_Γ al dispositivo de desencriptación 300 en secreto.

El dispositivo de encriptación 200 ejecuta el algoritmo Enc tomando como entrada un mensaje msg, una estructura de acceso S, y los parámetros públicos pk, y genera un texto cifrado ct_s. El dispositivo de encriptación 200 transmite el texto cifrado ct_s generado al dispositivo de desencriptación 300.

El dispositivo de desencriptación 300 ejecuta el algoritmo Dec tomando como entrada los parámetros públicos pk, la clave de desencriptación sk_Γ y el texto cifrado ct_s, y emite un mensaje msg o un símbolo distinguido $\perp$.

Tanto en el esquema KP-FE como en el esquema CP-FE, con el algoritmo Dec, basado en la estructura de acceso S y el conjunto de atributos Γ, se selecciona un subconjunto $I_{(\rho, \Gamma)}$ mediante el método descrito anteriormente y además se especifica un coeficiente $(\alpha_1, ..., \alpha_L)$ y un coeficiente $(\beta_1, ..., \beta_L)$. En base al subconjunto $I_{(\rho, \Gamma)}$, el coeficiente $(\alpha_1, ..., \alpha_L)$ y el coeficiente $(\beta_1, ..., \beta_L)$ el texto cifrado ct_Γ (o ct_s) es desencriptado y se calcula el mensaje msg.

Normalmente, el algoritmo Setup se ejecuta solo una vez en la configuración del sistema. El algoritmo KeyGen se ejecuta cada vez que se debe generar la clave de desencriptación del usuario. El algoritmo Enc se ejecuta cada vez que se debe encriptar el mensaje msg. El algoritmo Dec se ejecuta cada vez que se debe desencriptar el texto cifrado.

En el sistema criptográfico 10 según la realización 1, el esquema de encriptación funcional se constituye utilizando la estructura de acceso S que está basada en el programa de amplitud cuadrática. Como resultado, un rango ideal puede expresarse como una relación R.

Realización 2.

En la realización 2, se dará una explicación sobre un ejemplo de configuración de un esquema de encriptación funcional que utiliza un programa de amplitud cuadrática.

El esquema KP-FE es el ejemplo que se va a explicar.

La figura 5 es un diagrama de configuración de un dispositivo de generación de claves 100 según la realización 2. La figura 6 es un diagrama de configuración de un dispositivo de encriptación 200 según la realización 2. La figura 7 es un diagrama de configuración de un dispositivo de desencriptación 300 según la realización 2.

Las figuras 8 y 9 son diagramas de flujo que muestran el funcionamiento del dispositivo de generación de claves 100, en el que la figura 8 es un diagrama de flujo que muestra el proceso del algoritmo Setup, y la figura 9 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen. La figura 10 es un diagrama de flujo que muestra el funcionamiento del dispositivo de encriptación 200, que es el proceso del algoritmo Enc. La figura 11 es un diagrama de flujo que muestra el funcionamiento del dispositivo de desencriptación 300, que es el proceso del algoritmo Dec.

Se describirá la función y el funcionamiento del dispositivo de generación de claves 100.

El dispositivo de generación de claves 100 está provisto de una parte de generación de clave principal 110, una parte de almacenamiento de clave principal 120, una parte de entrada de información 130, una parte de generación de claves de desencriptación 140 y una parte de distribución de claves 150. La parte de generación de claves de desencriptación 140 está provista de una parte de generación de información secreta 141 y una parte de generación de elemento clave 142.

El proceso del algoritmo Setup se describirá haciendo referencia a la figura 8.

(S101: Etapa de generación de base ortogonal)

Con el dispositivo de procesamiento, la parte de generación de clave principal 110 calcula la fórmula 123, para generar parámetros param, bases B_0 y B^*_0, y bases B_t y B^*_t.

[Fórmula 123]

(1) entrada I^λ

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

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

(4)

$$n_0 := 2mf_{\max} + 1,$$
$$n_t := 2mf_{\max}k_{\max} + n \ (t = 1,...,d)$$

$$N_0 := n_0 + u_0 + w_0 + z_0,$$
$$N_t := n_t + u_t + w_t + z_t \ (t = 1,...,d)$$

Los procesos (5) a (9) se ejecutan para cada t de t = 0, …, d.

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

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

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

(8)

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

(9)

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

(10)

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

Concretamente, la parte de generación de clave principal 110 ejecuta los siguientes procesos.

(1) Con el dispositivo de entrada, la parte de generación de clave principal 110 toma como entrada el parámetro de seguridad λ (1^λ).

(2) Con el dispositivo de entrada, la parte de generación de clave principal 110 ejecuta el algoritmo G_{bpg} tomando como entrada el parámetro de seguridad λ introducido en (1), y genera el valor de los parámetros $\text{param}_G := (q, G, G_T, g, e)$ de los grupos de emparejamientos bilineales.

(3) Con el dispositivo de procesamiento, la parte de generación de clave principal 110 genera un número aleatorio Ψ.

(4) La parte de generación de clave principal 110 configura $n_0 + u_0 + w_0 + z_0$ en N_0, y configura $n_t + u_t + w_t + z_t$ en N_t para cada entero t de t = 1, …, d (d es un entero igual o mayor que 1). Se debe observar que n_0 es $2mf_{max} + 1$ y n_t es $2mf_{max}k_{max} + n$ donde: m es el número de factores obtenidos mediante factorización del polinomio objetivo d(x); f_{max} es el valor máximo (valor máximo de f_T que se describirá más adelante) de los grados de los factores obtenidos mediante la factorización del polinomio d(x) objetivo; k_{max} es el valor máximo del número de etiquetas ρ relacionadas con una parte de información de identificación t; n es un número entero mayor o igual que 1; y u_0, w_0, z_0, u_t, w_t y z_t son cada uno un entero mayor o igual que 0.

Posteriormente, la parte de generación de clave principal 110 ejecuta los siguientes procesos (5) a (9) relativos a cada entero t de t = 0, …, d.

(5) Con el dispositivo de procesamiento, la parte de generación de clave principal 110 ejecuta el algoritmo G_{dpva} tomando como entrada el parámetro de seguridad λ introducido en (1), N_t configurado en (4) y los valores de $param_G := (q, G, G_T, g, e)$ generados en (2), y genera los valores de los parámetros $param_{vt} := (q, V_t\ G_T, A_t, e)$ de los espacios vectoriales de emparejamientos dobles.

(6) Con el dispositivo de procesamiento, la parte de generación de claves 110 toma como entrada N_t configurada en (4), y F_q, y genera la transformación lineal $Xt := (\chi_{t,i,j})_{i,j}$ aleatoriamente. Se debe observar que GL quiere decir Grupo Lineal. concretamente, GL es un grupo lineal general, un conjunto de matrices cuadradas en las que el determinante no es 0, y un grupo con respecto a la multiplicación. Se debe observar que $(\chi_{t,i,j})_{i,j}$ significa una matriz relativa a los sufijos i y j de una matriz $\chi_{t,i,j}$, donde i, j = 1, …, N_t.

(7) Con el dispositivo de procesamiento y en base al número aleatorio Ψ y la transformación lineal X_t, la parte de generación de clave principal 110 genera $X^*_t := (v_{t,i,j})_{i,j} := \Psi \cdot (X_t^T)^{-1}$. Al igual que $(\chi_{t,i,j})_{i,j}$, $(v_{t,i,j})_{i,j}$ significa una matriz relativa a los sufijos i y j de una matriz $v_{t,i,j}$ donde i, j = 1,..., N_t.

(8) Con el dispositivo de procesamiento y basándose en la transformación lineal X_t generada en (6), la parte de generación de clave principal 110 genera una base B_t a partir de la base canónica A_t generada en (5). Se debe observar que $\vec{x}_{t,i}$ indica la fila de orden i de la transformación lineal X_t.

(9) Con el dispositivo de procesamiento y basándose en la transformación lineal X^*_t generada en (7), la parte de generación de clave principal 110 genera una base B^*_t a partir de la base canónica A_t generada en (5). Se debe observar que $\vec{v}_{t,i}$ indica la fila de orden i de la transformación lineal X^*_t.

(10) Con el dispositivo de procesamiento, la parte de generación de clave principal 110 configura e $(g, g)_\Psi$, en g_T. La parte de generación de clave principal 110 establece asimismo g_t y $\{param_{vt}\}_{t=0,...,d}$ generados en (5), en param.

En resumen, en (S101), la parte de generación de clave principal 110 ejecuta el algoritmo G_{ob} indicado en la fórmula 124, y genera param, las bases B_0 y B^*_0, y las bases B_t y B^*_t.

[Fórmula 124]

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

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

$$n_0 := 2mf_{max} + 1, \quad n_t := 2mf_{max}k_{max} + n\ (t = 1,...,d),$$

$$N_0 := n_0 + u_0 + w_0 + z_0,\ N_t := n_t + u_t + w_t + z_t\ (t = 1,...,d),$$

para $t = 0,...,d,$

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

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

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

, a continuación, en esta memoria, $\vec{\chi}_{t,i}$ y $\vec{\vartheta}_{t,i}$ indican las filas de orden i de X_t y X^*_t para i = 1, …, N_t, respectivamente,

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

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

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

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

(S102: Etapa de generación de parámetros públicos)

Con el dispositivo de procesamiento, la parte de generación de clave principal 110 genera las subbases $B^\wedge_0$ y $B^\wedge_t$ de las bases B_0 y B_t, respectivamente, que se generan en (S101), tal como se indica en la fórmula 125.

[Fórmula 125]

$$\hat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,n_0+u_0+w_0+1}, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}),$$

$$\hat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n}, \boldsymbol{b}_{t,n_t+u_t+w_t+1}, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t+z_t}) \quad \text{para t = 1, …, d}$$

La parte de generación de clave principal 110 trata las subbases generadas B^$_0$ y B^$_t$, el parámetro de seguridad λ introducido en (S101), y el param generado en (S101), para formar los parámetros públicos pk.

(S103: Etapa de generación de clave principal)

Con el dispositivo de procesamiento, la parte de generación de clave principal 110 genera las subbases B^*$_0$ y B^*$_t$, de las bases B*$_0$ y la base B*$_t$, respectivamente, que se generan en (S101), tal como se indica en la fórmula 126.

[Fórmula 126]

$$\hat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \ldots, \boldsymbol{b}_{0,n_0}^*, \boldsymbol{b}_{0,n_0+u_0+1}^*, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0}^*, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^*),$$

$$\hat{\mathbb{B}}_t^* := (\boldsymbol{b}_{t,1}^*, \ldots, \boldsymbol{b}_{t,n_t}^*, \boldsymbol{b}_{t,n_t+u_t+1}^*, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t}^*) \quad \text{para t = 1, …, d}$$

La parte de generación de la clave principal 110 trata las subbases B^*$_0$ y B^*$_t$, para formar la clave principal sk.

(S104: Etapa de almacenamiento de la clave principal)

La parte de almacenamiento de la clave principal 120 almacena los parámetros públicos pk generados en (S102), en el dispositivo de almacenamiento. La parte de almacenamiento de la clave principal 120 almacena asimismo la clave principal generada en (S103), en el dispositivo de almacenamiento.

Brevemente, de (S101) a (S103), el dispositivo de generación de claves 100 genera los parámetros públicos pk y principal sk ejecutando el algoritmo Setup indicado en la fórmula 127. A continuación, en (S104), el dispositivo de generación de claves 100 almacena los parámetros públicos pk generados y la clave principal sk, en el dispositivo de almacenamiento.

Se debe observar que los parámetros públicos se publican a través, por ejemplo, de una red, de modo que el dispositivo de encriptación 200 y el dispositivo de desencriptación 300 pueden obtenerlos.

[Fórmula 127]

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

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

$$\hat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,n_0+u_0+w_0+1}, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}),$$

$$\hat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n}, \boldsymbol{b}_{t,n_t+u_t+w_t+1}, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t+z_t}) \quad \text{para t = 1, …, d,}$$

$$\hat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \ldots, \boldsymbol{b}_{0,n_0}^*, \boldsymbol{b}_{0,n_0+u_0+1}^*, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0}^*, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^*),$$

$$\hat{\mathbb{B}}_t^* := (\boldsymbol{b}_{t,1}^*, \ldots, \boldsymbol{b}_{t,n_t}^*, \boldsymbol{b}_{t,n_t+u_t+1}^*, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t}^*) \quad \text{para t = 1, …, d,}$$

devolver $\mathsf{pk} := (1^\lambda, \{\hat{\mathbb{B}}_t\}_{t=0,\ldots,d}, \mathsf{param}), \quad \mathsf{sk} := \{\hat{\mathbb{B}}_t^*\}_{t=0,\ldots,d}$.

El proceso del algoritmo KeyGen se describirá haciendo referencia a la figura 9.

(S201: Etapa de introducción de información)

Con el dispositivo de entrada, la parte de entrada de información 130 toma como entrada la estructura de acceso S := (A, B, d(x), ρ) descrita anteriormente. Se debe observar que la información de los atributos del usuario de la clave

de desencriptación sk_s se configura en ρ. El polinomio objetivo d(x) incluido en la estructura de acceso S puede factorizarse en m de factores $d_\tau(x)^{f_\tau}$ donde τ = 1, ..., m, tal como se indica en la fórmula 128.

[Fórmula 128]

$$d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau}$$

(S202: Etapa de generación de información secreta π)

Con el dispositivo de procesamiento, la parte de generación de información secreta 141 genera información secreta $\pi_{\tau,\kappa,0}$ e información secreta $\pi_{\tau,\kappa,1}$ tal como se indica en la fórmula 129.

[Fórmula 129]

$$\pi_\tau \xleftarrow{U} \mathbb{F}_q,\ (\tau=1,...,m-1),\ \ \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{U} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,...,m;\ \ \kappa=0,...,f_\tau)$$

(S203: Etapa de generación de información secreta χ)

Con el dispositivo de procesamiento, la parte de generación de información secreta 141 genera información secreta $\chi_{\tau,\kappa,1}$ tal como se indica en la fórmula 130.

[Fórmula 130]

$$\chi_\tau \xleftarrow{U} \mathbb{F}_q,\ (\tau=1,...,m-1),\ \ \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{U} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,...,m;\ \ \kappa=0,...,f_\tau)$$

(S204: Etapa de generación de información secreta s)

Con el dispositivo de procesamiento, la parte de generación de información secreta 141 genera la información secreta $s_0^{(\tau,\kappa,0)}$ y la información secreta $s_0^{(\tau,\kappa,1)}$, así como la información secreta $s_i^{(\tau,\kappa,0)}$ y la información secreta $s_i^{(\tau,\kappa,1)}$, tal como se indica en la fórmula 131.

[Fórmula 131]

para $\tau=1,...,m,\ \ \kappa=0,...,f_\tau,\ \ \iota=0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ \ (\kappa=0,...,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x + \cdots + a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)} x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x + \cdots + b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)} x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{U} \mathbb{F}_q,\ \left(j=0,...,\mu^{(\tau,\kappa,\iota)}-1\right),$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{0,j}^{(\tau,\kappa)},$$

para $i=1,...,L,$

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q \quad (i=1,...,L;\ \tau=1,...,m-1;\iota=0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota} \quad (i=1,...,L;\ \iota=0,1),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1}$$

(S205: Etapa de generación de elemento de clave)

Con el dispositivo de procesamiento, con respecto a cada entero τ de τ = 1, …, m, cada entero κ de κ = 0, ..., f_τ, y cada entero ι de ι = 0, 1, la parte de generación de elemento de clave 142 genera un elemento $k^*_0{}^{(\tau,\kappa,\iota)}$ de la clave de desencriptación sk_s, tal como se indica en la fórmula 132.

[Fórmula 132]

$$\vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$

$$\boldsymbol{k}_0^{*(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,...,0}^{u_0},\ \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)}}^{w_0},\ \overbrace{0,...,0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\ \mathbb{B}_0^*$$

Tal como se ha descrito anteriormente, para las bases B y B* indicadas en la fórmula 113, se establece la fórmula 114. Por lo tanto, la fórmula 132 significa que: $s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota}$ se configura, como el coeficiente para un vector de base $b^*_{0,1}$ de una base B^*_0; $\vec{e}_0^{(\tau,\kappa,\iota)}$ se configura como el coeficiente para los vectores de base $b^*_{0,1+1}$, …, $b^*_{0,1+n0}$ de la base B^*_0; 0 se configura como el coeficiente para los vectores de base $b^*_{0,n0+1}$,…, $b^*_{0,n0+u0}$, de la base B^*_0; $\eta_{0,1}^{(\tau,\kappa,\iota)}$, …, $\eta_{0,w0}^{(\tau,\kappa,\iota)}$ son configurados cada uno como coeficiente para los vectores de base $b^*_{0,n0+u0+1}$, …, $b^*_{0,n0+u0+w0}$, de la base B^*_0; y 0 se configura como el coeficiente de los vectores de base $b^*_{0,n0+u0+w0+1}$, …, $b^*_{0,n0+u0+w0+z0}$ de la base B^*_0. Se debe observar que n0, u0, w0 y z0 representan respectivamente n_0, u_0, w_0 y z_0.

Asimismo, $\vec{e}_0^{(\tau,\kappa,\iota)}$ es un vector de $2mf_{max}$ dimensiones en el que 1 se configura como el coeficiente para un vector de base y 0 se configura como el coeficiente para otro vector de base, y el vector de base para el que 1 se configura como el coeficiente difiere para cada (τ,κ,ι).

De igual modo, $\vec{e}_0^{(\tau,\kappa,\iota)}$ es un vector de $2mf_{max}k_{max}$ dimensiones en el que 1 se configura como el coeficiente para un vector de base y 0 se configura como el coeficiente para otro vector de base, y el vector de base para el cual 1 se configura como el coeficiente difiere para cada (τ,κ,ι).

Asimismo, $\vec{e}_1$ es un vector n-dimensional en el que 1 se configura como el coeficiente para el vector de base $b^*_{t,l}$ y 0 se configura como el coeficiente para otro vector de base.

Con el dispositivo de procesamiento, con respecto a cada entero τ de τ = 1, …, m, cada número entero de κ de κ = 0, …, f_t y cada entero ι de ι = 0, 1, y cada entero i de i = 1, …, L, la parte de generación de elemento de clave 142 genera un elemento $k^*i^{(\tau,\kappa,\iota)}$ de la clave de desencriptación sk_s, tal como se indica en la fórmula 133.

[Fórmula 133]

Si $\rho(i) = (t, \vec{v}_i), \quad \theta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{e}_1 + \theta_i\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,...,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,...,0}^{z_t})\ \mathbb{B}_t^*,$$

si $\rho(i) = \neg(t, \vec{v}_i), \quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$k_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_\iota},\ \overbrace{0,...,0,}^{u_\iota}\ \overbrace{\vec{\eta}_i,}^{w_\iota}\ \overbrace{0,...,0}^{z_\iota})\ \mathbb{B}_i^*\ ,$$

si $\rho(i) = p_0, \qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_0},$

$$k_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,...,0,}^{u_0}\ \overbrace{\vec{\eta}_i,}^{w_0}\ \overbrace{0,...,0}^{z_0})\ \mathbb{B}_0^*$$

(S206: Etapa de distribución de claves)

Por ejemplo, con el dispositivo de comunicación, la parte de distribución de claves 150 distribuye la clave de desencriptación sk_s, constituida como elementos mediante la estructura de acceso S introducida en (S201) y $k^{*(\tau,\kappa,\iota)}_0, k^{*(\tau,\kappa,\iota)}_1, ..., k^{*(\tau,\kappa,\iota)}_L$, generada en (S205), al dispositivo de desencriptación 300 en secreto a través de la red. Por supuesto, la clave de desencriptación sk_s se puede distribuir al dispositivo de desencriptación 300 mediante otro método.

Brevemente, de (S201) a (S205), el dispositivo de generación de claves 100 genera la clave de desencriptación sk_s ejecutando el algoritmo KeyGen indicado en las fórmulas 134 a 135. A continuación, en (S206) el dispositivo de generación de claves 100 distribuye la clave de desencriptación generada sk_s al dispositivo de desencriptación 300.

[Fórmula 134]

$$\text{KeyGen}\left(\text{pk, sk, } \mathbb{S} := (\mathcal{A}, \mathcal{B}, d(x) = \prod_{\tau=1}^{m} d_\tau(x)^{f_\tau}, \rho)\right):$$

$$\pi_\tau \xleftarrow{\cup} \mathbb{F}_q,\ (\tau = 1,...,m-1),\ \pi_m := -\sum_{\tau=1}^{m-1} \pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\cup} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau = 1,...,m;\ \kappa = 0,...,f_\tau),$$

$$\chi_\tau \xleftarrow{\cup} \mathbb{F}_q,\ (\tau = 1,...,m-1),\ \chi_m := 1 - \sum_{\tau=1}^{m-1} \chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\cup} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau = 1,...,m;\ \kappa = 0,...,f_\tau),$$

para $\tau = 1,...,m,\ \kappa = 0,...,f_\tau,\ \iota = 0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ (\kappa = 0,...,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x + \cdots + a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)} x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x + \cdots + b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)} x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q,\ (j = 0,...,\mu^{(\tau,\kappa,\iota)} - 1),\ \vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{0,j}^{(\tau,\kappa)},$$

[Fórmula 135]

$$k_0^{*(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,...,0,}^{u_0}\ \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)},}^{w_0}\ \overbrace{0,...,0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\ \mathbb{B}_0^*\ ,$$

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

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q \quad (i = 1, \ldots, L;\ \tau = 1, \ldots, m-1; \iota = 0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota} \quad (i = 1, \ldots, L;\ \iota = 0,1),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1},$$

si $\rho(i) = (t, \vec{v}_i), \qquad \theta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{e}_1 + \theta_i \vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,\ldots,0}^{z_t})\ \mathbb{B}_t^*,$$

si $\rho(i) = \neg(t, \vec{v}_i), \qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,\ldots,0}^{z_t})\ \mathbb{B}_t^*,$$

si $\rho(i) = p_0, \qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_0},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_i}^{w_0},\ \overbrace{0,\ldots,0}^{z_0})\ \mathbb{B}_0^*,$$

devolver $\mathrm{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_0^{*(\tau,\kappa,\iota)}, \boldsymbol{k}_1^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}).$

Se describirá la función y el funcionamiento del dispositivo de encriptación 200.

El dispositivo de encriptación 200 está provisto de una parte de obtención de parámetros públicos 210, una parte de introducción de información 220, una parte de generación de datos encriptados 230 y una parte de transmisión de datos 240.

El proceso del algoritmo Enc se describirá haciendo referencia a la figura 10.

(S301: Etapa de obtención de parámetros públicos)

Por ejemplo, con el dispositivo de comunicación, la parte de obtención de parámetros públicos 210 obtiene los parámetros públicos pk generados por el dispositivo de generación de claves 100, a través de la red.

(S302: Etapa de introducción de información)

Con el dispositivo de introducción, la parte de introducción de información 220 toma como entrada el mensaje msg que se transmitirá al dispositivo de desencriptación 300. Asimismo, con el dispositivo de entrada, la parte de introducción de información 220 toma como entrada el conjunto de atributos $\Gamma := \{(t, \vec{x}_t := (x_{t,1}, \ldots, x_{t,n} \in \mathbb{F}_q^n)) \mid 1 \leq t \leq d\}$. Se debe observar que no es necesario que todos los números enteros t se encuentren dentro del intervalo de $1 \leq t \leq d$, sino que pueden ser uno o más de los enteros t que se encuentran dentro del intervalo de $1 \leq t \leq d$. Asimismo, por ejemplo, la información de atributos de usuario desencriptables se configura en el conjunto de atributos Γ.

(S303: Etapa de generación de elementos cifrados)

Con el dispositivo de procesamiento, la parte de generación de datos encriptados 230 genera un elemento c_0 del texto cifrado ct_Γ, tal como se muestra en la fórmula 136.

[Fórmula 136]

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

$$\vec{\varphi}_0 \xleftarrow{U} \mathbb{F}_q^{z_0 - 1},$$

$$c_0 := (\overbrace{\omega, 0,...,0,}^{n_0} \overbrace{0,...,0,}^{u_0} \overbrace{0,...,0,}^{w_0} \overbrace{\vec{\varphi}_0, \zeta}^{z_0})\, \mathbb{B}_0$$

Con el dispositivo de procesamiento, con respecto a cada entero t incluido en la información de atributos Γ, la parte de generación de datos encriptados 230 genera un elemento c_t del texto cifrado ct_Γ, tal como se indica en la fórmula 137.

