(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 684 945**

(51) Int. CI.:

H04L 9/32 (2006.01)
G09C 1/00 (2006.01)
H04L 9/08 (2006.01)
H04L 9/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.12.2011 PCT/JP2011/078463**

(87) Fecha y número de publicación internacional: **02.08.2012 WO12101913**

(96) Fecha de presentación y número de la solicitud europea: **08.12.2011 E 11856860 (9)**

(97) Fecha y número de publicación de la concesión europea: **11.07.2018 EP 2670081**

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

(30) Prioridad:

25.01.2011 JP 2011013281

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.10.2018

(73) Titular/es:

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

(72) Inventor/es:

TAKASHIMA, KATSUYUKI y
OKAMOTO, TATSUAKI

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema de procesamiento de firmas, dispositivo de generación de claves, dispositivo de firmas, dispositivo de verificación, método de procesamiento de firmas y programa de procesamiento de firmas

Campo técnico

La presente invención se refiere a un esquema de firmas basado en atributos (ABS). La invención se define en las reivindicaciones independientes.

Antecedentes de la técnica

Las Literaturas no de Patente 26, 29, 30, 34 a 37, 45 y 51 describen un esquema de firmas basado en atributos. Particularmente, las Literaturas no de Patente 36 y 37 describen un esquema de firmas basado en atributos que soporta un predicado monótono.

Lista de referencias

Literatura de Patente

Literatura no de Patente 1: Beimel, A., Secure schemes for secret sharing and key distribution. Tesis doctoral, Instituto de Tecnología de Israel, Technion, Haifa, Israel, 1996.

Literatura no de Patente 2: Belenkiy, M., Camenisch, J., Chase, M., Kohlweiss, M., Lysyanskaya, A. y Shacham, H.: Randomizable proofs and delegatable anonymous credentials. CRYPTO 2009. LNCS, Springer Heidelberg (2009)

Literatura no de Patente 3: Belenkiy, M., Chase, M., Kohlweiss, M. y Lysyanskaya, A.: P-signatures and noninteractive anonymous credentials. TCC 2008, LNCS, Springer Heidelberg (2008)

Literatura no de Patente 4: Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. En: Simposio sobre Seguridad y Privacidad del IEEE 2007, páginas 321-334. IEEE Press (2007)

Literatura no de Patente 5: Boneh, D., Boyen, X.: Efficient selective-ID secure identity based encryption without random oracles. En: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, páginas 223-238. Springer Heidelberg (2004)

Literatura no de Patente 6: Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. En: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, páginas 443-459. Springer Heidelberg (2004)

Literatura no de Patente 7: Boneh, D., Boyen, X., Goh, E.: Hierarchical identity based encryption with constant size ciphertext. En: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, páginas 440-456. Springer Heidelberg (2005)

Literatura no de Patente 8: Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. En: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, páginas 213-229. Springer Heidelberg (2001)

Literatura no de Patente 9: Boneh, D., Hamburg, M.: Generalized identity based and broadcast encryption scheme. En: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, páginas 455-470. Springer Heidelberg (2008)

Literatura no de Patente 10: Boneh, D., Katz, J., Improved efficiency for CCA-secure cryptosystems built using identity based encryption. RSA-CT 2005, LNCS, Springer Verlag (2005)

Literatura no de Patente 11: Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. En: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, páginas 535-554. Springer Heidelberg (2007)

Literatura no de Patente 12: X. Boyen: Mesh signatures. EUROCRYPT, LNCS, vol. 4515, páginas 210-227. Springer (2007)

Literatura no de Patente 13: Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). En: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, páginas 290-307. Springer Heidelberg (2006)

Literatura no de Patente 14: Camenisch, J. y Gross, T.: Efficient attributes for anonymous credentials. CCS 2008.

Literatura no de Patente 15: Camenisch, J. y Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optimal anonymity revocation. Eurocrypt 2001.

Literatura no de Patente 16: Camenisch, J. y Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. Crypto 2004.

Literatura no de Patente 17: Canetti, R., Halevi S., Katz J., Chosen-ciphertext security from identity-based encryption. EUROCRYPT 2004, LNCS, Springer-Verlag (2004)

Literatura no de Patente 18: Chaum, D.: Security without identification: Transaction systems to make big brother obsolete. CACM (1985).

Literatura no de Patente 19: D. Chaum y E. van Heyst: Group signatures. En las actas de EUROCRYPT'91, LNCS, vol. 547, páginas 257-265 (1991).