[Fórmula 137]

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

$$c_t := (\overbrace{\omega \vec{x}_t, 0,...,0}^{n_t} \overbrace{0,...,0,}^{u_t} \overbrace{0,...,0,}^{w_t} \overbrace{\vec{\varphi}_t}^{z_t})\, \mathbb{B}_t$$

Con el dispositivo de procesamiento, la parte de generación de datos encriptados 230 genera un elemento c_{d+1} del texto cifrado ct_Γ, tal como se indica en la fórmula 138.

[Fórmula 138]

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

(S304: Etapa de transmisión de datos)

Por ejemplo, con el dispositivo de comunicación, la parte de transmisión de datos 240 transmite el texto cifrado ct_Γ, constituido como elementos mediante el conjunto de atributos Γ introducidos en (S302) y c_0, c_t y c_{d+1} generados en (S303), al dispositivo de desencriptación 300 a través de la red. Por supuesto, el texto cifrado ct_Γ puede ser transmitido al dispositivo de desencriptación 300 por otro método.

Brevemente, de la (S301) a la (S303), el dispositivo de encriptación 200 genera el texto cifrado ctr_Γ ejecutando el algoritmo Enc indicado en la fórmula 139. A continuación, en (S304), el dispositivo de encriptación 200 transmite el texto cifrado ct_Γ generado al dispositivo de desencriptación 300.

[Fórmula 139]

$$\text{Enc}(\text{pk}, msg, \Gamma := \{(t, \vec{x}_t) \mid 1 \le t \le d\}):$$

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

$$\vec{\varphi}_0 \xleftarrow{U} \mathbb{F}_q^{z_0 - 1},$$

$$\vec{\varphi}_t \xleftarrow{U} \mathbb{F}_q^{z_t} \text{ for } (t, \vec{x}_t) \in \Gamma,$$

$$c_0 := (\overbrace{\omega, 0,...,0,}^{n_0} \overbrace{0,...,0,}^{u_0} \overbrace{0,...,0,}^{w_0} \overbrace{\vec{\varphi}_0, \zeta}^{z_0})\, \mathbb{B}_0$$

$$c_t := (\overbrace{\omega \vec{x}_t, 0,...,0}^{n_t} \overbrace{0,...,0,}^{u_t} \overbrace{0,...,0,}^{w_t} \overbrace{\vec{\varphi}_t}^{z_t})\, \mathbb{B}_t, \text{ para } (t, \vec{x}_t) \in \Gamma,$$

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

devolver $\mathrm{ct}_\Gamma := (\Gamma, c_0, \{c_t\}_{(t,\vec{x}_t)\in\Gamma}, c_{d+1})$.

Se describirá la función y el funcionamiento del dispositivo de desencriptación 300.

El dispositivo de desencriptación 300 está provisto de una parte de obtención de información 310, una parte de cálculo del programa de amplitud 320, una parte de cálculo de coeficientes complementarios 330 y una parte de desencriptación 340. La parte de obtención de información 310 está provista de una parte de obtención de clave de desencriptación 311 y una parte de obtención de texto cifrado 312. La parte de cálculo de coeficientes complementarios 330 está provista de una parte de selección polinómica 331 y una parte de cálculo de coeficientes 332. La parte de desencriptación 340 está provista de una parte de operación de emparejamiento 341 y una parte de cálculo de mensajes 342.

El proceso del algoritmo Dec se describirá haciendo referencia a la figura 11.

(S401: Etapa de obtención de clave de desencriptación)

Por ejemplo, con el dispositivo de comunicación, la parte de obtención de clave de desencriptación 311 obtiene la clave de desencriptación $sk_s := (S, k^{*(\tau,\kappa,\iota)}_0, k^{*(\tau,\kappa,\iota)}_1, ..., k^{*(\tau,\kappa,\iota)}_L)$ distribuida por el dispositivo de generación de claves 100, a través de la red. La parte de obtención de clave de desencriptación 311 obtiene asimismo los parámetros públicos pk generados por el dispositivo de generación de claves 100.

(S402: Etapa de obtención de texto cifrado)

Por ejemplo, con el dispositivo de comunicación, la parte de obtención de texto cifrado 312 obtiene el texto cifrado $ct_\Gamma := (\Gamma, c_0, c_t, c_{d+1})$ transmitido por el dispositivo de encriptación 200, a través de la red.

(S403: Etapa de cálculo del programa de amplitud)

Con el dispositivo de procesamiento, la parte de cálculo del programa de amplitud 320 comprueba si la estructura de acceso S incluida en la clave de desencriptación sk_s obtenida en (S401) acepta o no Γ incluido en el texto cifrado ct_Γ obtenido en (S402). El método de comprobar si la estructura de acceso S acepta o no Γ es el mismo que el descrito en "2-1. Programa de amplitud cuadrática en la realización 1".

La parte de cálculo del programa de alcance 320 avanza al proceso de (S404) si la estructura de acceso S acepta Γ (aceptar en S403). Si la estructura de acceso S rechaza Γ (rechazar en S403), la parte de cálculo del programa de amplitud 320 juzga que el texto cifrado ct_Γ no puede desencriptarse y finaliza el proceso.

(S404: Etapa de selección de polinomios)

Con el dispositivo de procesamiento, la parte de selección de polinomios 331 de la parte de cálculo de coeficientes complementarios 330 calcula $I_{(\rho,\Gamma)} \subseteq \{1, ..., L\}$. El método de calcular I(ρ,Γ) es el mismo que el descrito en "2 - 2. Producto interior de atributos y programa de amplitud cuadrática en la realización 1".

(S405: Paso de cálculo de coeficientes)

Con el dispositivo de procesamiento, la parte de cálculo de coeficientes 332 de la parte de cálculo de coeficientes complementarios 330 calcula los coeficientes $(\alpha_1, ..., \alpha_L)$, los coeficientes $(\beta_1, ..., \beta_L)$ y los grados $(\kappa_1, ..., \kappa_m)$ con el que se establece la fórmula 140.

Los coeficientes $(\alpha_1, ..., \alpha_L)$, los coeficientes $(\beta_1, ..., \beta_L)$ y los grados $(\kappa_1, ..., \kappa_m)$ pueden ser calculados por cualquier método, por ejemplo, ida y vuelta.

[Fórmula 140]

$$\prod_{\tau=1}^{m} d_\tau(x)^{\kappa_\tau} \mid (a_0(x) + \sum_{i=1}^{L} \alpha_i a_i(x)),$$ y

$$\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau - \kappa_\tau} \mid (b_0(x) + \sum_{i=1}^{L} \beta_i b_i(x))$$

Obsérvese que $\alpha_i = 0 = \beta_i$ con respecto a todo i no incluido en I(ρ,Γ).

(S406: Etapa de operación de emparejamiento)

La parte de operación de emparejamiento 341 de la parte de desencriptación 340 genera las claves de sesión $K_{\tau,0}$ y $K_{\tau,1}$ calculando la fórmula 141 con el dispositivo de procesamiento.

[Fórmula 141]

$$K_{\tau,0} := e(\boldsymbol{c}_0, \boldsymbol{k}_0^{*(\tau,\kappa_\tau,0)}) \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i} \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i} \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)},$$

$$K_{\tau,1} := e(\boldsymbol{c}_0, \boldsymbol{k}_0^{*(\tau,\kappa_\tau,1)}) \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i} \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i} \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i/(\vec{v}_i\cdot\vec{x}_t)},$$

donde $\mathcal{I}_{(\rho,\Gamma),0} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = p_0\}$,

$\mathcal{I}_{(\rho,\Gamma),+} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = (t,\vec{v}_i)\}$ y

$\mathcal{I}_{(\rho,\Gamma),-} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = \neg(t,\vec{v}_i)\}$

(S407: Etapa de cálculo de mensajes)

La parte de cálculo de mensaje 342 de la parte de desencriptación 340 genera un mensaje msg '(= msg) calculando la fórmula 142 con el dispositivo de procesamiento.

[Fórmula 142]

$$msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0} K_{\tau,1})$$

Se debe observar que mediante el cálculo de la fórmula 141, se puede obtener g_T^{ζ}, tal como se indica en la fórmula 143. Por lo tanto, calculando la fórmula 142, se puede obtener el mensaje msg' (= msg) m.

[Fórmula 143]

$$K_{\tau,0} := e(\boldsymbol{c}_0, \boldsymbol{k}_0^{*(\tau,\kappa_\tau,0)}) \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i}$$
$$\cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i} \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)},$$
$$= g_T^{\omega(\sum_{j=0}^{\mu(\tau,\kappa_\tau,0)-1}\delta_j^{(\tau,\kappa_\tau,0)}a_{0,j}^{(\tau,\kappa_\tau)}+\pi_{\tau,\kappa_\tau,0})+\zeta\chi_{\tau,\kappa_\tau,0}}$$
$$\cdot g_T^{\omega(\sum_{i=1}^{L}\alpha_i\sum_{j=0}^{\mu(\tau,\kappa_\tau,0)-1}\delta_j^{(\tau,\kappa_\tau,0)}a_{i,j}^{(\tau,\kappa_\tau)}+\xi_{i,\tau,0}))}$$
$$= g_T^{\omega(\sum_{j=0}^{\mu(\tau,\kappa_\tau,0)-1}\delta_j^{(\tau,\kappa_\tau,0)}a_{0,j}^{(\tau,\kappa_\tau)}+\pi_{\tau,\kappa_\tau,0})+\zeta\chi_{\tau,\kappa_\tau,0}}$$
$$\cdot g_T^{\omega(\sum_{j=0}^{\mu(\tau,\kappa_\tau,0)-1}\delta_j^{(\tau,\kappa_\tau,0)}\sum_{i=1}^{L}\alpha_i a_{i,j}^{(\tau,\kappa_\tau)}+\alpha_i\xi_{i,\tau,0})}$$
$$= g_T^{\omega(\sum_{j=0}^{\mu(\tau,\kappa_\tau,0)-1}\delta_j^{(\tau,\kappa_\tau,0)}(a_{0,j}^{(\tau,\kappa_\tau)}+\sum_{i=1}^{L}\alpha_i a_{i,j}^{(\tau,\kappa_\tau)})}$$
$$\cdot g_T^{\omega\pi_{\tau,\kappa_\tau,0}+\zeta\chi_{\tau,\kappa_\tau,0}+\omega\sum_{i=1}^{L}\alpha_i\xi_{i,\tau,0}}$$
$$= g_T^{\omega\pi_{\tau,\kappa_\tau,0}+\zeta\chi_{\tau,\kappa_\tau,0}+\omega\sum_{i=1}^{L}\alpha_i\xi_{i,\tau,0}}$$
$$K_{\tau,1} = g_T^{\omega\pi_{\tau,\kappa_\tau,1}+\zeta\chi_{\tau,\kappa_\tau,1}+\omega\sum_{i=1}^{L}\beta_i\xi_{i,\tau,1}}$$
$$\prod_{\tau=1}^{m} K_{\tau,0}K_{\tau,1} = g_T^{\sum_{\tau=1}^{m}(\omega(\pi_{\tau,\kappa_\tau,0}+\pi_{\tau,\kappa_\tau,1})+\zeta(\chi_{\tau,\kappa_\tau,0}+\chi_{\tau,\kappa_\tau,1})+\omega\sum_{i=1}^{L}(\alpha_i\xi_{i,\tau,0}+\beta_i\xi_{i,\tau,1}))}$$
$$= g_T^{\omega(\sum_{\tau=1}^{m}\pi_\tau+\zeta\sum_{\tau=1}^{m}\chi_\tau+\omega\sum_{i=1}^{L}\alpha_i(\sum_{\tau=1}^{m}\xi_{i,\tau,0})+\omega\sum_{i=1}^{L}\beta_i(\sum_{\tau=1}^{m}\xi_{i,\tau,1})}$$
$$= g_T^{\zeta}$$

En resumen, desde (S401) hasta (S407), el dispositivo de desencriptación 300 genera el mensaje msg '(= msg) ejecutando el algoritmo Dec indicado en la fórmula 144.

[Fórmula 144]

$$\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_0^{*(\tau,\kappa,\iota)}, \boldsymbol{k}_1^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}),$$
$$\mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,\vec{x}_t)\in\Gamma}, c_{d+1})):$$

Si $\mathbb{S} := (\mathcal{A}, \mathcal{B}, d(x), \rho)$ acepta $\Gamma := \{(t, \vec{x}_t)\}$,

entonces, calcular $\mathcal{I}_{(\rho,\Gamma)} \subseteq \{1,\ldots,L\}, (\alpha_1,\ldots,\alpha_L),$

$(\beta_1,\ldots,\beta_L)$ con $\alpha_i = 0 = \beta_i$ para todo $i \notin \mathcal{I}_{(\rho,\Gamma)}$, y $(\kappa_1,\ldots,\kappa_m)$ de tal manera que $\prod_{\tau=1}^{m} d_\tau(x)^{\kappa_\tau} \mid (a_0(x) + \sum_{i=1}^{L}\alpha_i a_i(x))$, y $\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau-\kappa_\tau} \mid (b_0(x) + \sum_{i=1}^{L}\beta_i b_i(x))$,

$$K_{\tau,0} := e(\boldsymbol{c}_0, \boldsymbol{k}_0^{*(\tau,\kappa_\tau,0)}) \cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i}$$
$$\cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i} \cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i/(\vec{v}_i \cdot \vec{x}_t)},$$
$$K_{\tau,1} := e(\boldsymbol{c}_0, \boldsymbol{k}_0^{*(\tau,\kappa_\tau,1)}) \cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i}$$
$$\cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i} \cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i/(\vec{v}_i \cdot \vec{x}_t)},$$

donde $\mathcal{I}_{(\rho,\Gamma),0} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = p_0\}$,

$\mathcal{I}_{(\rho,\Gamma),+} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = (t, \vec{v}_i)\}$ y $\mathcal{I}_{(\rho,\Gamma),-} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = \neg(t, \vec{v}_i)\}$.

devolver

$$msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0} K_{\tau,1}).$$

Tal como se describió anteriormente, el sistema criptográfico 10 según la realización 2 implementa el esquema de encriptación funcional que utiliza el programa de amplitud cuadrática.

Mediante la utilización del programa de amplitud cuadrática, se puede expresar un rango más amplio como la relación R.

En particular, en el sistema criptográfico 10 según la realización 2, para cada polinomio $d_\tau(x)^{f\tau}$ obtenido mediante factorización del polinomio objetivo d(x), un elemento que es el resto de dividir un polinomio $a_i(x)$ mediante un polinomio $d_\tau(x)^\kappa$ y un elemento que es un resto de dividir un polinomio $b_i(x)$ por un polinomio $d_\tau(x)^{f\tau-\kappa}$ se tratan como elementos clave $k^*{}_0^{(\tau,\kappa,\iota)}, k^*{}_1^{(\tau,\kappa,\iota)}, \ldots, k^*{}_L^{(\tau,\kappa,\iota)}$. Asimismo, la información secreta π y la información secreta χ se configuran compartiendo en cada elemento clave $k^*{}_0^{(\tau,\kappa,\iota)}$. Utilizando los coeficientes α y β, la operación de emparejamiento de los elementos clave y los elementos encriptados se realiza para poner el resto en cada elemento clave a 0 la información secreta π a 0 ya la información secreta χ a 1, extrayendo de ese modo las claves de sesión $K_{\tau,0}$ y $K_{\tau,1}$, 1 del texto cifrado. Esto implementa el esquema de encriptación funcional que utiliza el programa de amplitud cuadrática.

El esquema KP-FE se ha descrito anteriormente Si el algoritmo KeyGen, el algoritmo Enc y el algoritmo Dec son modificados tal como se indica en las fórmulas 145 a 148, puede realizarse el esquema CP-FE. Se debe observar que el algoritmo Setup es el mismo entre el esquema KP-FE y el esquema CP-FE.

[Fórmula 145]

$$\text{KeyGen}(\text{pk}, \text{sk}, \Gamma := \{(t, \vec{x}_t) \mid 1 \le t \le d\}):$$
$$\omega \xleftarrow{\text{U}} \mathbb{F}_q,$$
$$\vec{\varphi}_0 \xleftarrow{\text{U}} \mathbb{F}_q^{w_0},$$
$$\vec{\varphi}_t \xleftarrow{\text{U}} \mathbb{F}_q^{w_t} \text{ para } (t, \vec{x}_t) \in \Gamma,$$
$$\boldsymbol{k}_0^* := (\overbrace{\omega,}^{n_0}\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{\vec{\varphi}_0,}^{w_0}\ \overbrace{0,\ldots,0,1}^{z_0})\, \mathbb{B}_0^*,$$
$$\boldsymbol{k}_t^* := (\overbrace{\omega\vec{x}_t,}^{n_t}\ \overbrace{0,\ldots,0}^{u_t}\ \overbrace{\vec{\varphi}_t,}^{w_t}\ \overbrace{0,\ldots,0}^{z_t})\, \mathbb{B}_t^*,$$

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

[Fórmula 146]

$$\mathsf{Enc}\left(\mathsf{pk},\ msg,\ \mathbb{S} := (\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho)\right):$$

$$\pi_\tau \xleftarrow{\cup} \mathbb{F}_q,\ (\tau=1,...,m-1),\ \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\cup} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,...,m;\ \kappa=0,...,f_\tau),$$

$$\chi_\tau \xleftarrow{\cup} \mathbb{F}_q,\ (\tau=1,...,m-1),\ \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\cup} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,...,m;\ \kappa=0,...,f_\tau),$$

para $\tau=1,...,m,\ \ \kappa=0,...,f_\tau,\ \ \iota=0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ \ (\kappa=0,...,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x + \cdots + a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)} x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x + \cdots + b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)} x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q,\ \left(j=0,...,\mu^{(\tau,\kappa,\iota)}-1\right),\ \ \vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q^{z_0-1},$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)}\cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)}\cdot b_{0,j}^{(\tau,\kappa)},$$

[Fórmula 147]

$$\boldsymbol{c}_0^{(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)}+\pi_{\tau,\kappa,\iota},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,...,0}^{u_0},\ \overbrace{0,...,0}^{w_0},\ \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)},\ \zeta\chi_{\tau,\kappa,\iota}}^{z_0})\,\mathbb{B}_0\ ,$$

para $i=1,...,L,$

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q\ \left(i=1,...,L;\ \tau=1,...,m-1;\iota=0,1\right),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1}\xi_{i,\tau,\iota}\left(i=1,...,L;\ \iota=0,1\right),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)}\cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)}\cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1},$$

$\rho(i) = (t, \vec{v}_i), \quad \theta_i \xleftarrow{\cup} \mathbb{F}_q, \ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_t},$

si

$$\boldsymbol{c}_i^{(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{e}_1 + \theta_i\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{0,\ldots,0,}^{w_t}\ \overbrace{\vec{\eta}_i}^{z_t})\,\mathbb{B}_t\ ,$$

si $\rho(i) = \neg(t, \vec{v}_i), \quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_t},$

$$\boldsymbol{c}_i^{(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{0,\ldots,0,}^{w_t}\ \overbrace{\vec{\eta}_i}^{z_t})\,\mathbb{B}_t\ ,$$

si $\rho(i) = p_0, \quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_0},$

$$\boldsymbol{c}_i^{(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{0,\ldots,0,}^{w_0}\ \overbrace{\vec{\eta}_i}^{z_0})\,\mathbb{B}_0\ ,$$

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

devolver $\mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{c}_0^{(\tau,\kappa,\iota)}, \boldsymbol{c}_1^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{c}_L^{(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}, c_{d+1}).$

[Fórmula 148]

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

$\mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{c}_0^{(\tau,\kappa,\iota)}, \boldsymbol{c}_1^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{c}_L^{(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}, c_{d+1})):$

si $\mathbb{S} := (\mathcal{A}, \mathcal{B}, d(x), \rho)$ acepta $\Gamma := \{(t, \vec{x}_t)\},$

entonces, calcular $\mathcal{I}_{(\rho,\Gamma)} \subseteq \{1,\ldots,L\}, (\alpha_1,\ldots,\alpha_L),$

$(\beta_1,\ldots,\beta_L)$ con $\alpha_i = 0 = \beta_i$ para todo $i \notin \mathcal{I}_{(\rho,\Gamma)}$, y $(\kappa_1,\ldots,\kappa_m)$ de tal manera que $\prod_{\tau=1}^m d_\tau(x)^{\kappa_\tau} \mid (a_0(x) + \sum_{i=1}^L \alpha_i a_i(x))$, y $\prod_{\tau=1}^m d_\tau(x)^{f_\tau - \kappa_\tau} \mid (b_0(x) + \sum_{i=1}^L \beta_i b_i(x)),$

$$K_{\tau,0} := e(\boldsymbol{k}_0, \boldsymbol{c}_0^{*(\tau,\kappa_\tau,0)}) \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{k}_0, \boldsymbol{c}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i}$$
$$\cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{k}_t, \boldsymbol{c}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i} \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{k}_t, \boldsymbol{c}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)},$$

$$K_{\tau,1} := e(\boldsymbol{k}_0, \boldsymbol{c}_0^{*(\tau,\kappa_\tau,1)}) \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{k}_0, \boldsymbol{c}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i}$$
$$\cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{k}_t, \boldsymbol{c}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i} \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{k}_t, \boldsymbol{c}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i/(\vec{v}_i\cdot\vec{x}_t)},$$

donde $\mathcal{I}_{(\rho,\Gamma),0} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = p_0\},$

$$\mathcal{I}_{(\rho,\Gamma),+} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = (t, \vec{v}_i)\}$$ y

$$\mathcal{I}_{(\rho,\Gamma),-} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = \neg(t, \vec{v}_i)\}.$$

devolver

$$msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0} K_{\tau,1}).$$

El esquema de encriptación funcional se ha descrito anteriormente. Si el algoritmo Setup, el algoritmo KeyGen, el algoritmo Enc, y el algoritmo Dec se modifican tal como se indica en las fórmulas 149 a 153 se puede realizar un esquema de encriptación basado en atributos. Con el esquema de encriptación basado en atributos, en el algoritmo Setup, n_t es $2mf_{max}k_{max} + 2$.

[Fórmula 149]

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

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

$$\hat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,n_0+u_0+w_0+1}, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}),$$

$$\hat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \boldsymbol{b}_{t,2}, \boldsymbol{b}_{t,n_t+u_t+w_t+1}, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t+z_t}) \text{ para } t = 1,..,d,$$

$$\hat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \ldots, \boldsymbol{b}_{0,n_0}^*, \boldsymbol{b}_{0,n_0+u_0+1}^*, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0}^*, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^*),$$

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

devolver

$$\text{pk} := (1^\lambda, \{\hat{\mathbb{B}}_t\}_{t=0,\ldots,d}, \text{param}), \qquad \text{sk} := \{\hat{\mathbb{B}}_t^*\}_{t=0,\ldots,d}.$$

[Fórmula 150]

$$\text{KeyGen}\left(\text{pk, sk, } \mathbb{S} := (\mathcal{A}, \mathcal{B}, d(x) = \prod_{\tau=1}^{m} d_\tau(x)^{f_\tau}, \rho)\right):$$

$$\pi_\tau \xleftarrow{U} \mathbb{F}_q, \ (\tau = 1,\ldots,m-1), \ \pi_m := -\sum_{\tau=1}^{m-1} \pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{U} \mathbb{F}_q, \ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0} \ (\tau = 1,\ldots,m; \ \kappa = 0,\ldots,f_\tau),$$

$$\chi_\tau \xleftarrow{U} \mathbb{F}_q, \ (\tau = 1,\ldots,m-1), \ \chi_m := 1 - \sum_{\tau=1}^{m-1} \chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{U} \mathbb{F}_q, \ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0} \ (\tau = 1,\ldots,m; \ \kappa = 0,\ldots,f_\tau),$$

para $\tau = 1,\ldots,m, \ \kappa = 0,\ldots,f_\tau, \ \iota = 0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ \ (\kappa = 0,\ldots,f_\tau)$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x + \cdots + a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x + \cdots + b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q,\ \left(j = 0,\ldots,\mu^{(\tau,\kappa,\iota)}-1\right),\ \ \vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{0,j}^{(\tau,\kappa)},$$

[Fórmula 151]

$$\boldsymbol{k}_0^{*(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)},}^{w_0}\ \overbrace{0,\ldots,0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\ \mathbb{B}_0^*\ ,$$

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

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q\ \ (i = 1,\ldots,L;\ \tau = 1,\ldots,m-1;\iota = 0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota}\ (i = 1,\ldots,L;\ \iota = 0,1),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1},$$

si $\rho(i) = (t, v_i),\qquad \theta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)} + \theta_i v_i,\ -\theta_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,\ldots,0}^{z_t})\ \mathbb{B}_i^*\ ,$$

si $\rho(i) = -(t, v_i),\qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)} v_i,\ -s_i^{(\tau,\kappa,\iota)},\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,\ldots,0}^{z_t})\ \mathbb{B}_i^*\ ,$$

si $\rho(i) = p_0,\qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_0},$

$$k_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}}^{n_0}, \overbrace{\vec{e}_0^{(\tau,\kappa,\iota)}}^{}, \overbrace{0,...,0,}^{u_0} \overbrace{\vec{\eta}_i,}^{w_0} \overbrace{0,...,0}^{w_0}) \mathbb{B}_0^* ,$$

devolver

$$\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{k_0^{*(\tau,\kappa,\iota)}, k_1^{*(\tau,\kappa,\iota)}, ..., k_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,...,m;\kappa=0,...,f_\tau;\iota=0,1}).$$

[Fórmula 152]

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

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

$$\vec{\varphi}_0 \xleftarrow{\cup} \mathbb{F}_q^{z_0-1},$$

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

$$c_0 := (\overbrace{\omega,\ 0,...,0,}^{n_0} \overbrace{0,...,0,}^{u_0} \overbrace{0,...,0,}^{w_0} \overbrace{\vec{\varphi}_0,\ \zeta}^{z_0}) \mathbb{B}_0 ,$$

$$c_t := (\overbrace{\omega(1,x_t),\ 0,...,0}^{n_t} \overbrace{0,...,0,}^{u_t} \overbrace{0,...,0,}^{w_t} \overbrace{\vec{\varphi}_t}^{z_t}) \mathbb{B}_t \text{ , para } (t,x_t) \in \Gamma,$$

$$c_{d+1} := g_T^{\zeta} msg,\ \ \mathsf{ct}_\Gamma := (\Gamma, c_0, \{c_t\}_{(t,x_t)\in\Gamma}, c_{d+1}),$$

devolver ct_Γ.

[Fórmula 153]

$$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{k_0^{*(\tau,\kappa,\iota)}, k_1^{*(\tau,\kappa,\iota)}, ..., k_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,...,m;\kappa=0,...,f_\tau;\iota=0,1}),$$
$$\mathsf{ct}_\Gamma := (\Gamma, c_0, \{c_t\}_{(t,x_t)\in\Gamma}, c_{d+1})):$$

Si $\mathbb{S} := (\mathcal{A}, \mathcal{B}, d(x),\ \rho)$ acepta $\Gamma := \{(t,x_t)\},$

entonces calcular $\mathcal{I}_{(\rho,\Gamma)} \subseteq \{1,...,L\}, (\alpha_1,...,\alpha_L),$

$(\beta_1,...,\beta_L)$ con $\alpha_i = 0 = \beta_i$ para todo $i \notin \mathcal{I}_{(\rho,\Gamma)}$, y $(\kappa_1,...,\kappa_m)$ de tal manera que

$$\prod_{\tau=1}^m d_\tau(x)^{\kappa_\tau} \mid (a_0(x) + \sum_{i=1}^L \alpha_i a_i(x)),$$

y $$\prod_{\tau=1}^m d_\tau(x)^{f\tau-\kappa_\tau} \mid (b_0(x) + \sum_{i=1}^L \beta_i b_i(x)),$$

$$K_{\tau,0} := e(\boldsymbol{c}_0, \boldsymbol{k}_0^{*(\tau,\kappa_\tau,0)}) \cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i}$$

$$\cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i} \cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i/(v_i - x_t)},$$

$$K_{\tau,1} := e(\boldsymbol{c}_0, \boldsymbol{k}_0^{*(\tau,\kappa_\tau,1)}) \cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i}$$

$$\cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i} \cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i/(v_i - x_t)},$$

donde $\mathcal{I}_{(\rho,\Gamma),0} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = p_0\},$

$$\mathcal{I}_{(\rho,\Gamma),+} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = (t, v_i)\}$$ y

$$\mathcal{I}_{(\rho,\Gamma),-} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = \neg(t, v_i)\}.$$

devolver

$$msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0} K_{\tau,1}).$$

De igual modo, el esquema CP-FE indicado en las fórmulas 145 a 148 puede ser alterado con el esquema de encriptación basado en atributos

En la explicación anterior, $n_0 + u_0 + w_0 + z_0$ se configuran en N_0 y $n_t + u_t + w_t + z_t$ se configuran en N_t. Si, por ejemplo, $u_0 = n_0$, $w_0 = n_0$ y $z_0 = 2$, entonces $n_0 + n_0 + n_0 + 2 = 3n_0 + 2$ puede ser configurado en N_0. Si $u_t = n_t$, $w_t = n_t$ y $z_t = 1$, entonces $n_t + n_t + n_t + 1 = 3\,n_t + 1$ se puede configurar en N_t.

Realización 3

La realización 3 será un ejemplo de un esquema de encriptación funcional en el que, comparado con el esquema de encriptación funcional descrito en la realización 2, el número de bases aumenta, pero el número de dimensiones de cada base disminuye.

La explicación se dará en la realización 3 principalmente en porciones que son diferentes del sistema criptográfico 10 según la realización 2.

Las configuraciones de un dispositivo de generación de claves 100, un dispositivo de encriptación 200 y un dispositivo de desencriptación 300 según la realización 3 son respectivamente las mismas que las configuraciones del dispositivo de generación de claves 100, el dispositivo de encriptación 200 y el dispositivo de desencriptación 300 según la realización 2 mostrada en las figuras 5 y 7.

El proceso de un algoritmo Dec según la realización 3 es el mismo que el proceso del algoritmo Dec según la realización 2. Por lo tanto, se describirán los procesos de un algoritmo Setup, un algoritmo KeyGen y un algoritmo Enc según la realización 3.

Los flujos de proceso del algoritmo Setup, el algoritmo KeyGen y el algoritmo Enc según la realización 3 son los mismos que los flujos de proceso del algoritmo Setup, el algoritmo KeyGen y el algoritmo Enc según la realización 2 mostrados en las figuras 8 a 10.

El proceso del algoritmo Setup se describirá haciendo referencia a la figura 8.

(S101: Etapa de generación de base ortogonal)

Los procesos de (1) a (3) son los mismos que los de la realización 2.

(4) Una parte de generación de clave principal 110 configura $n_0 + u_0 + w_0 + z_0$ en N_0, y configura $n_t + u_t + w_t + z_t$, en N_t relativo a cada entero t de t = 1, …, d (d es un entero mayor o igual que 1). Se debe observar que n_0 es 1 y n_t es n donde: n es un entero mayor o igual que 1 y u_0, w_0, z_0, u_t, w_t y z_t son cada uno entero mayor o igual que 0.

Posteriormente, la parte de generación de clave principal 110 ejecuta los procesos (5) a (9) relativos a los enteros τ, κ, ι y t de τ = 1, …, m, κ = 0, ..., f_τ, ι = 0, 1, y t = 0, …, d

El proceso de (5) es el mismo que en la realización 2.

(6) La parte de generación de clave principal 110 genera la transformación lineal $X_t^{(\tau,\kappa,\iota)} := (\chi_{t,i,j}^{(\tau,\kappa,\iota)})_{i,j}$ aleatoriamente, de la misma manera que en la realización 2.

(7) La parte de generación de clave principal 110 genera $X^*{}_t^{(\tau,\kappa,\iota)} := (\nu_{t,i,j}^{(\tau,\kappa,\iota)})_{i,j} := \psi \cdot (X_t^{(\tau,\kappa,\iota)T})^{-1}$, de la misma manera que en la realización 2.

(8) En base a la transformación lineal $X_t^{(\tau,\kappa,\iota)}$ generada en (6), la parte de generación de clave principal 110 genera una base $B_t^{(\tau,\kappa,\iota)}$ a partir de una base canónica A_t generada en (5), de la misma manera que en la realización 2.

(9), En base a la transformación lineal $X^*{}_t^{(\tau,\kappa,\iota)}$ generada en (7), la parte de generación de clave principal 110 genera una base B $B^*{}_t^{(\tau,\kappa,\iota)}$ a partir de una base canónica A_t generada en (5), de la misma manera que en la realización 2.

El proceso de (10) es el mismo que en la realización 2.

(S102: Etapa de generación de parámetros públicos)

Con el dispositivo de procesamiento, la parte de generación de clave principal 110 genera las subbases $B\hat{}_0^{(\tau,\kappa,\iota)}$ y $B\hat{}_t^{(\tau,\kappa,\iota)}$ de las bases $B_0^{(\tau,\kappa,\iota)}$ y $B_t^{(\tau,\kappa,\iota)}$, respectivamente, que se generan en (S101), tal como se indica en la fórmula 154.

[Fórmula 154]

$$\hat{\mathbb{B}}_0^{(\tau,\kappa,\iota)} := (\boldsymbol{b}_{0,1}^{(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,n_0+u_0+w_0+1}^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^{(\tau,\kappa,\iota)}),$$

$$\hat{\mathbb{B}}_t^{(\tau,\kappa,\iota)} := (\boldsymbol{b}_{t,1}^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n}^{(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,n_t+u_t+w_t+1}^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t+z_t}^{(\tau,\kappa,\iota)})$$

para $t = 1, .., d$

La parte de generación de clave principal 110 trata las subbases $B\hat{}_0^{(\tau,\kappa,\iota)}$ y $B\hat{}_t^{(\tau,\kappa,\iota)}$ generadas, el parámetro de seguridad λ introducido en (S101) y el param generado en (S101), para formar los parámetros públicos pk.

(S103: Etapa de generación de clave principal)

Con el dispositivo de procesamiento, la parte de generación de clave principal 110 genera las subbases $B\hat{}^*{}_0^{(\tau,\kappa,\iota)}$ y $B\hat{}^*{}_t^{(\tau,\kappa,\iota)}$ de las bases $B^*{}_0^{(\tau,\kappa,\iota)}$ y $B^*{}_t^{(\tau,\kappa,\iota)}$, respectivamente, que se generan en (S101), tal como se indica en la fórmula 155.

[Fórmula 155]

$$\hat{\mathbb{B}}_0^{*(\tau,\kappa,\iota)} := (\boldsymbol{b}_{0,1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{0,n_0}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,n_0+u_0+1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^{*(\tau,\kappa,\iota)}),$$

$$\hat{\mathbb{B}}_t^{*(\tau,\kappa,\iota)} := (\boldsymbol{b}_{t,1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n_t}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,n_t+u_t+1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t}^{*(\tau,\kappa,\iota)})$$

para $t = 1,..,d$

La parte de generación de clave principal 110 trata las subbases $\mathrm{B}^{\wedge *}{}_0^{(\tau,\kappa,\iota)}$ y $\mathrm{B}^{\wedge *}{}_t^{(\tau,\kappa,\iota)}$ generadas para formar la clave principal sk.

El proceso de (S104) es el mismo que el de la realización 2.

En resumen, desde (S101) hasta (S103), el dispositivo de generación de claves 100 genera los parámetros públicos pk y la clave principal sk ejecutando el algoritmo de Setup indicado en la fórmula 156. A continuación, en (S104), el dispositivo de generación de claves 100 almacena los parámetros públicos pk generados y la clave principal sk, en el dispositivo de almacenamiento.

[Fórmula 156]

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

$$(\mathrm{param}, (\mathbb{B}_t^{(\tau,\kappa,\iota)}, \mathbb{B}_t^{*(\tau,\kappa,\iota)})_{t=0,\ldots,d;\ \tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau;\ \iota=0,1})$$

$$\xleftarrow{R} \mathcal{G}_{\mathrm{ob}}(1^\lambda),$$

para $\tau = 1,\ldots,m,\quad \kappa = 0,\ldots,f_\tau,\quad \iota = 0,1,$

$$\hat{\mathbb{B}}_0^{(\tau,\kappa,\iota)} := (\boldsymbol{b}_{0,1}^{(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,n_0+u_0+w_0+1}^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^{(\tau,\kappa,\iota)}),$$

$$\hat{\mathbb{B}}_t^{(\tau,\kappa,\iota)} := (\boldsymbol{b}_{t,1}^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n}^{(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,n_t+u_t+w_t+1}^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t+z_t}^{(\tau,\kappa,\iota)})$$

para $t = 1,..,d,$

$$\hat{\mathbb{B}}_0^{*(\tau,\kappa,\iota)} := (\boldsymbol{b}_{0,1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{0,n_0}^{*(\tau,\kappa,\iota)},$$

$$\boldsymbol{b}_{0,n_0+u_0+1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^{*(\tau,\kappa,\iota)}),$$

$$\hat{\mathbb{B}}_t^{*(\tau,\kappa,\iota)} := (\boldsymbol{b}_{t,1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n_t}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,n_t+u_t+1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t}^{*(\tau,\kappa,\iota)})$$

para $t = 1,..,d,$

devolver

$$\mathrm{pk} := (1^\lambda, \{\hat{\mathbb{B}}_t\}_{t=0,\ldots,d}, \mathrm{param}), \qquad \mathrm{sk} := \{\hat{\mathbb{B}}_t^*\}_{t=0,\ldots,d}.$$

El proceso del algoritmo KeyGen se describirá haciendo referencia a la figura 9.

Los procesos de (S201) a (S204) y de (S206) son los mismos que los de la realización 2.

(S205: Etapa de generación de elemento clave)

Con el dispositivo de procesamiento, con respecto a cada número entero τ de τ = 1, …, m, cada entero κ de κ = 0, ..., f_τ, y cada entero ι de ι = 0, 1, una parte de generación de elemento clave 142 genera un elemento $\mathrm{k}^*{}_0^{(\tau,\kappa,\iota)}$ de una clave de desencriptación sk_s, tal como se indica en la fórmula 157.

[Fórmula 157]

$$\vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$

$$\boldsymbol{k}_0^{*(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota}}^{n_0}, \overbrace{0,...,0,}^{u_0} \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)},}^{w_0} \overbrace{0,...,0,\ \chi_{\tau,\kappa,\iota}}^{z_0}) \mathbb{B}_0^{*(\tau,\kappa,\iota)}$$

Con el dispositivo de procesamiento, con respecto a cada entero τ de τ = 1, …, m, cada entero κ de κ = 0, ..., f_τ, cada entero ι de ι = 0, 1, y cada entero i de i = 1, …, L, la parte de generación de elementos de clave 142 genera un elemento $k^{*(\tau,\kappa,\iota)}_i$ de la clave de desencriptación sk_s tal como se indica en la fórmula 158.

[Fórmula 158]

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

$$\theta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{e}_1 + \theta_i \vec{v}_i,}^{n_t} \overbrace{0,...,0,}^{u_t} \overbrace{\vec{\eta}_i,}^{w_t} \overbrace{0,...,0}^{z_t}) \mathbb{B}_t^{*(\tau,\kappa,\iota)},$$

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

$$\vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{v}_i,}^{n_t} \overbrace{0,...,0,}^{u_t} \overbrace{\vec{\eta}_i,}^{w_t} \overbrace{0,...,0}^{z_t}) \mathbb{B}_t^{*(\tau,\kappa,\iota)},$$

si $\rho(i) = p_0,$

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

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)},}^{n_0} \overbrace{0,...,0,}^{u_0} \overbrace{\vec{\eta}_i,}^{w_0} \overbrace{0,...,0}^{z_0}) \mathbb{B}_0^{*(\tau,\kappa,\iota)}$$

En resumen, de (S201) a (S205), el dispositivo de generación de claves 100 genera la clave de desencriptación sk_s ejecutando el algoritmo KeyGen, indicado en las fórmulas 159 a 160. A continuación, en (S206), el dispositivo de generación de claves 100 distribuye la clave de desencriptación sk_s generada, al dispositivo de desencriptación 300.

[Fórmula 159]

$$\text{KeyGen}\left(\text{pk, sk, } \mathbb{S} := (\mathcal{A}, \mathcal{B}, d(x) = \prod_{\tau=1}^{m} d_\tau(x)^{f_\tau}, \rho)\right):$$

$$\pi_\tau \xleftarrow{\cup} \mathbb{F}_q,\ (\tau = 1,...,m-1),\ \pi_m := -\sum_{\tau=1}^{m-1} \pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\cup} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau = 1,...,m;\ \kappa = 0,...,f_\tau),$$

$$\chi_\tau \xleftarrow{\cup} \mathbb{F}_q,\ (\tau = 1,...,m-1),\ \chi_m := 1 - \sum_{\tau=1}^{m-1} \chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\cup} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau = 1,...,m;\ \kappa = 0,...,f_\tau),$$

para $\tau = 1,...,m,\ \kappa = 0,...,f_\tau,\ \iota = 0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ \ (\kappa = 0,...,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x + \cdots + a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)} x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x + \cdots + b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)} x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q,\ \left(j = 0,...,\mu^{(\tau,\kappa,\iota)}-1\right),\ \ \vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{0,j}^{(\tau,\kappa)},$$

[Fórmula 160]

$$\boldsymbol{k}_0^{*(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota}}^{n_0},\ \overbrace{0,...,0}^{u_0},\ \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)}}^{w_0},\ \overbrace{0,...,0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\ \mathbb{B}_0^{*(\tau,\kappa,\iota)},$$

para $i = 1,...,L,$

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q\ \ \left(i = 1,...,L;\ \tau = 1,...,m-1; \iota = 0,1\right),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota}\left(i = 1,...,L;\ \iota = 0;1\right),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1},$$

si $\rho(i) = (t, \vec{v}_i),\qquad \theta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{e}_1 + \theta_i\vec{v}_i}^{n_t},\ \overbrace{0,...,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,...,0}^{z_t})\ \mathbb{B}_t^{*(\tau,\kappa,\iota)},$$

si $\rho(i) = \neg(t, \vec{v}_i),\qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{v}_i,}^{n_t}\ \overbrace{0,...,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,...,0}^{z_t})\ \mathbb{B}_t^{*(\tau,\kappa,\iota)},$$

si $\rho(i) = p_0,\qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_0},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)},}^{n_0}\ \overbrace{0,...,0,}^{u_0}\ \overbrace{\vec{\eta}_i,}^{w_0}\ \overbrace{0,...,0}^{z_0})\ \mathbb{B}_0^{*(\tau,\kappa,\iota)},$$

devolver

$$\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_0^{*(\tau,\kappa,\iota)}, \boldsymbol{k}_1^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}).$$

El proceso del algoritmo Enc se describirá haciendo referencia a la figura 10.

Los procesos de (S301) a (S302) y de (S304) son los mismos que los de la realización 2.

(S303: Etapa de generación de elementos de cifrado)

Con el dispositivo de procesamiento, una parte de generación de datos encriptados 230 genera un elemento $c_0^{(\tau,\kappa,\iota)}$ de un texto cifrado ctΓ indicado en la fórmula 161.

[Fórmula 161]

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

$$\vec{\varphi}_0 \xleftarrow{\cup} \mathbb{F}_q^{z_0-1},$$

$$\boldsymbol{c}_0^{(\tau,\kappa,\iota)} := (\overbrace{\omega,}^{n_0} \overbrace{0,\ldots,0,}^{u_0} \overbrace{0,\ldots,0,}^{w_0} \overbrace{\vec{\varphi}_0, \zeta}^{z_0})\, \mathbb{B}_0^{(\tau,\kappa,\iota)}$$

Con el dispositivo de procesamiento, con respecto a cada entero t incluido en la información de atributos Γ, la parte de generación de datos encriptados 230 genera un elemento $c_t^{(\tau,\kappa,\iota)}$ del texto cifrado ct_Γ, tal como se indica en la fórmula 162.

[Fórmula 162]

$$\vec{\varphi}_t \xleftarrow{\cup} \mathbb{F}_q^{z_t} \text{ for } (t, \vec{x}_t) \in \Gamma,$$

$$\boldsymbol{c}_t^{(\tau,\kappa,\iota)} := (\overbrace{\omega \vec{x}_t,}^{n_t} \overbrace{0,\ldots,0,}^{u_t} \overbrace{0,\ldots,0,}^{w_t} \overbrace{\vec{\varphi}_t}^{z_t})\, \mathbb{B}_t^{(\tau,\kappa,\iota)}$$

Con el dispositivo de procesamiento, la parte de generación de datos encriptados 230 genera un elemento c_{d+1} del texto cifrado ct_Γ, tal como se indica en la fórmula 163.

[Fórmula 163]

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

En resumen, de (S301) a (S303), el dispositivo de encriptación 200 genera el texto cifrado ct_Γ, ejecutando el algoritmo Enc indicado en la fórmula 164. A continuación, en (S304), el dispositivo de encriptación 200 transmite el texto cifrado ct_Γ, generado al dispositivo de desencriptación 300.

[Fórmula 164]

$$\mathsf{Enc}(\mathsf{pk}, msg, \Gamma := \{(t, \vec{x}_t) \mid 1 \le t \le d\}):$$

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

$$\vec{\varphi}_0 \xleftarrow{\cup} \mathbb{F}_q^{z_0-1},$$

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

$$\boldsymbol{c}_0^{(\tau,\kappa,\iota)} := (\overbrace{\omega,}^{n_0} \overbrace{0,\ldots,0,}^{u_0} \overbrace{0,\ldots,0,}^{w_0} \overbrace{\vec{\varphi}_0, \zeta}^{z_0})\, \mathbb{B}_0^{(\tau,\kappa,\iota)},$$

$$c_t^{(\tau,\kappa,\iota)} := (\overbrace{\vec{\omega x_t},}^{n_t}\ \overbrace{0,...,0,}^{u_t}\ \overbrace{0,...,0,}^{w_t}\ \overbrace{\vec{\varphi}_t}^{z_t})\,\mathbb{B}_t^{(\tau,\kappa,\iota)}\ ,\ \text{para}\ (t,\vec{x}_t)\in\Gamma,$$

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

devolver

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

Tal como se ha descrito anteriormente, el sistema de encriptación 10 según la realización 3 implementa un esquema de encriptación funcional en el que, por ejemplo, en comparación con el esquema de encriptación funcional descrito en la realización 2, el número de bases aumenta, pero el número de dimensiones de cada base disminuye.

El esquema de KP-FE se ha descrito anteriormente Si el algoritmo KeyGen y el algoritmo Enc se modifican tal como se indica en las fórmulas 165 a 167, puede realizarse el esquema CP-FE. Se debe observar que el algoritmo Setup es el mismo entre el esquema KP-FE y el esquema CP-FE. El algoritmo Dec es el mismo que el algoritmo Dec indicado en la fórmula 148.

[Fórmula 165]

$$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \Gamma := \{(t,\vec{x}_t)\,|\,1\le t\le d\}):$$

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

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

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

$$k_0^{*(\tau,\kappa,\iota)} := (\overbrace{\omega,}^{n_0}\ \overbrace{0,...,0,}^{u_0}\ \overbrace{\vec{\varphi}_0,}^{w_0}\ \overbrace{0,...,0,1}^{z_0})\,\mathbb{B}_0^{*(\tau,\kappa,\iota)}\ ,$$

$$k_t^{*(\tau,\kappa,\iota)} := (\overbrace{\vec{\omega x_t},}^{n_t}\ \overbrace{0,...,0,}^{u_t}\ \overbrace{\vec{\varphi}_t,}^{w_t}\ \overbrace{0,...,0}^{z_t})\,\mathbb{B}_t^{*(\tau,\kappa,\iota)}\ ,\ \text{para}\ (t,\vec{x}_t)\in\Gamma$$

devolver

$$\mathsf{sk}_\Gamma := (\Gamma,\ k_0^*, \{k_t^*\}_{(t,\vec{x}_t)\in\Gamma}).$$

[Fórmula 166]

$$\mathsf{Enc}\left(\mathsf{pk},\ msg,\ \mathbb{S} := (\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho)\right):$$

$$\pi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,...,m-1),\ \ \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,...,m;\ \ \kappa=0,...,f_\tau),$$

$$\chi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,...,m-1),\ \ \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,...,m;\ \ \kappa=0,...,f_\tau),$$

para $\tau=1,...,m,\ \ \kappa=0,...,f_\tau,\ \ \iota=0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ \ (\kappa = 0,\ldots,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x + \cdots + a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x + \cdots + b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q,\ \left(j = 0,\ldots,\mu^{(\tau,\kappa,\iota)}-1\right),\ \ \vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q^{z_0-1},$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{0,j}^{(\tau,\kappa)},$$

[Fórmula 167]

$$c_0^{(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota}}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{0,\ldots,0,}^{w_0}\ \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)},\ \zeta\chi_{\tau,\kappa,\iota}}^{z_0})\ \mathbb{B}_0^{(\tau,\kappa,\iota)},$$

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

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q\ \ \left(i = 1,\ldots,L;\ \tau = 1,\ldots,m-1;\iota = 0,1\right),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota}\left(i = 1,\ldots,L;\ \iota = 0,1\right),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1},$$

si $\rho(i) = (t,\vec{v}_i),\qquad \theta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_t},$

$$c_i^{(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{e}_1 + \theta_i\vec{v}_i,}^{n_t}\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{0,\ldots,0,}^{w_t}\ \overbrace{\vec{\eta}_i}^{z_t})\ \mathbb{B}_t^{(\tau,\kappa,\iota)},$$

si $\rho(i) = \neg(t,\vec{v}_i),\qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_t},$

$$c_i^{(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{v}_i,}^{n_t}\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{0,\ldots,0,}^{w_t}\ \overbrace{\vec{\eta}_i}^{z_t})\ \mathbb{B}_t^{(\tau,\kappa,\iota)},$$

si $\rho(i) = p_0,\qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_0},$

$$c_i^{(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}}^{n_0}, \overbrace{0,...,0,}^{u_0} \overbrace{0,...,0,}^{w_0} \overbrace{\vec{\eta}_i}^{z_0}) \, \mathbb{B}_0^{(\tau,\kappa,\iota)},$$

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

devolver

$$\mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, \{c_0^{(\tau,\kappa,\iota)}, c_1^{(\tau,\kappa,\iota)}, ..., c_L^{(\tau,\kappa,\iota)}\}_{\tau=1,...,m;\kappa=0,...,f_\tau;\iota=0,1}, c_{d+1}).$$

El esquema de encriptación funcional se ha descrito anteriormente. Si el algoritmo Setup, el algoritmo KeyGen y el algoritmo Enc se modifican tal como se indica en las fórmulas 168 a 171, puede realizarse un esquema de encriptación basado en atributos. Con el esquema de encriptación basado en atributos, en el algoritmo Setup, n_t es 2. El algoritmo Dec es el mismo que el algoritmo Dec indicado en la fórmula 153.

[Fórmula 168]

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

$$(\mathsf{param}, (\mathbb{B}_t^{(\tau,\kappa,\iota)}, \mathbb{B}_t^{*(\tau,\kappa,\iota)})_{t=0,...,d;\ \tau=1,...,m;\ \kappa=0,...,f_\tau;\ \iota=0,1}) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}(1^\lambda),$$

para $\tau = 1,...,m, \quad \kappa = 0,...,f_\tau, \quad \iota = 0,1,$

$$\hat{\mathbb{B}}_0^{(\tau,\kappa,\iota)} := (\boldsymbol{b}_{0,1}^{(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,n_0+u_0+w_0+1}^{(\tau,\kappa,\iota)}, ..., \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^{(\tau,\kappa,\iota)}),$$

$$\hat{\mathbb{B}}_t^{(\tau,\kappa,\iota)} := (\boldsymbol{b}_{t,1}^{(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,2}^{(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,n_t+u_t+w_t+1}^{(\tau,\kappa,\iota)}, ..., \boldsymbol{b}_{t,n_t+u_t+w_t+z_t}^{(\tau,\kappa,\iota)})$$

para $t = 1,..,d,$

$$\hat{\mathbb{B}}_0^{*(\tau,\kappa,\iota)} := (\boldsymbol{b}_{0,1}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,1+u_0+1}^{*(\tau,\kappa,\iota)}, ..., \boldsymbol{b}_{0,1+u_0+w_0}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,1+u_0+w_0+z_0}^{*(\tau,\kappa,\iota)}),$$

$$\hat{\mathbb{B}}_t^{*(\tau,\kappa,\iota)} := (\boldsymbol{b}_{t,1}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,2}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,2+u_t+1}^{*(\tau,\kappa,\iota)}, ..., \boldsymbol{b}_{t,2+u_t+w_t}^{*(\tau,\kappa,\iota)})$$

para $t = 1,..,d,$

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

[Fórmula 169]

$$\mathsf{KeyGen}\left(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (\mathcal{A}, \mathcal{B}, d(x) = \prod_{\tau=1}^{m} d_\tau(x)^{f_\tau}, \rho)\right):$$

$$\pi_\tau \xleftarrow{U} \mathbb{F}_q, \ (\tau = 1,...,m-1), \ \pi_m := -\sum_{\tau=1}^{m-1} \pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{U} \mathbb{F}_q, \ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0} \ (\tau = 1,...,m; \ \kappa = 0,...,f_\tau),$$

$$\chi_\tau \xleftarrow{U} \mathbb{F}_q, \ (\tau = 1,...,m-1), \ \chi_m := 1 - \sum_{\tau=1}^{m-1} \chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{U} \mathbb{F}_q, \ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0} \ (\tau = 1,...,m; \ \kappa = 0,...,f_\tau),$$

para $\tau = 1,...,m, \quad \kappa = 0,...,f_\tau, \quad \iota = 0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa), \quad \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}), \quad (\kappa = 0,...,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x + \cdots + a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x + \cdots + b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q, \ \left(j = 0,...,\mu^{(\tau,\kappa,\iota)}-1\right), \quad \vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{0,j}^{(\tau,\kappa)},$$

[Fórmula 170]

$$\boldsymbol{k}_0^{*(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota}}^{n_0}, \overbrace{0,...,0,}^{u_0} \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)},}^{w_0} \overbrace{0,...,0,\ \chi_{\tau,\kappa,\iota}}^{z_0}) \, \mathbb{B}_0^{*(\tau,\kappa,\iota)},$$

para $i = 1,...,L,$

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q \ \left(i = 1,...,L; \ \tau = 1,...,m-1; \iota = 0,1\right),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota} \left(i = 1,...,L; \ \iota = 0,1\right),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1},$$

si $\rho(i) = (t, v_i), \qquad \theta_i \xleftarrow{\cup} \mathbb{F}_q, \ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)} + \theta_i v_i, \ -\theta_i,}^{n_t} \overbrace{0,...,0,}^{u_t} \overbrace{\vec{\eta}_i,}^{w_t} \overbrace{0,...,0}^{z_t}) \, \mathbb{B}_i^{*(\tau,\kappa,\iota)},$$

si $\rho(i) = \neg(t, v_i), \qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)} v_i, \ -s_i^{(\tau,\kappa,\iota)},}^{n_t} \overbrace{0,...,0,}^{u_t} \overbrace{\vec{\eta}_i,}^{w_t} \overbrace{0,...,0}^{z_t}) \, \mathbb{B}_i^{*(\tau,\kappa,\iota)},$$

si $\rho(i) = p_0, \qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_0},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)},}^{n_0} \overbrace{0,...,0,}^{u_0} \overbrace{\vec{\eta}_i,}^{w_0} \overbrace{0,...,0}^{w_0}) \, \mathbb{B}_0^{*(\tau,\kappa,\iota)},$$

devolver $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{k_0^{*(\tau,\kappa,\iota)}, k_1^{*(\tau,\kappa,\iota)}, \ldots, k_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1})$.

[Fórmula 171]

$\mathsf{Enc}(\mathsf{pk}, msg, \Gamma := \{(t,x_t) | 1 \le t \le d\})$:

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

$\vec{\varphi}_0 \xleftarrow{\cup} \mathbb{F}_q^{z_0-1},$

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

$$c_0^{(\tau,\kappa,\iota)} := (\overbrace{\omega}^{n_0}, \overbrace{0,\ldots,0}^{u_0}, \overbrace{0,\ldots,0}^{w_0}, \overbrace{\vec{\varphi}_0, \zeta}^{z_0})_{\mathbb{B}_0^{(\tau,\kappa,\iota)}},$$

$$c_t^{(\tau,\kappa,\iota)} := (\overbrace{\omega(1,x_t)}^{n_t}, \overbrace{0,\ldots,0}^{u_t}, \overbrace{0,\ldots,0}^{w_t}, \overbrace{\vec{\varphi}_t}^{z_t})_{\mathbb{B}_t^{(\tau,\kappa,\iota)}}, \text{ para } (t,x_t) \in \Gamma,$$

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

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

Del mismo modo, el esquema CP-FE indicado en las fórmulas 165 a 167 puede ser alterado al esquema de encriptación basado en atributos

En la explicación anterior $n_0 + u_0 + w_0 + z_0$ se configura en N_0 y $n_t + u_t + w_t + z_t$ se configura en N_1. Si, por ejemplo, $u_0 = n_0$, $w_0 = n_0$ y $z_0 = 2$, entonces $n_0 + n_0 + n_0 + 2 = 3n_0 + 2$ ($n_0 = 1$ y, en consecuencia, $N_0 = 5$) se puede configurar en N_0. Si $u_t = n_t$, $w_t = n_t$ y $z_t = 1$, entonces $n_t + n_t + n_t + 1 = 3n_t + 1$ se puede configurar en N_t.

Realización 4.

En las realizaciones 2 y 3, para cada polinomio $d_\tau(x)^{f\tau}$ obtenido por factorización del polinomio objetivo d(x), un elemento que es un resto de dividir un polinomio $a_i(x)$ por un polinomio $d_\tau(x)^\kappa$ y un elemento que es un resto de dividir un polinomio $b_i(x)$ por un polinomio $d_\tau(x)^{f\tau-\kappa}$ son tratados como elementos clave.

En la Realización 4, para cada polinomio $d_\tau(x)^{f\tau}$ obtenido por factorización del polinomio objetivo d(x), un elemento obtenido sustituyendo un valor aleatorio γ en un polinomio $d_\tau(x)^\kappa$ y un elemento obtenido sustituyendo un valor aleatorio γ en un polinomio $d_\tau(x)^{f\tau-\kappa}$ son tratados como elementos clave.

Las configuraciones de un dispositivo de generación de claves 100, un dispositivo de encriptación 200, y un dispositivo de desencriptación 300 según la realización 4 son respectivamente las mismas que las configuraciones del dispositivo de generación de claves 100, el dispositivo de encriptación 200 y el dispositivo de desencriptación 300 según la realización 2 mostrada en las figuras 5 y 7.

Los procesos de un algoritmo Setup y un algoritmo Enc según la realización 4 son los mismos que los procesos del algoritmo Setup y el algoritmo Enc según la realización 2.

El flujo de proceso del algoritmo Dec según la realización 4 es el mismo que el flujo de proceso del algoritmo Dec según la realización 2 mostrada en la figura 11.

La figura 12 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen según la realización 4.

El proceso del algoritmo KeyGen se describirá haciendo referencia a la figura 12.

Los procesos de (S501) a (S503) son los mismos que los procesos de (S201) a (S203) mostrados en la Figura 9, y el proceso de (S505) es el mismo que el proceso de (S206) mostrado en la figura 9.

(S504: Etapa de generación del elemento clave)

Con el dispositivo de procesamiento, con respecto a cada entero τ de τ = 1, ..., m, cada entero κ de κ = 0, ..., f_τ, cada entero ι de ι= 0, 1 y cada entero j de j = 1, ..., μ + 1, una parte de generación de elementos clave 142 genera los elementos $k^*_{0,j}{}^{(\tau,\kappa,\iota)}$ y $k^*_{0,\mu+1}{}^{(\tau,\kappa,\iota)}$ de una clave de desencriptación sk_s tal como se indica en la fórmula 172.

[Fórmula 172]

$$\gamma \xleftarrow{U} \mathbb{F}_q,\ \vec{\eta}_{0,0},\ldots,\vec{\eta}_{0,\mu+1} \xleftarrow{U} \mathbb{F}_q^{w_0},$$

$$\boldsymbol{k}^{*(\tau,\kappa,0)}_{0,j} := (\overbrace{\delta(\gamma^j \cdot d_\tau(\gamma)^\kappa,\ \vec{e}^{(\tau,\kappa,0)}_{0,j})}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_{0,j}}^{w_0},\ \overbrace{0,\ldots,0}^{z_0})\ \mathbb{B}^*_0,$$

$$\boldsymbol{k}^{*(\tau,\kappa,1)}_{0,j} := (\overbrace{\delta(\gamma^j \cdot d_\tau(\gamma) f_\tau - \kappa,\ \vec{e}^{(\tau,\kappa,1)}_{0,j})}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_{0,j}}^{w_0},\ \overbrace{0,\ldots,0}^{z_0})\ \mathbb{B}^*_0,$$

$$s_0 := -a_0(\gamma)\ \text{si}\ \iota = 0,\quad s_0 := -b_0(\gamma)\ \text{si}\ \iota = 1,$$

$$\boldsymbol{k}^{*(\tau,\kappa,\iota)}_{0,\mu+1} := (\overbrace{\delta(s_0 + \pi_{\tau,\kappa,\iota},\ \vec{e}^{(\tau,\kappa,\iota)}_{0,\mu+1})}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_{0,\mu+1}}^{w_0},\ \overbrace{0,\ldots,0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\ \mathbb{B}^*_0$$

Con el dispositivo de procesamiento, con respecto a cada τ de τ = 1, ..., m, cada entero κ de κ = 0, ..., f_τ, cada entero ι de ι= 0, 1, y cada entero de i de i = 1, …, L, la parte de generación de elementos clave 142 genera un elemento $k^*_i{}^{(\tau,\kappa,\iota)}$ de la clave de desencriptación sk_s, tal como se indica en la fórmula 173.

[Fórmula 173]

$$\xi_{i,\tau,\iota} \xleftarrow{U} \mathbb{F}_q\ \ (i = 1,\ldots,L;\ \tau = 1,\ldots,m-1;\iota = 0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota}\ (i = 1,\ldots,L;\ \iota = 0,1),$$

$$s_i := -a_i(\gamma) + \xi_{i,\tau,0}\ \text{si}\ \iota = 0,\qquad s_i := -b_i(\gamma) + \xi_{i,\tau,1}\ \text{si}\ \iota = 1,$$

$$\text{si}\ \rho(i) = (t,\vec{v}_i),\qquad \theta_i \xleftarrow{U} \mathbb{F}_q,\quad \vec{\eta}_i \xleftarrow{U} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}^{*(\tau,\kappa,\iota)}_i := (\overbrace{\delta(s_i\vec{e}_1 + \theta_i\vec{v}_i),\ \vec{e}^{(\tau,\kappa,\iota)}_i}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,\ldots,0}^{z_t})\ \mathbb{B}^*_t,$$

$$\text{si}\ \rho(i) = \neg(t,\vec{v}_i),\qquad \vec{\eta}_i \xleftarrow{U} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}^{*(\tau,\kappa,\iota)}_i := (\overbrace{\delta s_i\vec{v}_i,\ \vec{e}^{(\tau,\kappa,\iota)}_i}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,\ldots,0}^{z_t})\ \mathbb{B}^*_t$$

Se debe observar que $e^{\rightarrow}{}_{0,j}{}^{(\tau,\kappa,\iota)}\ (j = 1, \ldots, \mu+1)$ es un vector de $2mf_{max}$ dimensiones en el que 1 se configura como el coeficiente para un vector base y 0 se configura como el coeficiente para otro vector de base, y el vector de base para el cual 1 se configura como coeficiente es diferente para cada uno (τ,κ,ι).

En resumen, de (S501) a (S504), el dispositivo de generación de claves 100 genera la clave de desencriptación sk_s, ejecutando el algoritmo KeyGen indicado en las fórmulas 174 a 175. A continuación, en (S505), el dispositivo de generación de claves 100 distribuye la clave de desencriptación generada sk_s al dispositivo de desencriptación 300.

[Fórmula 174]

$$\mathrm{KeyGen}\left(\mathrm{pk},\ \mathrm{sk},\ \mathbb{S} \coloneqq (\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho)\right):$$

$$\pi_\tau \xleftarrow{\cup} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \pi_m \coloneqq -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\cup} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} \coloneqq \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

$$\chi_\tau \xleftarrow{\cup} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \chi_m \coloneqq 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\cup} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} \coloneqq \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

para $\tau=1,\ldots,m,\ \ \kappa=0,\ldots,f_\tau,\ \ \iota=0,1,$

$$\gamma \xleftarrow{\cup} \mathbb{F}_q,\ \ \vec{\eta}_{0,0},\ldots,\vec{\eta}_{0,\mu+1} \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$

para $j=0,\ldots,\mu,$

$$\boldsymbol{k}_{0,j}^{*(\tau,\kappa,0)} \coloneqq (\overbrace{\delta(\gamma^j\cdot d_\tau(\gamma)^\kappa,\ \vec{e}_{0,j}^{(\tau,\kappa,0)})}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{\vec{\eta}_{0,j},}^{w_0}\ \overbrace{0,\ldots,0}^{z_0})\,\mathbb{B}_0^*,$$

$$\boldsymbol{k}_{0,j}^{*(\tau,\kappa,1)} \coloneqq (\overbrace{\delta(\gamma^j\cdot d_\tau(\gamma)^{f_\tau-\kappa},\ \vec{e}_{0,j}^{(\tau,\kappa,1)})}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{\vec{\eta}_{0,j},}^{w_0}\ \overbrace{0,\ldots,0}^{z_0})\,\mathbb{B}_0^*,$$

$$s_0 \coloneqq -a_0(\gamma)\ \text{si}\ \iota=0,\ \ s_0 \coloneqq -b_0(\gamma)\ \text{si}\ \iota=1,$$

$$\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,\iota)} \coloneqq (\overbrace{\delta(s_0+\pi_{\tau,\kappa,\iota},\ \vec{e}_{0,\mu+1}^{(\tau,\kappa,\iota)})}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{\vec{\eta}_{0,\mu+1},}^{w_0}\ \overbrace{0,\ldots0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\,\mathbb{B}_0^*,$$

[Fórmula 175]

para i = 1,..., L,

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q\ (i=1,\ldots,L;\ \tau=1,\ldots,m-1;\iota=0,1),$$

$$\xi_{i,m,\iota} \coloneqq -\sum_{\tau=1}^{m-1}\xi_{i,\tau,\iota}\,(i=1,\ldots,L;\ \iota=0,1),$$

$$s_i \coloneqq -a_i(\gamma)+\xi_{i,\tau,0}\ \text{si}\ \iota=0,\qquad s_i \coloneqq -b_i(\gamma)+\xi_{i,\tau,1}\ \text{si}\ \iota=1,$$

$$\text{si}\ \rho(i)=(t,\vec{\nu}_i),\qquad \theta_i \xleftarrow{\cup} \mathbb{F}_q,\quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} \coloneqq (\overbrace{\delta(s_i\vec{e}_1+\theta_i\vec{\nu}_i),\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^*,$$

si $\rho(i) = \neg(t, \vec{v}_i), \qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{\delta s_i \vec{v}_i, \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t}, \overbrace{0,...,0,}^{u_t} \overbrace{\vec{\eta}_i,}^{w_t} \overbrace{0,...,0}^{z_t}) \mathbb{B}_t^*,$$

$$\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_{0,0}^{*(\tau,\kappa,\iota)}, ..., \boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,\iota)},$$

$$\boldsymbol{k}_1^{*(\tau,\kappa,\iota)}, ..., \boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,...,m;\kappa=0,...,f_\tau;\iota=0,1}).$$

devolver

El proceso del algoritmo Dec se describirá haciendo referencia a la figura 11.

Los procesos de (S401) a (S404) son los mismos que en la realización 2.

(S405: Etapa de cálculo de coeficientes)

Con el dispositivo de procesamiento, una parte de cálculo de coeficientes 332 de la parte de cálculo de coeficientes 330 complementaria calcula los coeficientes $(\alpha_1, ..., \alpha_L)$, , los coeficientes $(\beta_1, ..., \beta_L)$, y un grado κ con los que se establece la fórmula 176.

[Fórmula 176]

$$h_{\tau,\kappa,0}(x) \cdot d_\tau(x)^\kappa = a_0(x) + \sum_{i=1}^{L} \alpha_i a_i(x), \text{ y}$$
$$h_{\tau,\kappa,1}(x) \cdot d_\tau(x)^{f_\tau - \kappa} = b_0(x) + \sum_{i=1}^{L} \beta_i b_i(x)$$

Se debe observar que $\alpha_i = 0 = \beta_i$ con respecto a todo i no incluido en $I_{(\rho,\Gamma)}$. Asimismo, $h_{\tau,\kappa,\iota}(x) := h_{\tau,\kappa,\iota,0} + h_{\tau,\kappa,\iota,1}x + \ldots h_{\tau,\kappa,\iota,\mu}x^\mu$ con respecto a todos los enteros τ de τ= 1, …, m y todos los enteros ι de ι = 0, 1.

(S406: Etapa de operación de emparejamiento)

Una parte de operación de emparejamiento 341 de una parte de desencriptación 340 genera las claves de sesión $K_{\tau,0}$ y $K_{\tau,1}$ calculando la fórmula 177 con el dispositivo de procesamiento.

[Fórmula 177]

$$K_{\tau,0} := e(\boldsymbol{c}_0, \sum_{j=0}^{\mu} h_{\tau,\kappa,0,j} \boldsymbol{k}_{0,j}^{*(\tau,\kappa,0)}) \cdot e(\boldsymbol{c}_0, \boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,0)}) \cdot$$
$$\prod_{i \in I_\delta,+} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i} \cdot \prod_{i \in I_\delta,-} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i/(\vec{v}_i \cdot \vec{x}_t)},$$

$$K_{\tau,1} := e(\boldsymbol{c}_0, \sum_{j=0}^{\mu} h_{\tau,\kappa,1,j} \boldsymbol{k}_{0,j}^{*(\tau,\kappa,1)}) \cdot e(\boldsymbol{c}_0, \boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,1)}) \cdot$$
$$\prod_{i \in I_\delta,+} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa,1)})^{\beta_i} \cdot \prod_{i \in I_\delta,-} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa,1)})^{\beta_i/(\vec{v}_i \cdot \vec{x}_t)},$$

donde $I_{\delta,+} := \{i \in I_\delta \mid \rho(i) = (t, \vec{v}_i)\}$ y $I_{\delta,-} := \{i \in I_\delta \mid \rho(i) = \neg(t, \vec{v}_i)\}$

(S407: Etapa de cálculo de mensajes)

Una parte de cálculo de mensajes 342 genera un mensaje msg' (= msg) calculando la fórmula 178 con el dispositivo de procesamiento.

[Fórmula 178]

$$msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0} K_{\tau,1})$$

Se debe observar que se puede obtener g_T^{ζ}, calculando la fórmula 177, tal como se indica en la fórmula 179. Por lo tanto, calculando la fórmula 178, se puede obtener el mensaje msg' (= msg) m.

[Fórmula 179]

$$K_{\tau,0} := e(\boldsymbol{c}_0, \sum_{j=0}^{\mu} h_{\tau,\kappa,0,j} \boldsymbol{k}_{0,j}^{*(\tau,\kappa,0)}) \cdot e(\boldsymbol{c}_0, \boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,0)}) \cdot$$

$$\prod_{i \in I_\delta,+} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i} \cdot \prod_{i \in I_\delta,-} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i / (\vec{v}_i \cdot \vec{x}_t)}$$

$$= g_T^{\delta\omega\left(\sum_{j=0}^{\mu} h_{\tau,\kappa,0,j} \gamma^j \cdot d_\tau(\gamma)^\kappa\right)} \cdot g_T^{\delta\omega\left(-a_0(\gamma) + \pi_{\tau,\kappa,0}\right) + \zeta\chi_{\tau,\kappa,0}}$$

$$\cdot g_T^{\delta\omega \sum_{i=1}^{L} \left(-\alpha_i a_i(\gamma) + \alpha_i \xi_{i,\tau,0}\right)}$$

$$= g_T^{\delta\omega h_{\tau,\kappa,0}(\gamma) \cdot d_\tau(\gamma)^\kappa} \cdot g_T^{-\delta\omega\left(a_0(\gamma) + \sum_{i=1}^{L} \alpha_i a_i(\gamma)\right)}$$

$$\cdot g_T^{\delta\omega\pi_{\tau,\kappa,0} + \zeta\chi_{\tau,\kappa,0} + \sum_{i=1}^{L} \alpha_i \xi_{i,\tau,0}}$$

$$= g_T^{\delta\omega\pi_{\tau,\kappa,0} + \zeta\chi_{\tau,\kappa,0} + \sum_{i=1}^{L} \alpha_i \xi_{i,\tau,0}}$$

$$K_{\tau,1} = g_T^{\delta\omega\pi_{\tau,\kappa,1} + \zeta\chi_{\tau,\kappa,1} + \sum_{i=1}^{L} \beta_i \xi_{i,\tau,1}}$$

$$\prod_{\tau=1}^{m} K_{\tau,0} K_{\tau,1} = g_T^{\sum_{\tau=1}^{m} (\delta\omega(\pi_{\tau,\kappa,0} + \pi_{\tau,\kappa,1}) + \zeta(\chi_{\tau,\kappa,0} + \chi_{\tau,\kappa,1}) + \sum_{i=1}^{L} (\alpha_i \xi_{i,\tau,0} + \beta_i \xi_{i,\tau,1}))}$$

$$= g_T^{\omega \sum_{\tau=1}^{m} \pi_\tau + \zeta \sum_{\tau=1}^{m} \chi_\tau + \omega \sum_{i=1}^{L} \alpha_i (\sum_{\tau=1}^{m} \xi_{i,\tau,0}) + \omega \sum_{i=1}^{L} \beta_i (\sum_{\tau=1}^{m} \xi_{i,\tau,1})}$$

$$= g_T^{\zeta}$$

En resumen, desde (S401) hasta (S407), el dispositivo de desencriptación 300 genera el mensaje msg' (= msg) ejecutando el algoritmo Dec indicado en la fórmula 180.

[Fórmula 180]

$$\mathrm{Dec}(\mathrm{pk}, \mathrm{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_{0,0}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,\iota)},$$

$$\boldsymbol{k}_1^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}),$$

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

si $\mathbb{S} := (\mathcal{A}, \mathcal{B}, d(x), \rho)$ acepta $\Gamma := \{(t, \vec{x}_t)\}$,

entonces, calcular $I_\delta \subseteq \{1,...,L\}, (\alpha_1,...,\alpha_L), (\beta_1,...,\beta_L)$ y κ con $h_{\tau,\kappa,\iota}(x) := h_{\tau,\kappa,\iota,0} + h_{\tau,\kappa,\iota,1}\, x + \cdots + h_{\tau,\kappa,\iota,\mu}\, x^\mu$ para todo $\tau = 1,...,m$ y $\iota = 0,1$ de tal manera que

$$h_{\tau,\kappa,0}(x) \cdot d_\tau(x)^\kappa = a_0(x) + \sum_{i=1}^{L} \alpha_i a_i(x), \text{ y}$$

$$h_{\tau,\kappa,1}(x) \cdot d_\tau(x)^{f_\tau - \kappa} = b_0(x) + \sum_{i=1}^{L} \beta_i b_i(x),$$

$$K_{\tau,0} := e(\boldsymbol{c}_0, \sum_{j=0}^{\mu} h_{\tau,\kappa,0,j} \boldsymbol{k}_{0,j}^{*(\tau,\kappa,0)}) \cdot e(\boldsymbol{c}_0, \boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,0)}) \cdot \prod_{i \in I_\delta,+} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i} \cdot \prod_{i \in I_\delta,-} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i / (\vec{v}_i \cdot \vec{x}_t)},$$

$$K_{\tau,1} := e(\boldsymbol{c}_0, \sum_{j=0}^{\mu} h_{\tau,\kappa,1,j} \boldsymbol{k}_{0,j}^{*(\tau,\kappa,1)}) \cdot e(\boldsymbol{c}_0, \boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,1)}) \cdot \prod_{i \in I_\delta,+} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa,1)})^{\beta_i} \cdot \prod_{i \in I_\delta,-} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa,1)})^{\beta_i / (\vec{v}_i \cdot \vec{x}_t)},$$

donde $I_{\delta,+} := \{i \in I_\delta \mid \rho(i) = (t, \vec{v}_i)\}$ y $I_{\delta,-} := \{i \in I_\delta \mid \rho(i) = \neg(t, \vec{v}_i)\}$.

devolver

$$msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0} K_{\tau,1}).$$

Tal como se ha descrito anteriormente, un sistema criptográfico 10 según la realización 4 implementa el esquema de encriptación funcional tratando el elemento obtenido sustituyendo el valor aleatorio γ en el polinomio $d_\tau(x)^\kappa$ y el elemento obtenido sustituyendo el valor aleatorio γ en el polinomio $d_\tau(x)^{f_\tau - \kappa}$, como elementos clave.

El esquema KP-FE se ha descrito anteriormente. Si el algoritmo KeyGen, el algoritmo Enc y el algoritmo Dec se modifican tal como se indica en las fórmulas 181 a 184, puede realizarse el esquema CP-FE. Se debe observar que el algoritmo Setup es el mismo entre el esquema KP-FE y el esquema CP-FE.

[Formula 181]

$$\text{KeyGen}(\text{pk}, \text{sk}, \Gamma := \{(t, \vec{x}_t) \mid 1 \le t \le d\}):$$

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

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

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

$$\boldsymbol{k}_0^* := (\overbrace{\omega,\ 0,...,0,}^{n_0}\ \overbrace{0,...,0,}^{u_0}\ \overbrace{\vec{\varphi}_0,}^{w_0}\ \overbrace{0,...,0,1}^{z_0})\, \mathbb{B}_0^*,$$

$$\boldsymbol{k}_t^* := (\overbrace{\vec{\omega x}_t}^{n_t},\ \overbrace{0,...,0}^{u_t},\ \overbrace{0,...,0,}^{w_t}\ \overbrace{\vec{\varphi}_t,}^{z_t}\ \overbrace{0,...,0}^{})\ \mathbb{B}_t^*\ ,\ \text{para}\ (t,\vec{x}_t)\in\Gamma,$$

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

[Fórmula 182]

$$\mathsf{Enc}\left(\mathsf{pk},\ msg,\ \mathbb{S} := (\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho)\right):$$

$$\pi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,...,m-1),\ \ \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,...,m;\ \kappa=0,...,f_\tau),$$

$$\chi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,...,m-1),\ \ \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,...,m;\ \kappa=0,...,f_\tau),$$

para $\tau=1,...,m,\ \ \kappa=0,...,f_\tau,\ \ \iota=0,1,$

$$\gamma \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \ \vec{\eta}_{0,0},...,\vec{\eta}_{0,\mu} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0},\ \ \vec{\eta}_{0,\mu+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0-1}$$

para $j=0,...,\mu,$

$$c_{0,j}^{(\tau,\kappa,0)} := (\overbrace{\delta(\gamma^j\cdot d_\tau(\gamma)^\kappa,\ \vec{e}_0^{(\tau,\kappa,0)})}^{n_0},\ \overbrace{0,...,0,}^{u_0}\ \overbrace{0,...,0,}^{w_0}\ \overbrace{\vec{\eta}_{0,j}}^{z_0})\ \mathbb{B}_0\ ,$$

$$c_{0,j}^{(\tau,\kappa,1)} := (\overbrace{\delta(\gamma^j\cdot d_\tau(\gamma)^{f_\tau-\kappa},\ \vec{e}_0^{(\tau,\kappa,1)})}^{n_0},\ \overbrace{0,...,0,}^{u_0}\ \overbrace{0,...,0,}^{w_0}\ \overbrace{\vec{\eta}_{0,j}}^{z_0})\ \mathbb{B}_0\ ,$$

$$s_0 := -a_0(\gamma)\ \text{si}\ \iota=0,\ \ s_0 := -b_0(\gamma)\ \text{si}\ \iota=1,$$

$$c_{0,\mu+1}^{(\tau,\kappa,\iota)} := (\overbrace{\delta(s_0+\pi_{\tau,\kappa,\iota},\ \vec{e}_0^{(\tau,\kappa,\iota)})}^{n_0},\ \overbrace{0,...,0,}^{u_0}\ \overbrace{0,...0,}^{w_0}\ \overbrace{\vec{\eta}_{0,\mu+1},\ \zeta\chi_{\tau,\kappa,\iota}}^{z_0})\ \mathbb{B}_0\ ,$$

[Fórmula 183]

para $i=1,...,L,$

$$\xi_{i,\tau,\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q\ \ (i=1,...,L;\ \tau=1,...,m-1;\iota=0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1}\xi_{i,\tau,\iota}\ (i=1,...,L;\ \iota=0,1),$$

$$s_i := -a_i(\gamma)+\xi_{i,\tau,0}\ \text{si}\ \iota=0,\qquad s_i := -b_i(\gamma)+\xi_{i,\tau,1}\ \text{si}\ \iota=1,$$

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

$$c_i^{(\tau,\kappa,\iota)} := (\overbrace{\delta(s_i\vec{e}_1+\theta_i\vec{v}_i),\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,...,0,}^{u_t}\ \overbrace{0,...,0,}^{w_t}\ \overbrace{\vec{\eta}_i}^{z_t})_{\mathbb{B}_t},$$

si $\rho(i) = \neg(t,\vec{v}_i), \qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_t},$

$$c_i^{(\tau,\kappa,\iota)} := (\overbrace{\delta s_i\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,...,0,}^{u_t}\ \overbrace{0,...,0,}^{w_t}\ \overbrace{\vec{\eta}_i}^{z_t})_{\mathbb{B}_t},$$

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

devolver

$$\mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, \{c_{0,0}^{(\tau,\kappa,\iota)},...,c_{0,\mu+1}^{(\tau,\kappa,\iota)},$$
$$c_1^{(\tau,\kappa,\iota)},...,c_L^{(\tau,\kappa,\iota)}\}_{\tau=1,...,m;\kappa=0,...,f_\tau;\iota=0,1}, c_{d+1}).$$

[Fórmula 184]

$$\mathsf{Dec}(\mathsf{pk}, \mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, \{c_{0,0}^{(\tau,\kappa,\iota)},...,c_{0,\mu+1}^{(\tau,\kappa,\iota)},$$
$$c_1^{(\tau,\kappa,\iota)},...,c_L^{(\tau,\kappa,\iota)}\}_{\tau=1,...,m;\kappa=0,...,f_\tau;\iota=0,1}, c_{d+1}),$$
$$\mathsf{sk}_\Gamma := (\Gamma, k_0^*, \{k_t^*\}_{(t,\vec{x}_t)\in\Gamma})):$$

si $\mathbb{S} := (\mathcal{A},\mathcal{B},d(x),\ \rho)_{\text{acepta}}\ \Gamma := \{(t,\vec{x}_t)\},$

entonces calcular $I_\delta \subseteq \{1,...,L\}, (\alpha_1,...,\alpha_L),\ (\beta_1,...,\beta_L)$ y

κ con $h_{\tau,\kappa,\iota}(x) := h_{\tau,\kappa,\iota,0} + h_{\tau,\kappa,\iota,1}\ x + \cdots + h_{\tau,\kappa,\iota,\mu}\ x^\mu$

para todo $\tau = 1,...,m$ y $\iota = 0,1$ de tal manera que

$$h_{\tau,\kappa,0}(x)\cdot d_\tau(x)^\kappa = a_0(x) + \sum_{i=1}^{L}\alpha_i a_i(x), \text{ y}$$

$$h_{\tau,\kappa,1}(x)\cdot d_\tau(x)^{f_\tau-\kappa} = b_0(x) + \sum_{i=1}^{L}\beta_i b_i(x),$$

$$K_{\tau,0} := e(k_0^*, \sum_{j=0}^{\mu} h_{\tau,\kappa,0,j}c_{0,j}^{(\tau,\kappa,0)})\cdot e(k_0^*, c_{0,\mu+1}^{(\tau,\kappa,0)})\cdot$$
$$\prod_{i\in I_\delta,+} e(k_t^*, c_i^{(\tau,\kappa,0)})^{\alpha_i}\cdot\prod_{i\in I_\delta,-} e(k_t^*, c_i^{(\tau,\kappa,0)})^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)},$$

$$K_{\tau,1} := e(k_0^*, \sum_{j=0}^{\mu} h_{\tau,\kappa,1,j}c_{0,j}^{(\tau,\kappa,1)})\cdot e(k_0^*, c_{0,\mu+1}^{(\tau,\kappa,1)})\cdot$$
$$\prod_{i\in I_\delta,+} e(k_t^*, c_i^{(\tau,\kappa,1)})^{\beta_i}\cdot\prod_{i\in I_\delta,-} e(k_t^*, c_i^{(\tau,\kappa,1)})^{\beta_i/(\vec{v}_i\cdot\vec{x}_t)},$$

donde $I_{\delta,+} := \{i \in I_\delta \mid \rho(i) = (t, \vec{v}_i)\}$ y $I_{\delta,-} := \{i \in I_\delta \mid \rho(i) = \neg(t, \vec{v}_i)\}$.

devolver

$$msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0} K_{\tau,1}).$$

El esquema de encriptación funcional se ha descrito anteriormente. Si el algoritmo KeyGen y el algoritmo Dec se modifican tal como se indica a continuación, en las fórmulas 185 a 187, se puede realizar un esquema de encriptación basado en atributos. Con el esquema de encriptación basado en atributos, en el algoritmo Setup, n_t es $2mf_{max}k_{max} + 2$. El algoritmo Setup es el mismo que el algoritmo Setup indicado en la fórmula 149, y el algoritmo Enc es el mismo que el algoritmo Enc indicado en la fórmula 152.

[Fórmula 185]

$$\mathsf{KeyGen}\left(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (\mathcal{A}, \mathcal{B}, d(x) = \prod_{\tau=1}^{m} d_\tau(x)^{f_\tau}, \rho)\right):$$

$$\pi_\tau \xleftarrow{\cup} \mathbb{F}_q,\ (\tau = 1,\ldots,m-1),\ \pi_m := -\sum_{\tau=1}^{m-1} \pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\cup} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau = 1,\ldots,m;\ \kappa = 0,\ldots,f_\tau),$$

$$\chi_\tau \xleftarrow{\cup} \mathbb{F}_q,\ (\tau = 1,\ldots,m-1),\ \chi_m := 1 - \sum_{\tau=1}^{m-1} \chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\cup} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau = 1,\ldots,m;\ \kappa = 0,\ldots,f_\tau),$$

para $\tau = 1,\ldots,m,\ \kappa = 0,\ldots,f_\tau,\ \iota = 0,1,$

$$\gamma \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_{0,0},\ldots,\vec{\eta}_{0,\mu+1} \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$

para $j = 0,\ldots,\mu,$

$$k_{0,j}^{*(\tau,\kappa,0)} := (\overbrace{\delta(\gamma^j \cdot d_\tau(\gamma)^\kappa,\ \vec{e}_0^{(\tau,\kappa,0)})}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_{0,j}}^{w_0},\ \overbrace{0,\ldots,0}^{z_0})\,\mathbb{B}_0^*,$$

$$k_{0,j}^{*(\tau,\kappa,1)} := (\overbrace{\delta(\gamma^j \cdot d_\tau(\gamma)^{f_\tau-\kappa},\ \vec{e}_0^{(\tau,\kappa,1)})}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_{0,j}}^{w_0},\ \overbrace{0,\ldots,0}^{z_0})\,\mathbb{B}_0^*,$$

$s_0 := -a_0(\gamma)$ si $\iota = 0,\ s_0 := -b_0(\gamma)$ si $\iota = 1,$

$$k_{0,\mu+1}^{*(\tau,\kappa,\iota)} := (\overbrace{\delta(s_0 + \pi_{\tau,\kappa,\iota},\ \vec{e}_0^{(\tau,\kappa,\iota)})}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_{0,\mu+1}}^{w_0},\ \overbrace{0,\ldots 0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\,\mathbb{B}_0^*,$$

[Fórmula 186]

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

$$\xi_{i,\tau,\iota} \xleftarrow{U} \mathbb{F}_q \ (i=1,\ldots,L;\ \tau=1,\ldots,m-1;\iota=0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota} (i=1,\ldots,L;\ \iota=0,1),$$

$$s_i := -a_i(\gamma)+\xi_{i,\tau,0} \text{ si } \iota=0, \qquad s_i := -b_i(\gamma)+\xi_{i,\tau,1} \text{ si } \iota=1,$$

si $\rho(i)=(t,v_i), \qquad \theta_i \xleftarrow{U} \mathbb{F}_q, \quad \vec{\eta}_i \xleftarrow{U} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{\delta(s_i+\theta_i v_i,\ -\theta_i,\ \vec{e}_i^{(\tau,\kappa,\iota)})}^{n_t},\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^*,$$

si $\rho(i)=(t,v_i), \qquad \vec{\eta}_i \xleftarrow{U} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{\delta(s_i v_i,\ s_i,\ \vec{e}_i^{(\tau,\kappa,\iota)})}^{n_t},\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^*,$$

devolver $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_{0,0}^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,\iota)},$

$$\boldsymbol{k}_1^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}).$$

[Fórmula 187]

$$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_{0,0}^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,\iota)},$$

$$\boldsymbol{k}_1^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}),$$

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

si $\mathbb{S} := (\mathcal{A},\mathcal{B},d(x),\ \rho)$ acepta $\Gamma := \{(t,x_t)\},$

entonces, calcular $I_\delta \subseteq \{1,\ldots,L\}, (\alpha_1,\ldots,\alpha_L),\ (\beta_1,\ldots,\beta_L)$ y

κ $h_{\tau,\kappa,\iota}(x) := h_{\tau,\kappa,\iota,0} + h_{\tau,\kappa,\iota,1}\,x+\cdots+h_{\tau,\kappa,\iota,\mu}\,x^\mu$

para todo $\tau=1,\ldots,m$ and $\iota=0,1$ de tal manera que

$$h_{\tau,\kappa,0}(x)\cdot d_\tau(x)^\kappa = a_0(x)+\sum_{i=1}^{L}\alpha_i a_i(x),$$ y

$$h_{\tau,\kappa,1}(x)\cdot d_\tau(x)^{f_\tau-\kappa}=b_0(x)+\sum_{i=1}^{L}\beta_i b_i(x),$$

$$K_{\tau,0}:=e(c_0,\sum_{j=0}^{\mu}h_{\tau,\kappa,0,j}k_{0,j}^{*(\tau,\kappa,0)})\cdot e(c_0,k_{0,\mu+1}^{*(\tau,\kappa,0)})\cdot$$

$$\prod_{i\in I_\delta,+}e(c_t,k_i^{*(\tau,\kappa,0)})^{\alpha_i}\cdot\prod_{i\in I_\delta,-}e(c_t,k_i^{*(\tau,\kappa,0)})^{\alpha_i/(v_i-x_t)},$$

$$K_{\tau,1}:=e(c_0,\sum_{j=0}^{\mu}h_{\tau,\kappa,1,j}k_{0,j}^{*(\tau,\kappa,1)})\cdot e(c_0,k_{0,\mu+1}^{*(\tau,\kappa,1)})\cdot$$

$$\prod_{i\in I_\delta,+}e(c_t,k_i^{*(\tau,\kappa,1)})^{\beta_i}\cdot\prod_{i\in I_\delta,-}e(c_t,k_i^{*(\tau,\kappa,1)})^{\beta_i/(v_i-x_t)},$$

donde $I_{\delta,+}:=\{i\in I_\delta\mid\rho(i)=(t,v_i)\}$ y $I_{\delta,-}:=\{i\in I_\delta\mid\rho(i)=\neg(t,v_i)\}.$

devolver

$$msg':=c_{d+1}/(\prod_{\tau=1}^{m}K_{\tau,0}K_{\tau,1}).$$

Realizando la misma modificación, el esquema CP-FE indicado en las fórmulas 181 a 184 puede ser alterado al esquema de encriptación basado en atributos.

En la explicación anterior, $n_0 + u_0 + w_0 + z_0$ se configura en N_0 y $n_t + u_t + w_t + z_t$ se configura en N_t. Si, por ejemplo, $u_0 = n_0$, $w_0 = n_0$, y $z_0 = 2$, entonces $n_0 + n_0 + n_0 + 2 = 3n_0 + 2$ puede configurarse en N_0. Si $u_t = n_t$, $w_t = n_t$ y $z_t = 2$, entonces $n_t + n_t + n_t + 2 = 3n_t + 2$ puede configurarse en N_t.

La explicación anterior presenta un esquema de encriptación funcional en el que, con el esquema de encriptación funcional según la realización 2, la longitud de la clave de desencriptación y el texto cifrado aumenta, pero el número de bases disminuye. Basándose en el esquema de encriptación funcional según las realizaciones 3 y 4, el esquema de encriptación funcional según la realización 4 puede transformarse fácilmente en un esquema de encriptación funcional en el que el número de bases aumenta, pero el número de grados de cada base disminuye, como con el esquema de encriptación funcional según la realización 3.

Las realizaciones anteriores explicaron el esquema KP-FE y el esquema CP-FE. El esquema FE de política unificada (UP-FE – Unified Policy FE, en inglés) descrito en la bibliografía de no de patente 4 puede ser construido fácilmente a partir del esquema KP-FE y del esquema CP-FE.

Realización 5.

En las realizaciones anteriores, se ha descrito el método de implementar el proceso criptográfico en los espacios vectoriales dobles. En la realización 5, se describirá un método para implementar un proceso criptográfico en grupos aditivos dobles.

En resumen, en las realizaciones anteriores, se implementa un proceso primitivo criptográfico en el grupo cíclico del orden q primo. Si un anillo R se expresa utilizando un número compuesto M, como en la fórmula 188, el proceso criptográfico descrito en las realizaciones anteriores puede aplicarse a un grupo aditivo que tiene un anillo R como coeficiente.

[Fórmula 188]

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

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 primitivo criptográfico en el grupo aditivo doble.

En las realizaciones anteriores, desde el punto de vista de la prueba de seguridad, ρ(i) con respecto a cada entero i de i = 1, …, L puede limitarse a una tupla positiva $(t, v^{\rightarrow})$ o una tupla negativa $\neg(t, v^{\rightarrow})$ para diferente información de identificación t correspondiente.

En otras palabras, sea una función $\rho^{\sim}$ el mapa de {1, ..., L} → {1, ..., d} siendo $\rho^{\sim}(i)$ = t cuando $\rho(i) = (t, v^{\rightarrow})$ o $\rho(i) = \neg (t, v^{\rightarrow})$. En este caso, $\rho^{\sim}$ puede limitarse a la inyección. Se debe observar que ρ(i) es ρ(i) en la estructura de acceso S := (M, ρ(i)) descrita anteriormente.

En esta realización, se describirá la configuración de hardware de un sistema de procesamiento criptográfico 10 (un dispositivo de generación de claves 100, un dispositivo de encriptación 200 y un dispositivo de desencriptación 300).

La figura 13 es un diagrama que muestra un ejemplo de la configuración de hardware de cada dispositivo de generación de claves 100, el dispositivo de encriptación 200 y el dispositivo de desencriptación (300).

Tal como se muestra en la figura 13, cada uno del dispositivo de generación de claves 100, el dispositivo de encriptación 200, y el dispositivo de desencriptación 300 incluye una CPU 911 (unidad de procesamiento central – Central Processing Unit, en inglés; también denominada dispositivo de procesamiento central, dispositivo de procesamiento, dispositivo de cálculo, microprocesador, microordenador o procesador) que ejecuta programas. La CPU 911 está conectada a una ROM 913, una RAM 914, una pantalla LCD 901 (pantalla de cristal líquido – Liquid Crystal Display, en inglés), un teclado 902 (K/B – KeyBoard, en inglés), una placa de comunicación 915 y un dispositivo de disco magnético 920 a través de un bus 912, y controla estos dispositivos de 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 tarjeta de memoria de lectura / escritura. El dispositivo de disco magnético 920 está conectado a través de una interfaz de disco fija predeterminada.

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

El dispositivo de disco magnético 920, ROM 913 o similar almacena un sistema operativo 921 (OS – Operating System, en inglés), 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 "parte de generación de clave principal 110", "parte de almacenamiento de clave principal 120", "parte de introducción de información 130", "parte de generación de clave de desencriptación 140", “parte de distribución de clave 150", "parte de obtención de parámetros públicos 210", "parte de introducción de información 220", "parte de generación de datos encriptados 230", "parte de transmisión de datos 240", "parte de obtención de información 310" , “parte de cálculo de programa de amplitud 320”, “parte de cálculo de coeficientes complementarios 330", "parte de desencriptación 340", y similares en la descripción anterior, y otros programas. Los programas son leídos y ejecutados por la CPU 911.

Los archivos 924 almacenan información, datos, valores de señal, valores variables y parámetros tales como los "parámetros públicos pk", la "clave secreta principal sk", las "claves de desencriptación sk_v y sk_Γ", los "textos cifrados ct_Γ y ct_s", la "estructura de acceso S", la "información de atributos", el "mensaje msg", y similares de la explicación anterior, como los elementos de un "archivo" y "base de datos". El "archivo" y la "base de datos" se almacenan en un medio de grabación tal como un disco o memoria. La información, datos, valores de señal, valores de variable y parámetros almacenados en el medio de grabación tal como el disco o memoria son leídos a la memoria principal o memoria caché por la CPU 911 mediante un circuito de lectura / escritura y se utilizan para las operaciones de la CPU 911 tales como extracción, búsqueda (search), búsqueda (look-up), comparación, cálculo (computation), cálculo (calculation), salida, impresión y visualización. La información, los datos, los valores de las señales, los valores de las variables y los parámetros se almacenan temporalmente en la memoria principal, la memoria caché o la memoria intermedia durante las operaciones de la CPU 911, incluyendo extracción, búsqueda (search), búsqueda (look-up), comparación, cálculo (computation), cálculo (calculation), salida, impresión y visualización.

Las flechas de los diagramas de flujo en la explicación anterior indican principalmente entrada / salida de datos y señales. Los valores de datos y señales se registran en la memoria de la memoria 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", "medio" o "función"; o una "etapa", "procedimiento" o "proceso". El "dispositivo" puede ser un "circuito", "equipo", "medio", o "función"; o una "etapa", "procedimiento" o "proceso". El "proceso" puede ser una "etapa". Concretamente, la "parte" puede ser implementada mediante el firmware almacenado en la ROM 913. Alternativamente, la "parte" puede ser implementada solo mediante software; solo mediante hardware tal como un elemento, un dispositivo, un sustrato o una línea de cableado; mediante una combinación de software y hardware; o además mediante una combinación de software, hardware y firmware. El firmware y el software se almacenan, como programa, en el medio de grabación tal como la ROM 913. El programa es leído por la CPU 911 y ejecutado por la CPU 911. Concretamente, el programa hace que el ordenador o similar funcione como un "parte" descrita anteriormente. Alternativamente, el programa hace que el ordenador o similar ejecute el procedimiento y el método de la "parte" descrita anteriormente.

Lista de señales de referencia

100: dispositivo de generación de claves;

110: parte de generación de clave principal;

120: parte de almacenamiento de clave principal;

130: parte de introducción de información;

140: parte de generación de clave de desencriptación;

141: parte de generación de información secreta;

142: parte de generación de elementos clave;

150: parte de distribución de claves;

200: dispositivo de encriptación;

210: parte de obtención de parámetros públicos;

220: parte de introducción de información;

230: parte de generación de datos encriptados;

240: parte de transmisión de datos;

300: dispositivo de desencriptación;

311: parte de obtención de clave de desencriptación;

312: parte de obtención de texto cifrado;

320: parte de cálculo del programa de amplitud;

330: parte de cálculo de coeficientes complementarios;

331: parte de selección de polinomios;

332: parte de cálculo de coeficientes;

340: parte de desencriptación; 341: parte de operación de emparejamiento;

342: parte de cálculo de mensajes.

REIVINDICACIONES

1. Sistema criptográfico (10) que comprende un dispositivo de encriptación (200) y un dispositivo de desencriptación (300),

comprendiendo el dispositivo de encriptación

una parte de generación de texto cifrado (230) que genera una de primera información que incluye un programa de amplitud cuadrática, incluyendo el programa de amplitud cuadrática una serie de polinomios $D_i(x)$, y una información de predicado, y una segunda información que incluye información de atributos, tal como texto cifrado, comprendiendo el dispositivo de desencriptación

una parte de selección de polinomios (331) que, tratando una información restante de la primera y la segunda información, como una clave de desencriptación y basándose en la información de predicado incluida en la primera información y en la información de atributos incluida en la segunda información, selecciona al menos un polinomio $D_i(x)$ de la serie de polinomios $D_i(x)$,

una parte de cálculo de coeficientes (332) que calcula un coeficiente Δ_i, que permite que un polinomio constituido a partir de un polinomio $\Delta_i D_i(x)$ sea dividido por el polinomio d(x), obteniéndose el polinomio $\Delta_i D_i(x)$ multiplicando el polinomio $D_i(x)$ seleccionado por la parte de selección polinómica, por el coeficiente Δ_i, y

una parte de desencriptación (340) que desencripta el texto cifrado en base al coeficiente Δ_i, calculado por la parte de cálculo de coeficientes, si el programa de amplitud cuadrática acepta la información de atributos.

2. Sistema criptográfico según la reivindicación 1,

en donde la serie de polinomios Di(x) incluye un polinomio $a_i(x)$ y un polinomio $b_i(x)$ relativos a cada entero i de i = 0, …, L, siendo L un entero mayor o igual que 1,

en donde la parte de selección de polinomios, en base a la información de atributos y a la información de predicado, selecciona un conjunto I de un entero i de i = 1, …, L, por lo que seleccionar un polinomio $a_0(x)$ y un polinomio $b_0(x)$ y el polinomio $a_i(x)$ y el polinomio $b_i(x)$ relativos al número entero i incluido en el conjunto I, y

en donde la parte de cálculo de coeficientes calcula, como el coeficiente Δ_i, un coeficiente α_i, y un coeficiente β_i, que permiten que $(a_0(x) + \Sigma_{i\in I}\alpha_i a_i(x)) \cdot (b_0(x) + \Sigma_{i\in I}\beta_i b_i(x))$ sea dividido por el polinomio d(x).

3. El sistema criptográfico según la reivindicación 2,

en donde el polinomio d(x) es factorizado en un polinomio $d_\tau(x)^{f\tau}$ donde τ= 1, …, m, siendo m un entero mayor o igual que 1,

en donde la parte de cálculo de coeficientes calcula el coeficiente α_i, el coeficiente β_i y un grado κ_τ que permiten que $\Pi_{\tau=1}{}^m d_\tau(x)^{\kappa\tau}$ divida $(a_0(x) + \Sigma_{i\in I}\alpha_i a_i(x))$ y permiten que $\Pi_{\tau=1}{}^m d_\tau(x)^{f\tau-\kappa\tau}$ divida $(b_0(x) + \Sigma_{i\in I}\beta_i b_i(x))$, y

en donde la parte de desencriptación descifra el texto cifrado en base al coeficiente α_i, al coeficiente β_i y a un grado κ_τ.

4. Sistema criptográfico según la reivindicación 2 o 3,

en donde la información de atributos incluye un vector de atributos $\vec{x}_t$ relativo al menos a un entero t de t = 1, …, d, siendo d un entero mayor o igual que 1,

en donde la información de predicado incluye una tupla $(t, \vec{v}_i)$ de un identificador t y un vector de predicado $\vec{v}_i$ referente a cada entero i de i = 1, …, L y

en donde la parte de selección de polinomios determina, con respecto a la tupla $(t, \vec{v}_i)$ respecto a cada entero i de i = 1, …, L, independientemente de si el entero i debe incluirse o no en el conjunto I, en base a si es o no un producto interno del vector predicado $\vec{v}_i$ de la tupla y el vector de atributo $\vec{x}_t$ relativo a la información de identificación t de la tupla es 0.

5. El sistema criptográfico según la reivindicación 4,

en donde la tupla $(t, \vec{v}_i)$ está relacionada con cualquiera de una tupla positiva y una tupla negativa, y

en donde la parte de selección de polinomios, cuando la tupla $(t, \vec{v}_i)$ está relacionada con la tupla positiva, incluye el entero i en el conjunto I si el producto interno es 0 y cuando la tupla $(t, \vec{v}_i)$ está relacionada con la tupla negativa, incluye el entero i en el conjunto I si el producto interno no es 0.

6. Sistema criptográfico según una cualquiera de las reivindicaciones 1 a 5,

en donde el polinomio d(x) está factorizado en un polinomio $d_\tau(x)^{f\tau}$ donde τ = 1, ..., m, siendo m un entero mayor o igual que 1,

en donde la primera información incluye, para cada polinomio $d_\tau(x)^{f\tau}$, un elemento en el que se configura la información obtenida mediante el polinomio $d_\tau(x)^{f\tau}$, y

en donde la parte de desencriptación desencripta el texto cifrado en base al coeficiente Δ_i y el elemento.

7. Sistema criptográfico según la reivindicación 6,

en donde la primera información incluye, para cada polinomio $d_\tau(x)^{f\tau}$ y en relación con cada número entero de κ de κ = 0, ..., f_τ, y cada entero i de i = 0, …, L, un elemento en el cual se configura un resto de división del polinomio $a_i(x)$ por un polinomio $d_\tau(x)^{\kappa}$ y un elemento en el que se establece un resto de división del polinomio $b_i(x)$ por un polinomio $d_\tau(x)^{f\tau-\kappa}$.

8. Sistema criptográfico según la reivindicación 6,

en donde la primera información incluye, para cada polinomio $d_\tau(x)^{f\tau}$, un elemento en el que se configura un valor sustituido por un valor predeterminado γ.

9. Sistema criptográfico según una cualquiera de las reivindicaciones 6 a 8,

en donde la parte de desencriptación lleva a cabo, en base al coeficiente Δ_i, una operación predeterminada relativa al elemento con el fin de obtener información obtenida del polinomio $d_\tau(x)^{f\tau}$ a 0, desencriptando con ello el texto cifrado.

10. Procedimiento criptográfico que comprende:

una etapa de generación de texto cifrado de, con un dispositivo de encriptación (200), generar una de la primera información que incluye un programa de amplitud cuadrática, incluyendo el programa de amplitud cuadrática un polinomio d(x), una serie de polinomios $D_i(x)$, y una información de predicado y una segunda información que incluye información de atributos, como texto cifrado;

una etapa de selección de polinomios de, con un dispositivo de desencriptación (300), tratar la restante de una de la primera información y la segunda información como clave de desencriptación y en base a la información de predicado incluida en la primera información y en la información de atributos incluida en la segunda información, seleccionar al menos un polinomio $D_i(x)$ de la serie de polinomios $D_i(x)$;

una etapa de cálculo de coeficientes de, con el dispositivo de desencriptación, calcular un coeficiente Δ_i que permita que un polinomio constituido a partir de un polinomio $\Delta_i D_i(x)$ se divida por el polinomio d(x), obteniéndose el polinomio $\Delta_i D_i(x)$ multiplicando por el polinomio $D_i(x)$ seleccionado en la etapa de selección de polinomios por el coeficiente Δ_i; y

una etapa de desencriptación de, con el dispositivo de desencriptación, desencriptar el texto cifrado en base al coeficiente Δ_i calculado en la etapa de cálculo de coeficientes, si el programa de amplitud cuadrática acepta la información de atributos.

11. Programa criptográfico que hace que un ordenador ejecute un proceso de generación de encriptación de texto cifrado de generar una de la primera información que incluye un programa de amplitud cuadrática, incluyendo el programa de amplitud cuadrática un polinomio d(x), una serie de polinomios $D_i(x)$, y una información de predicado, y una segunda información que incluye información de atributos, como un texto cifrado,

un proceso de selección de polinomios de, tratando un resto de la primera información y la segunda información como una clave de desencriptación y en base a la información de predicado incluida en la primera información y a la información de atributos incluida en la segunda información seleccionando al menos un polinomio $D_i(x)$ de la serie de polinomios $D_i(x)$,

un proceso de cálculo de coeficientes para calcular un coeficiente Δ_i que permite que un polinomio constituido en base a un polinomio $\Delta_i D_i(x)$ sea dividido por el polinomio d(x), obteniéndose el polinomio $\Delta_i D_i(x)$ multiplicando el polinomio $D_i(x)$ seleccionado en el proceso de selección de polinomios, mediante el coeficiente Δ_i, y

un proceso de desencriptación para desencriptar el texto cifrado en base al coeficiente Δ_i calculado en el proceso de cálculo de coeficientes, si el programa de amplitud cuadrática acepta la información de atributos.

12. Dispositivo de desencriptación (300) que comprende:

una parte de obtención de información (310) que obtiene una de la primera información que incluye un programa de amplitud cuadrática, incluyendo el programa de amplitud cuadrática un polinomio d(x), una serie de polinomios $D_i(x)$, y una información de predicado, y una segunda información que incluye una información de atributos, como un texto cifrado, y una restante de la primera información y la segunda información, como una clave de desencriptación;

una parte de selección de polinomios (331) que, basándose en la información de predicado incluida en la primera información y en la información de atributos incluida en la segunda información, siendo la primera información y la segunda información generadas por la parte de obtención de información, selecciona al menos un polinomio $D_i(x)$ de la serie de polinomios $D_i(x)$;

una parte de cálculo de coeficientes (332) que calcula un coeficiente Δ_i que permite que un polinomio constituido en base a un polinomio $\Delta_i Di(x)$ sea dividido por el polinomio d(x), obteniéndose el polinomio $\Delta_i Di(x)$ multiplicando el polinomio $D_i(x)$ seleccionado mediante la parte de selección de polinomios, por el coeficiente Δ_i; y

una parte de desencriptación (340) que descifra el texto cifrado mediante la clave de desencriptación en base al coeficiente Δ_i, calculado mediante la parte de cálculo de coeficientes, si el programa de amplitud cuadrática acepta la información de atributos.

Fig. 1

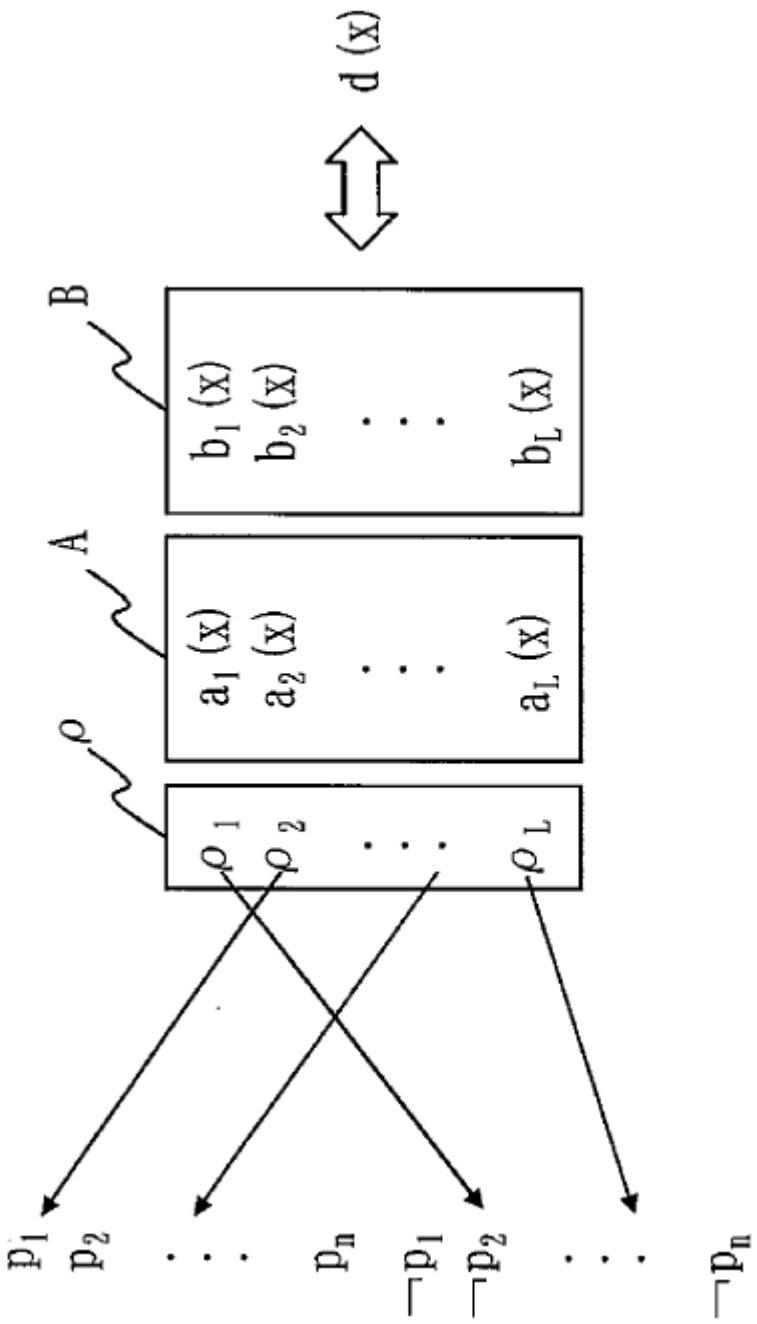


Fig. 2

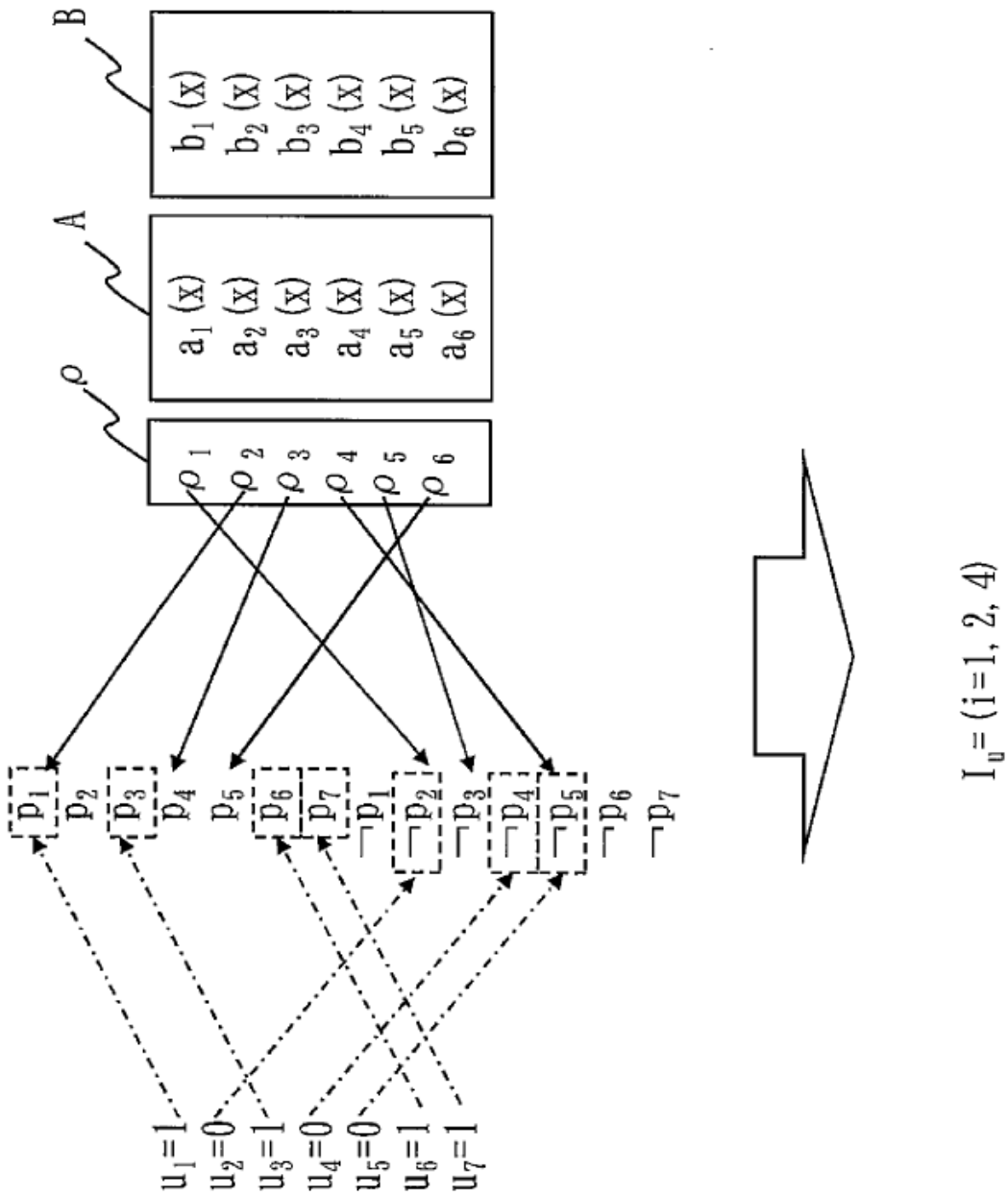

B
A
ρ
b1 (x) b2 (x) b3 (x) b4 (x) b5 (x) b6 (x)
a1 (x) a2 (x) a3 (x) a4 (x) a5 (x) a6 (x)
ρ 1 ρ 2 ρ 3 ρ 4 ρ 5 ρ 6
p1 p2 p3 p4 p5 p6 p7 ¬p1 ¬p2 ¬p3 ¬p4 ¬p5 ¬p6 ¬p7
u1=1 u2=0 u3=1 u4=0 u5=0 u6=1 u7=1
Iu= (i=1, 2, 4)

Fig. 3

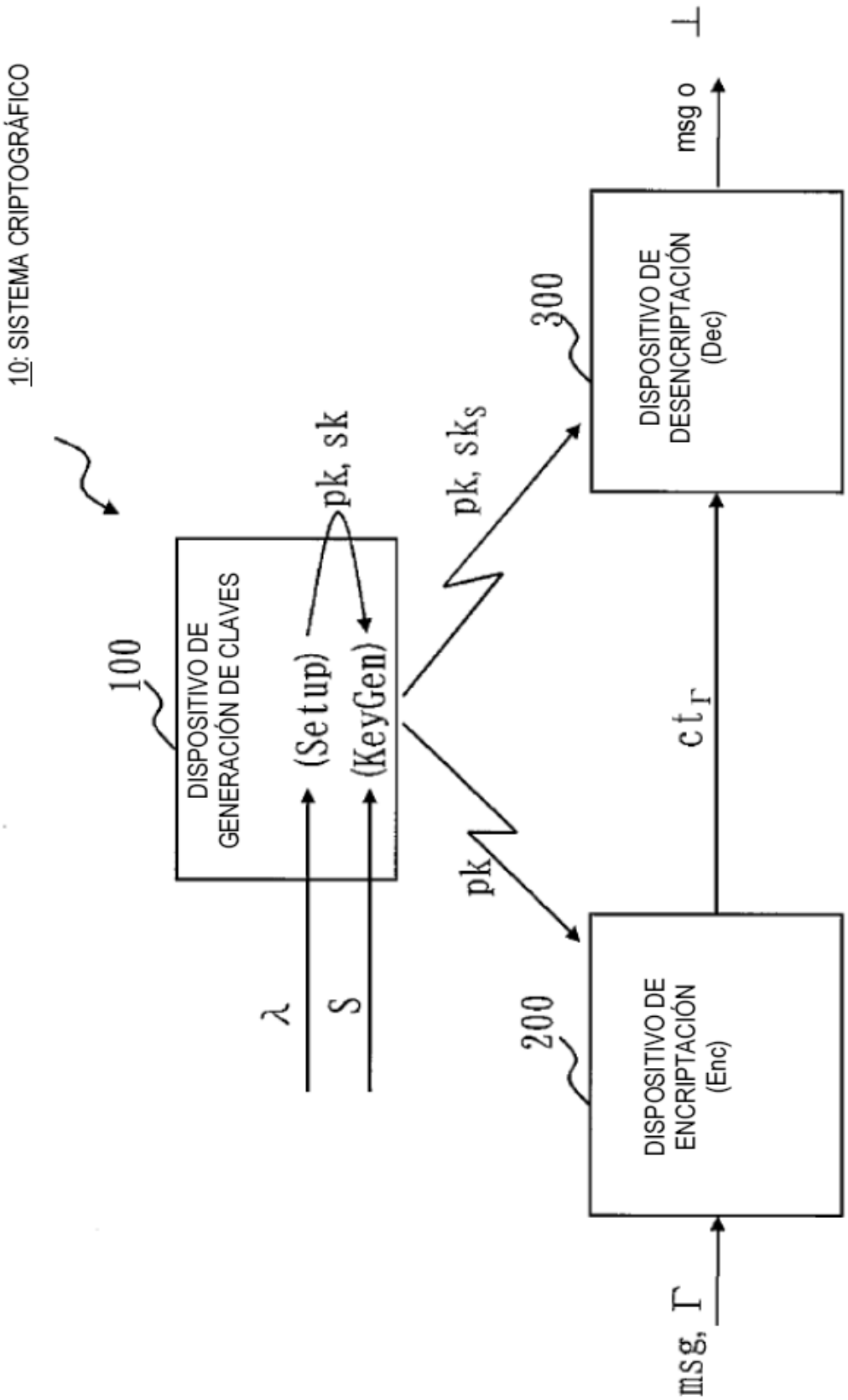

10: SISTEMA CRIPTOGRÁFICO
100
DISPOSITIVO DE GENERACIÓN DE CLAVES
(Setup)
(KeyGen)
λ
S
pk, sk
pk
pk, sk_S
200
DISPOSITIVO DE ENCRIPTACIÓN (Enc)
300
DISPOSITIVO DE DESENCRIPTACIÓN (Dec)
msg, Γ
ct_Γ
msg o ⊥

Fig. 4

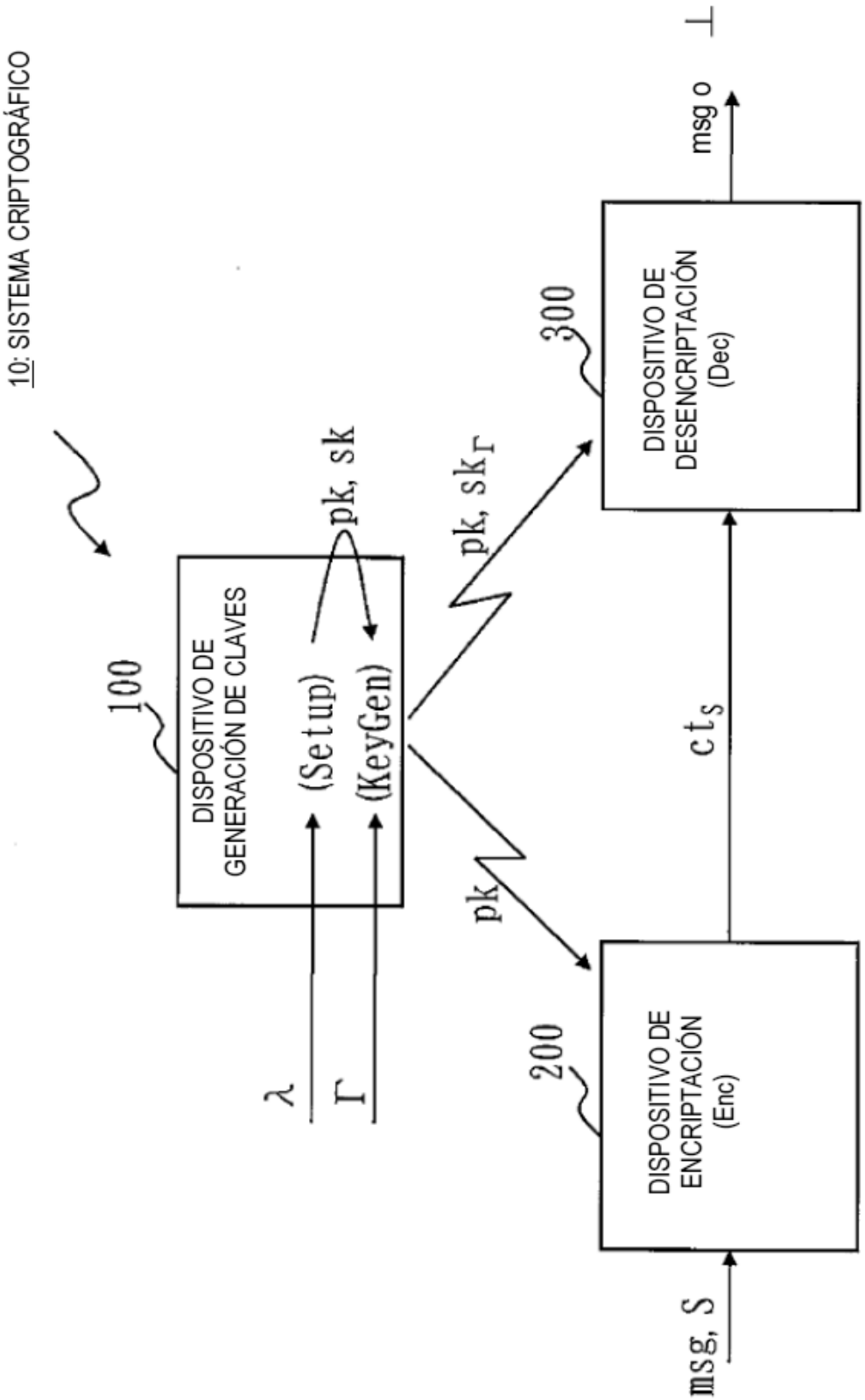

10: SISTEMA CRIPTOGRÁFICO
100
DISPOSITIVO DE GENERACIÓN DE CLAVES
(Setup)
(KeyGen)
λ
Γ
pk, sk
pk, skΓ
pk
300
DISPOSITIVO DE DESENCRIPTACIÓN (Dec)
msg o ⊥
200
DISPOSITIVO DE ENCRIPTACIÓN (Enc)
msg, S
ctS

Fig. 5

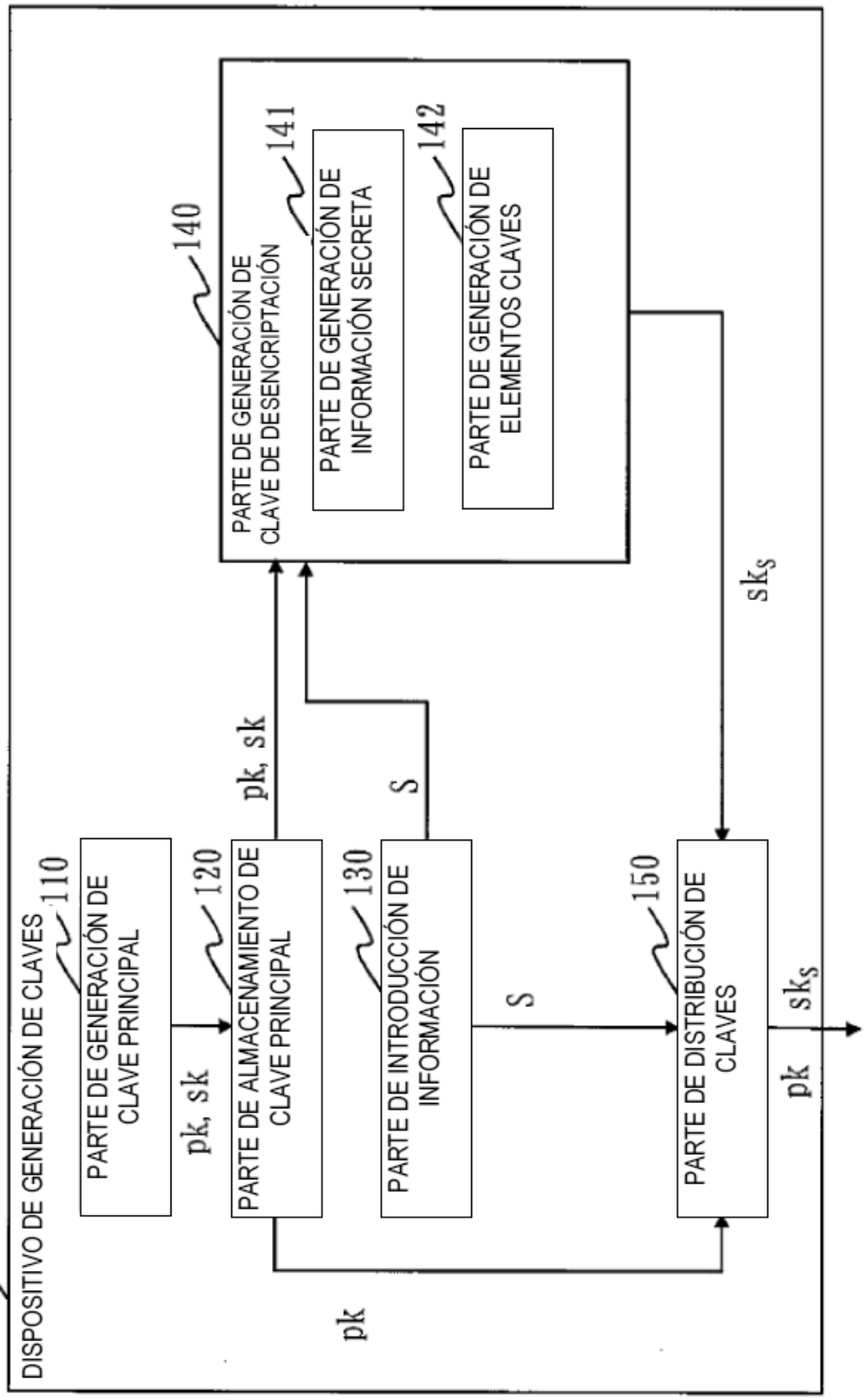

100
DISPOSITIVO DE GENERACIÓN DE CLAVES
110
PARTE DE GENERACIÓN DE CLAVE PRINCIPAL
120
PARTE DE ALMACENAMIENTO DE CLAVE PRINCIPAL
130
PARTE DE INTRODUCCIÓN DE INFORMACIÓN
140
PARTE DE GENERACIÓN DE CLAVE DE DESENCRIPTACIÓN
141
PARTE DE GENERACIÓN DE INFORMACIÓN SECRETA
142
PARTE DE GENERACIÓN DE ELEMENTOS CLAVES
150
PARTE DE DISTRIBUCIÓN DE CLAVES
pk, sk
pk, sk
S
S
pk
pk
sk$_S$
sk$_S$

Fig. 6

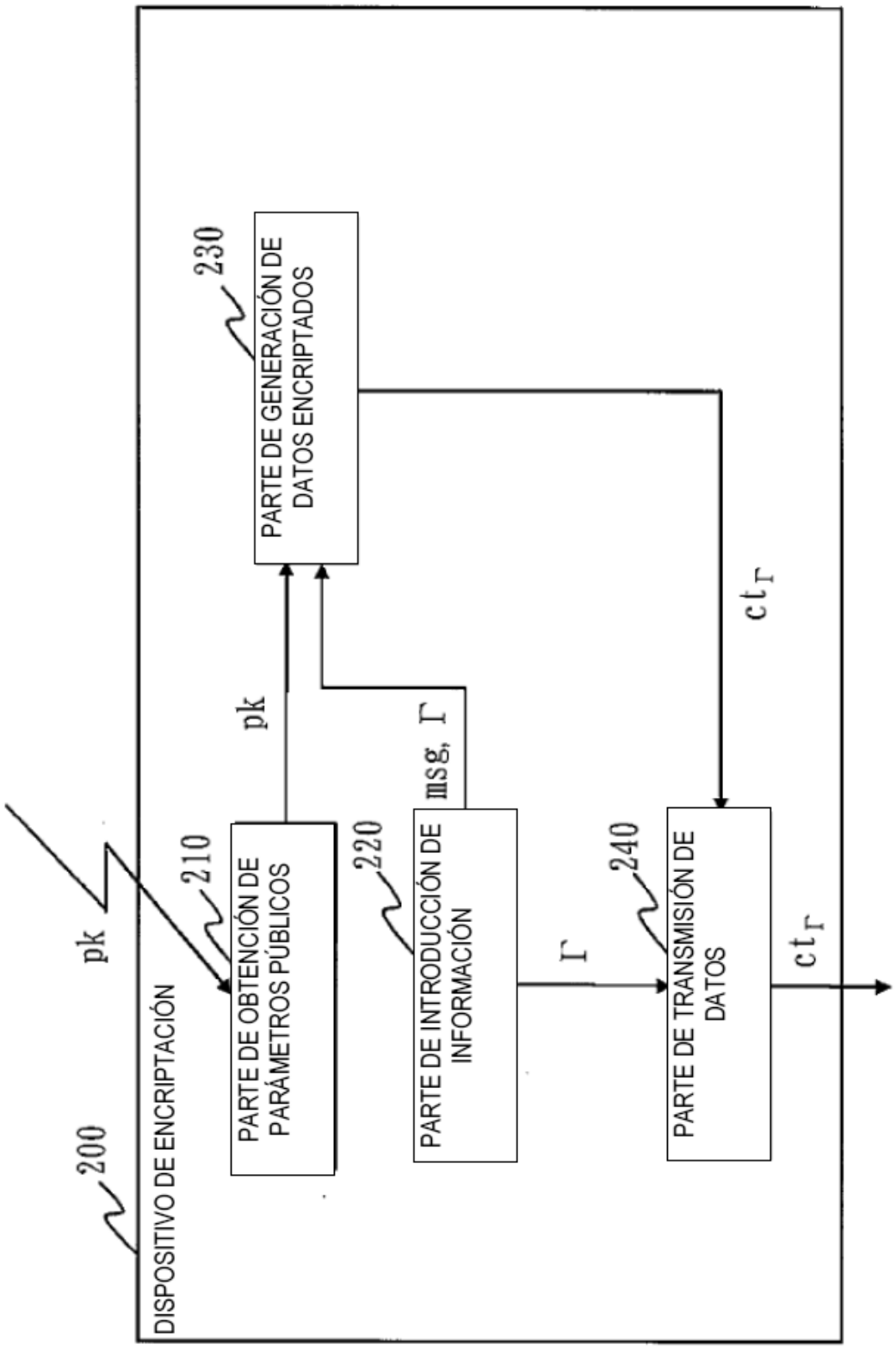

DISPOSITIVO DE ENCRIPTACIÓN
200
pk
PARTE DE OBTENCIÓN DE PARÁMETROS PÚBLICOS
210
pk
PARTE DE INTRODUCCIÓN DE INFORMACIÓN
220
msg, Γ
Γ
PARTE DE GENERACIÓN DE DATOS ENCRIPTADOS
230
ct_Γ
PARTE DE TRANSMISIÓN DE DATOS
240
ct_Γ

Fig. 7

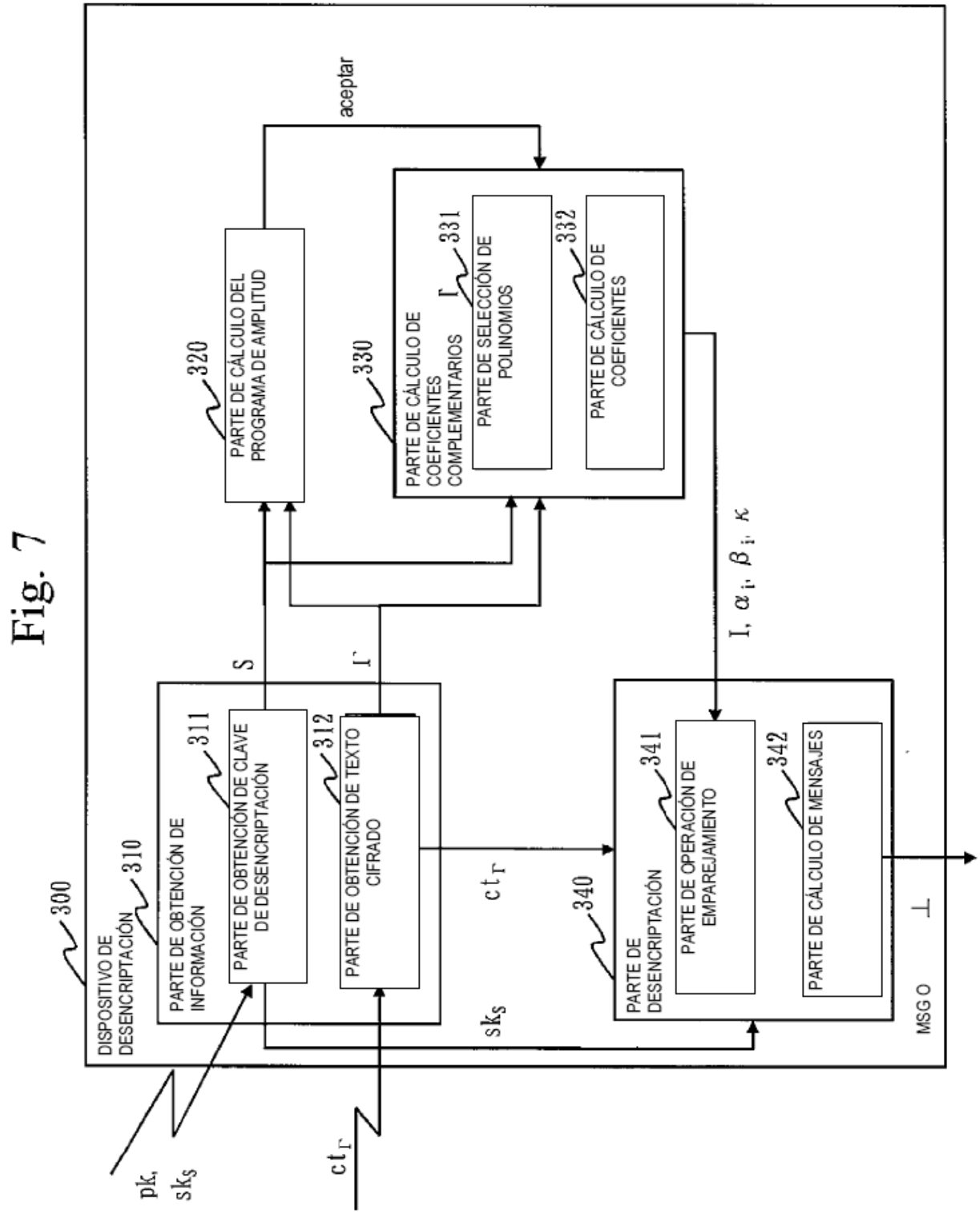

300
DISPOSITIVO DE DESENCRIPTACIÓN
310
PARTE DE OBTENCIÓN DE INFORMACIÓN
311
PARTE DE OBTENCIÓN DE CLAVE DE DESENCRIPTACIÓN
312
PARTE DE OBTENCIÓN DE TEXTO CIFRADO
320
PARTE DE CÁLCULO DEL PROGRAMA DE AMPLITUD
330
PARTE DE CÁLCULO DE COEFICIENTES COMPLEMENTARIOS
331
PARTE DE SELECCIÓN DE POLINOMIOS
332
PARTE DE CÁLCULO DE COEFICIENTES
340
PARTE DE DESENCRIPTACIÓN
341
PARTE DE OPERACIÓN DE EMPAREJAMIENTO
342
PARTE DE CÁLCULO DE MENSAJES
aceptar
S
Γ
I, α_i, β_i, κ
ct_Γ
sk_S
MSG O
⊥
pk,
sk_S
ct_Γ

Fig. 8

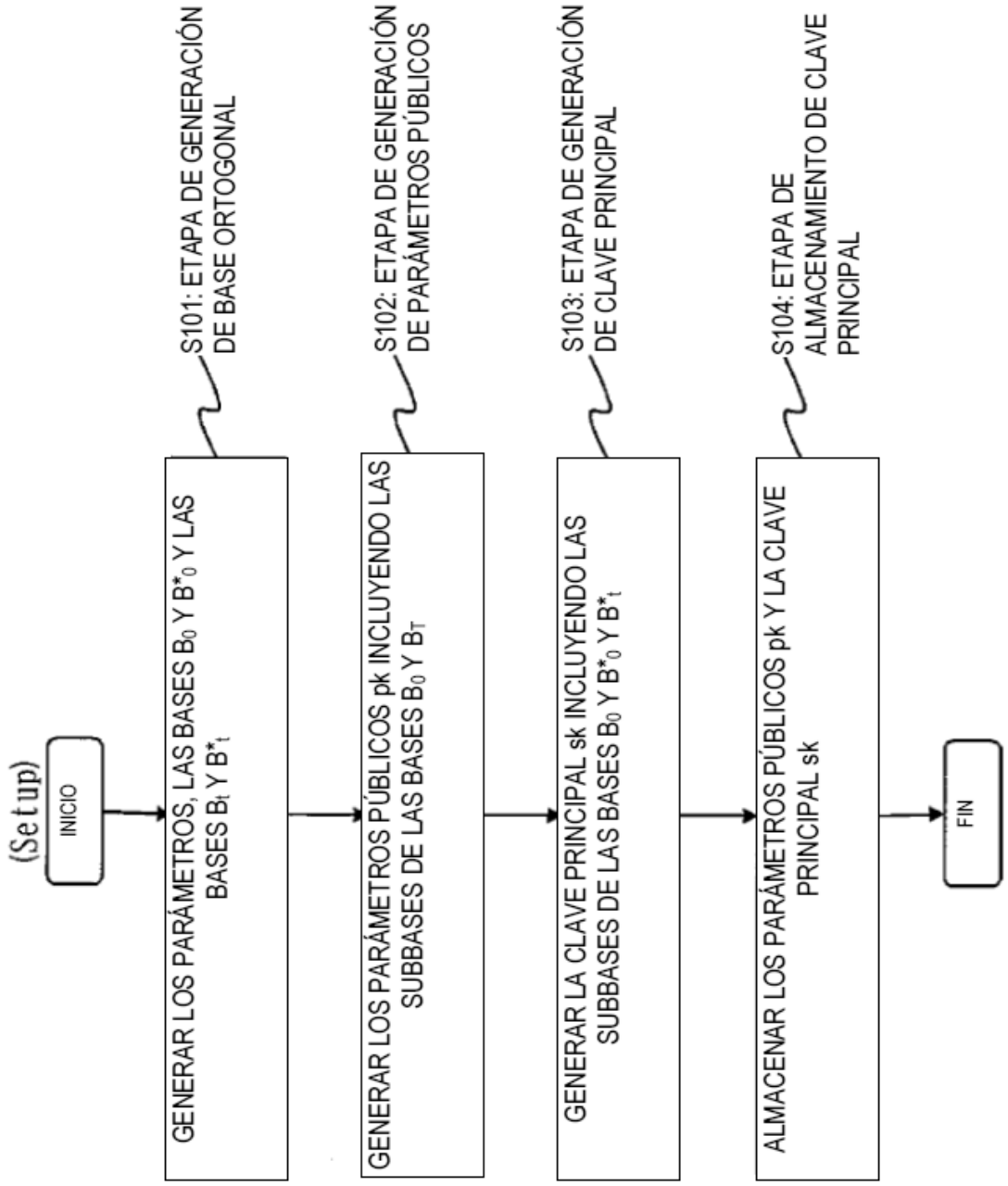

(Setup)
INICIO
GENERAR LOS PARÁMETROS, LAS BASES B_0 Y B^*_0 Y LAS BASES B_t Y B^*_t
S101: ETAPA DE GENERACIÓN DE BASE ORTOGONAL
GENERAR LOS PARÁMETROS PÚBLICOS pk INCLUYENDO LAS SUBBASES DE LAS BASES B_0 Y B_T
S102: ETAPA DE GENERACIÓN DE PARÁMETROS PÚBLICOS
GENERAR LA CLAVE PRINCIPAL sk INCLUYENDO LAS SUBBASES DE LAS BASES B_0 Y B^*_0 Y B^*_t
S103: ETAPA DE GENERACIÓN DE CLAVE PRINCIPAL
ALMACENAR LOS PARÁMETROS PÚBLICOS pk Y LA CLAVE PRINCIPAL sk
S104: ETAPA DE ALMACENAMIENTO DE CLAVE PRINCIPAL
FIN

Fig. 9

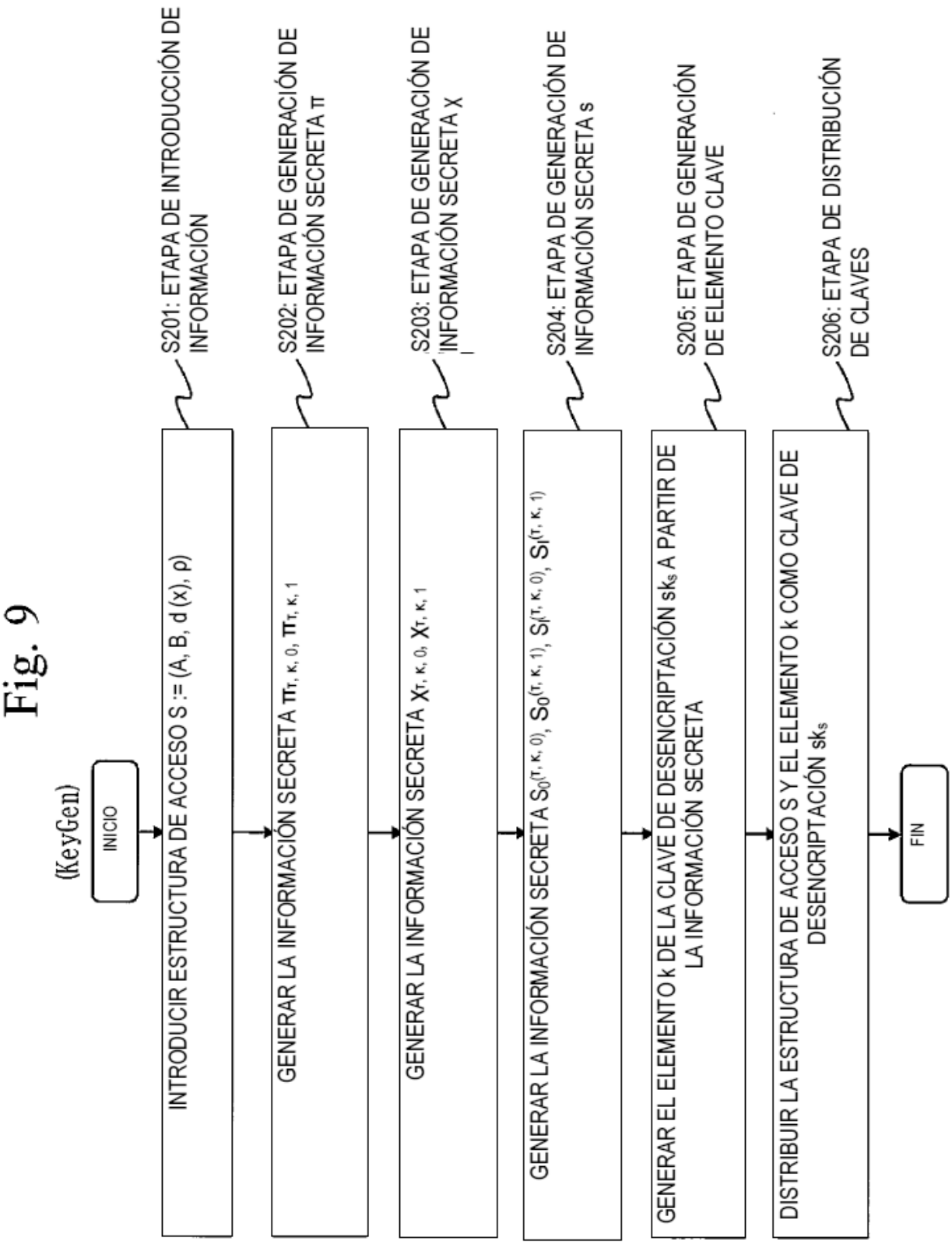

(KeyGen)
INICIO
INTRODUCIR ESTRUCTURA DE ACCESO S := (A, B, d (x), ρ)
S201: ETAPA DE INTRODUCCIÓN DE INFORMACIÓN
GENERAR LA INFORMACIÓN SECRETA $\pi_{\tau,\kappa,0}$, $\pi_{\tau,\kappa,1}$
S202: ETAPA DE GENERACIÓN DE INFORMACIÓN SECRETA π
GENERAR LA INFORMACIÓN SECRETA $X_{\tau,\kappa,0}$, $X_{\tau,\kappa,1}$
S203: ETAPA DE GENERACIÓN DE INFORMACIÓN SECRETA X
GENERAR LA INFORMACIÓN SECRETA $S_0^{(\tau,\kappa,0)}$, $S_0^{(\tau,\kappa,1)}$, $S_l^{(\tau,\kappa,0)}$, $S_l^{(\tau,\kappa,1)}$
S204: ETAPA DE GENERACIÓN DE INFORMACIÓN SECRETA s
GENERAR EL ELEMENTO k DE LA CLAVE DE DESENCRIPTACIÓN sk_s A PARTIR DE LA INFORMACIÓN SECRETA
S205: ETAPA DE GENERACIÓN DE ELEMENTO CLAVE
DISTRIBUIR LA ESTRUCTURA DE ACCESO S Y EL ELEMENTO k COMO CLAVE DE DESENCRIPTACIÓN sk_s
S206: ETAPA DE DISTRIBUCIÓN DE CLAVES
FIN

Fig. 10

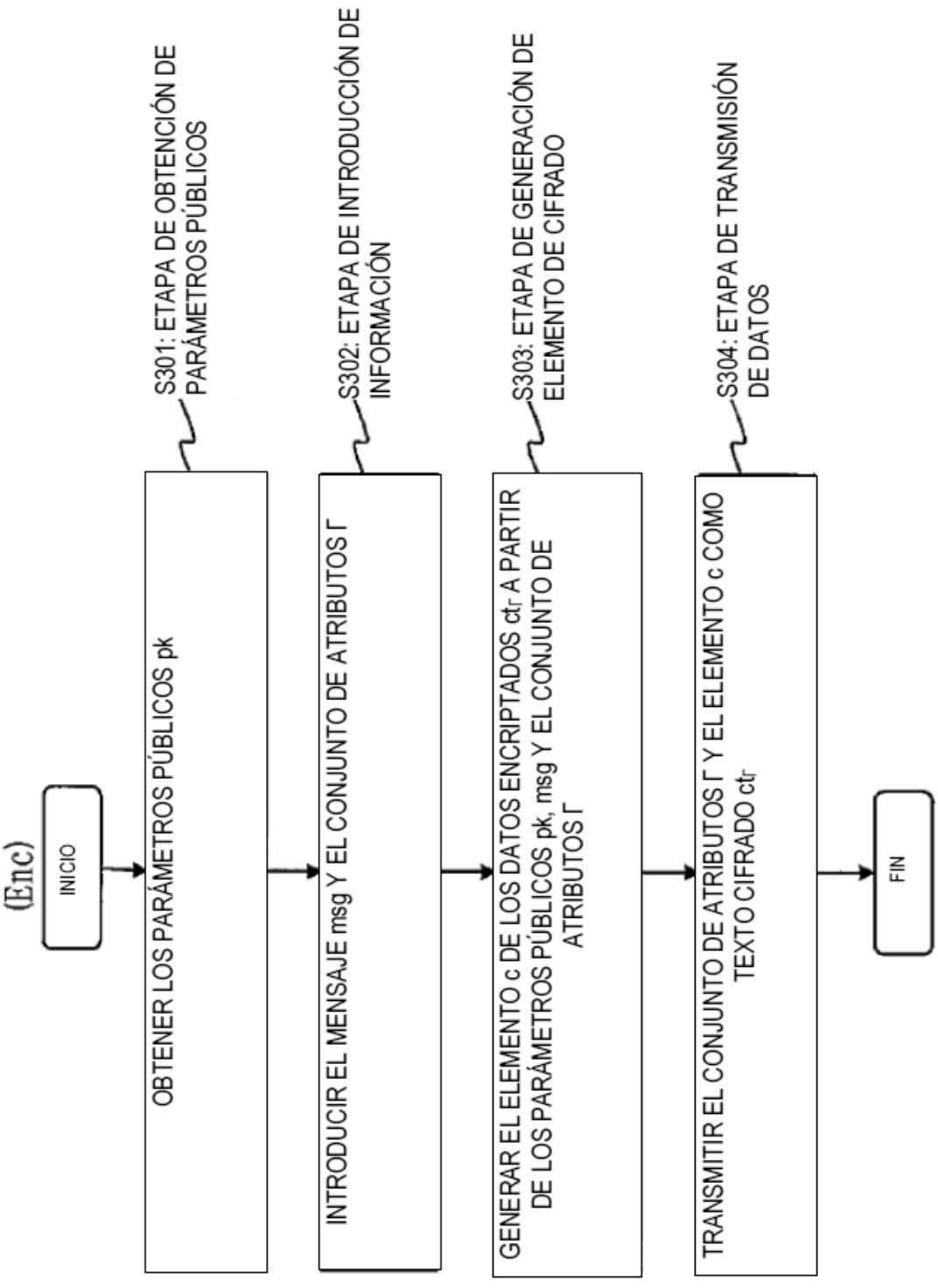

(Enc)
INICIO
OBTENER LOS PARÁMETROS PÚBLICOS pk
S301: ETAPA DE OBTENCIÓN DE PARÁMETROS PÚBLICOS
INTRODUCIR EL MENSAJE msg Y EL CONJUNTO DE ATRIBUTOS Γ
S302: ETAPA DE INTRODUCCIÓN DE INFORMACIÓN
GENERAR EL ELEMENTO c DE LOS DATOS ENCRIPTADOS ctΓ A PARTIR DE LOS PARÁMETROS PÚBLICOS pk, msg Y EL CONJUNTO DE ATRIBUTOS Γ
S303: ETAPA DE GENERACIÓN DE ELEMENTO DE CIFRADO
TRANSMITIR EL CONJUNTO DE ATRIBUTOS Γ Y EL ELEMENTO c COMO TEXTO CIFRADO ctΓ
S304: ETAPA DE TRANSMISIÓN DE DATOS
FIN

Fig. 11

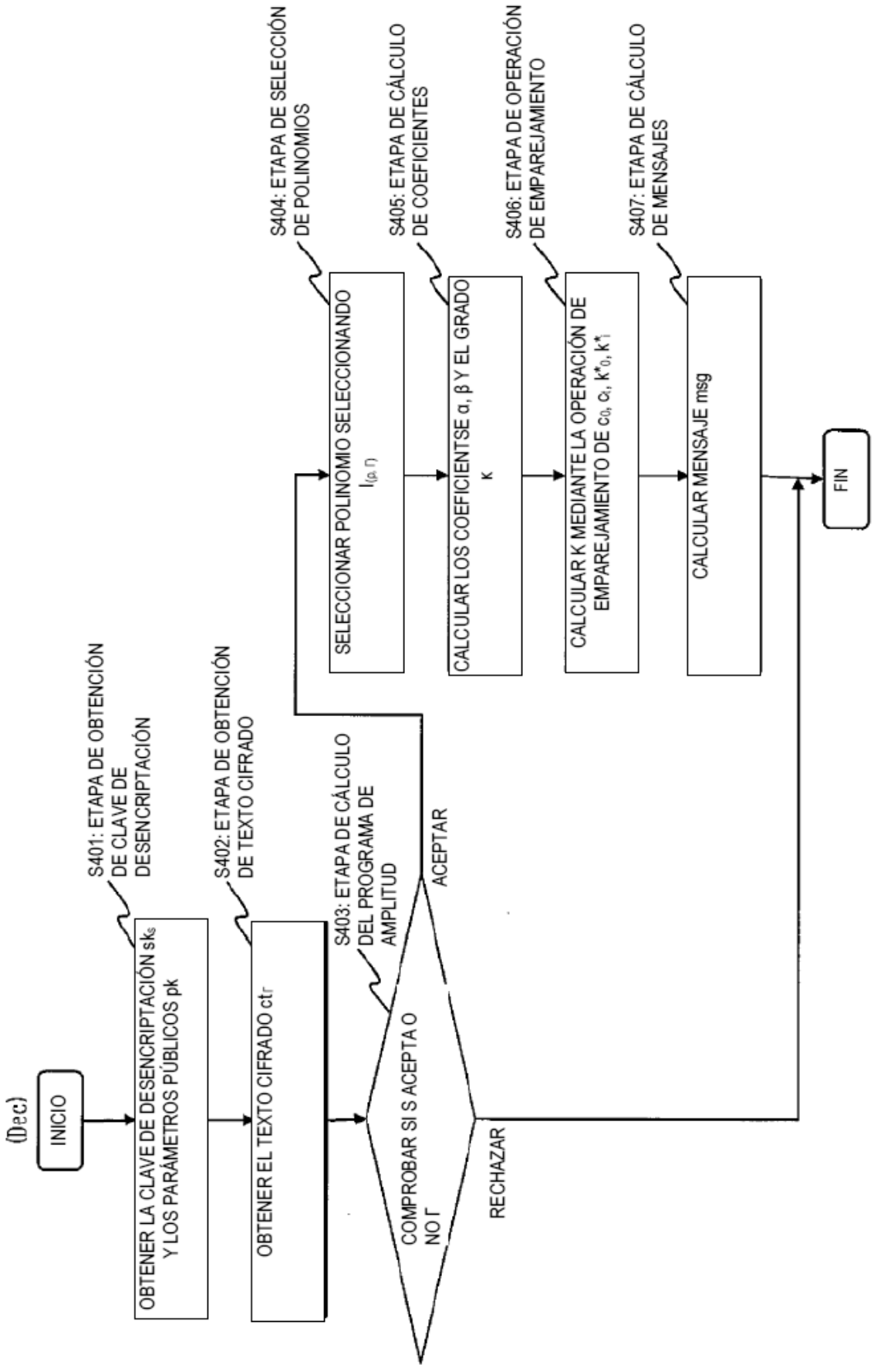

(Dec)
INICIO
S401: ETAPA DE OBTENCIÓN DE CLAVE DE DESENCRIPTACIÓN
OBTENER LA CLAVE DE DESENCRIPTACIÓN sk_S Y LOS PARÁMETROS PÚBLICOS pk
S402: ETAPA DE OBTENCIÓN DE TEXTO CIFRADO
OBTENER EL TEXTO CIFRADO ctr
S403: ETAPA DE CÁLCULO DEL PROGRAMA DE AMPLITUD
COMPROBAR SI S ACEPTA O NO Γ
ACEPTAR
RECHAZAR
S404: ETAPA DE SELECCIÓN DE POLINOMIOS
SELECCIONAR POLINOMIO SELECCIONANDO $I_{(\rho,\Gamma)}$
S405: ETAPA DE CÁLCULO DE COEFICIENTES
CALCULAR LOS COEFICIENTSE α, β Y EL GRADO κ
S406: ETAPA DE OPERACIÓN DE EMPAREJAMIENTO
CALCULAR K MEDIANTE LA OPERACIÓN DE EMPAREJAMIENTO DE c_0, α_i, k^*_0, k^*_1
S407: ETAPA DE CÁLCULO DE MENSAJES
CALCULAR MENSAJE msg
FIN

Fig. 12

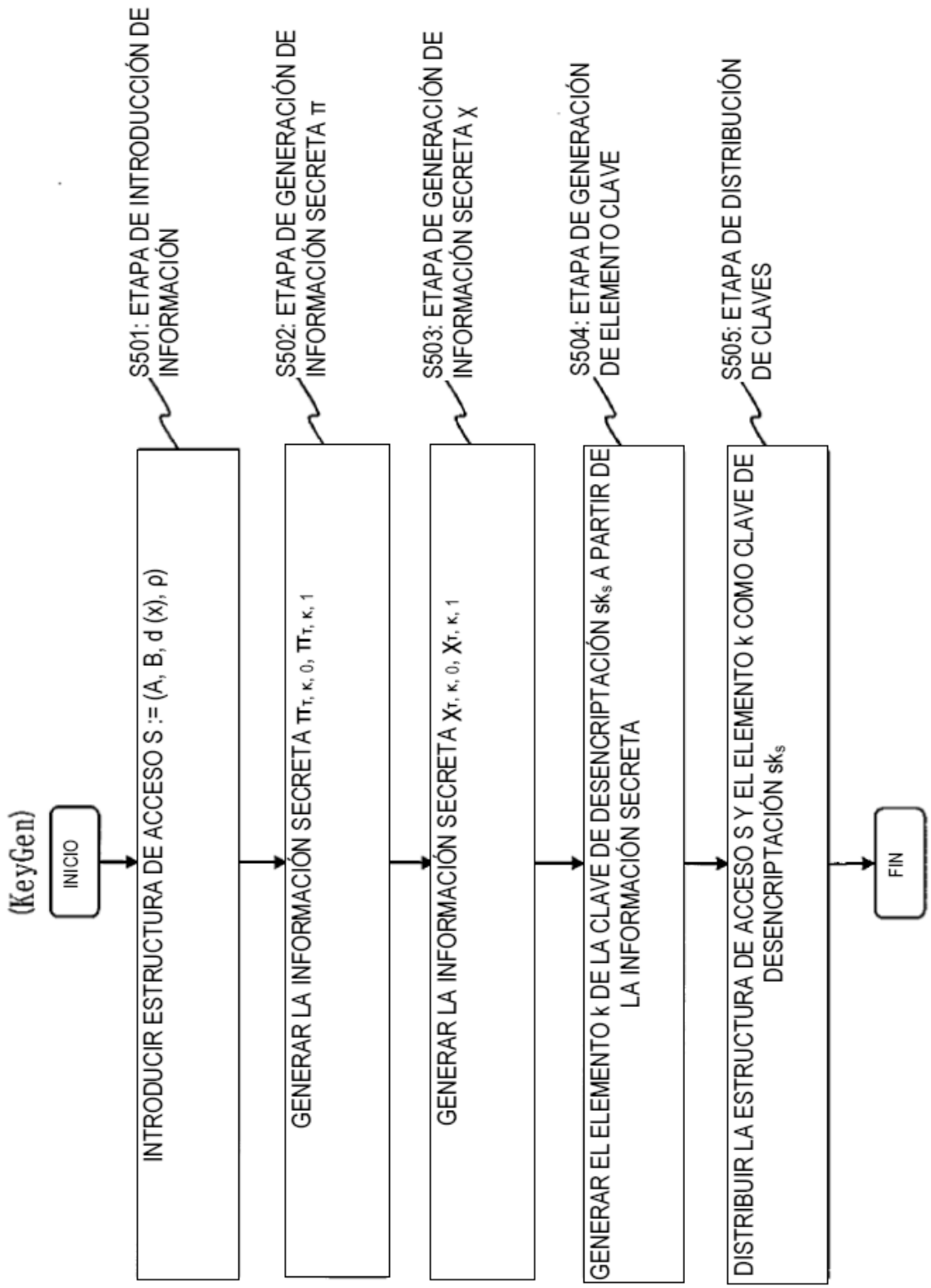
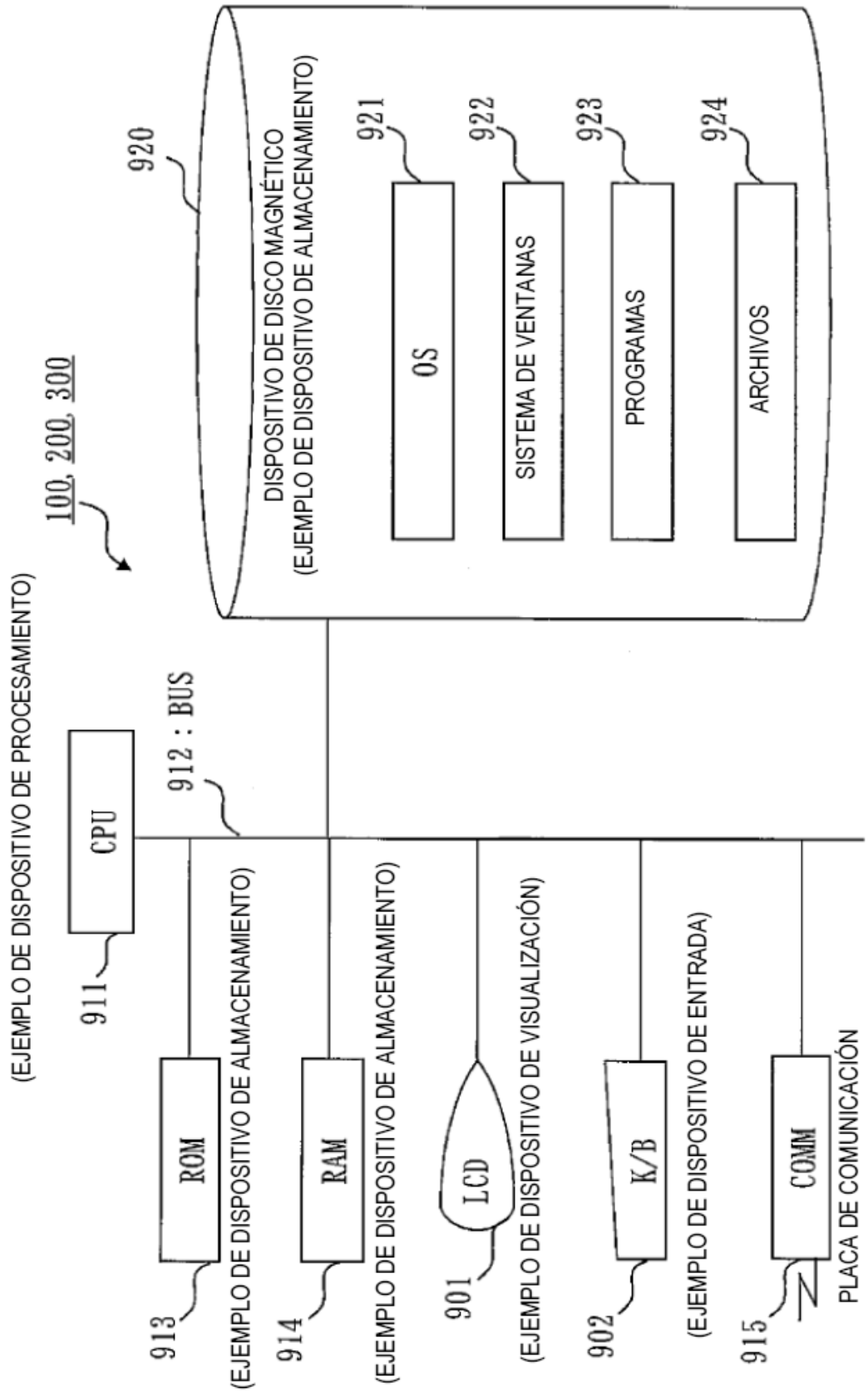

(KeyGen)
INICIO
INTRODUCIR ESTRUCTURA DE ACCESO S := (A, B, d (x), ρ)
S501: ETAPA DE INTRODUCCIÓN DE INFORMACIÓN
GENERAR LA INFORMACIÓN SECRETA $\pi_{\tau,\kappa,0}$, $\pi_{\tau,\kappa,1}$
S502: ETAPA DE GENERACIÓN DE INFORMACIÓN SECRETA π
GENERAR LA INFORMACIÓN SECRETA $\chi_{\tau,\kappa,0}$; $\chi_{\tau,\kappa,1}$
S503: ETAPA DE GENERACIÓN DE INFORMACIÓN SECRETA χ
GENERAR EL ELEMENTO k DE LA CLAVE DE DESENCRIPTACIÓN sk_s A PARTIR DE LA INFORMACIÓN SECRETA
S504: ETAPA DE GENERACIÓN DE ELEMENTO CLAVE
DISTRIBUIR LA ESTRUCTURA DE ACCESO S Y EL ELEMENTO k COMO CLAVE DE DESENCRIPTACIÓN sk_s
S505: ETAPA DE DISTRIBUCIÓN DE CLAVES
FIN

Fig. 13


100, 200, 300
920
DISPOSITIVO DE DISCO MAGNÉTICO
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
921
OS
922
SISTEMA DE VENTANAS
923
PROGRAMAS
924
ARCHIVOS
(EJEMPLO DE DISPOSITIVO DE PROCESAMIENTO)
911
CPU
912 : BUS
913
ROM
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
914
RAM
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
901
LCD
(EJEMPLO DE DISPOSITIVO DE VISUALIZACIÓN)
902
K/B
(EJEMPLO DE DISPOSITIVO DE ENTRADA)
915
COMM
PLACA DE COMUNICACIÓN