Literatura no de Patente 20: Cocks, C.: An identity based encryption scheme based on quadratic residues. En: Honary, B. (ed.) Conf. Int. IMA. LNCS, vol. 2260, páginas 360-363. Springer Heidelberg (2001)

Literatura no de Patente 21: Gentry, C.: Practical identity-based encryption without random oracles. En: Vaudenay, S. (ed.) EURO-CRYPT 2006. LNCS, vol. 4004, páginas 445-464. Springer Heidelberg (2006)

Literatura no de Patente 22: Gentry, C., Halevi, S.: Hierarchical identity-based encryption with polynomially many levels. En: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, páginas 437-456. Springer Heidelberg (2009)

Literatura no de Patente 23: Gentry, C., Silverberg, A: Hierarchical ID-based cryptography. En: Zheng, Y. (ed.) ASIACRYPT 2002.LNCS, vol. 2501, páginas 548-566. Springer Heidelberg (2002)

Literatura no de Patente 24: Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. En: Conferencia ACM sobre Seguridad Informática y de Comunicaciones 2006, páginas 89-98, ACM (2006).

Literatura no de Patente 25: Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. En: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, páginas 415-432. Springer Heidelberg (2008)

Literatura no de Patente 26: S. Guo e Y. Zeng: Attribute-based Signature Scheme, En ISA'08, páginas 509-511 (2008).

Literatura no de Patente 27: Horwitz, J., Lynn, B.: Towards hierarchical identity-based encryption. En: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, páginas 466-481. Springer Heidelberg (2002)

Literatura no de Patente 28: Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. En: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, páginas 146-162. Springer Heidelberg (2008)

Literatura no de Patente 29: D. Khader: Attribute Based Group Signatures, Cryptology ePrint Archive, Informe 2007/159 (2007). http://eprint.iacr.org/2007/159.

Literatura no de Patente 30: D. Khader: Attribute Based Group Signature with Revocation. Cryptology ePrint Archive, Informe 2007/241, (2007). http://eprint.iacr.org/2007/241.

Literatura no de Patente 31: Lewko, A., Okamoto, T., Sahai, A., Takashima, K. y Waters, B.: Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption, EUROCRYPT 2010. LNCS, Springer Heidelberg (2010).

Literatura no de Patente 32: Lewko, A.B., Waters, B.: Fully secure HIBE with short ciphertexts. ePrint, IACR, http://eprint.iacr.org/2009/482

Literatura no de Patente 33: Lewko, A.B., Waters, B.: Decentralizing Attribute-Based Encryption, ePrint, IACR, http://eprint.iacr.org/2010/351.

Literatura no de Patente 34: Jin Li, Man Ho Au, Willy Susilo, Dongqing Xie, Kui Ren: Attribute-based Signature and its Application, ASIACCS' 2010, ACM (2010).

Literatura no de Patente 35: J. Li y K. Kim: Attribute-based ring signatures. 2008. Disponible en http://eprint.iacr.org/2008/394. Para aparecer en el Diario de Ciencias de la Información.

Literatura no de Patente 36: Maji, H., Prabhakaran, M., Rosulek, M.: Attribute-based Signatures: Achieving Attribute-Privacy and Collusion-Resistance. ePrint, IACR, http://eprint.iacr.org/2008/328

Literatura no de Patente 37: Maji, H., Prabhakaran, M., Rosulek, M.: Attribute-Based Signatures. http://www.cs.uiuc.edu/mmp/research.html

Literatura no de Patente 38: Okamoto, T., Takashima, K.: Homomorphic encryption and signatures from vector decomposition. En: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, páginas 57-74. Springer Heidelberg (2008)

Literatura no de Patente 39: Okamoto, T., Takashima, K.: Hierarchical predicate encryption for Inner-Products, En: ASIACRYPT 2009, Springer Heidelberg (2009)

Literatura no de Patente 40: Okamoto, T., Takashima, K.: Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption, en: CRYPTO 2010, Springer Heidelberg (2010).

Literatura no de Patente 41: Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. En: Conferencia ACM sobre Seguridad Informática y de Comunicaciones 2007, paginas 195-203, ACM (2007)

Literatura no de Patente 42: Pirretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure attribute-based systems. En: Conferencia ACM sobre Seguridad Informática y de Comunicaciones 2006, páginas 99-112, ACM, (2006)

Literatura no de Patente 43: Pirretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure attribute-based systems. En: Conferencia ACM sobre Seguridad Informática y de Comunicaciones 2006, páginas 99-112, ACM, (2006).

Literatura no de Patente 44: Sahai, A., Waters, B.: Fuzzy identity-based encryption. En: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, páginas 457-473. Springer Heidelberg (2005)

Literatura no de Patente 45: S. F. Shahandashti y R. Safavi-Naini: Threshold attribute-based signatures and their application to anonymous credential systems. En AFRICACRYPT'09, páginas 198-216 (2009).

Literatura no de Patente 46: A Shamir: Identity-based cryptosystems and signature schemes. En CRYPTO'84, páginas 47-53 (1984).

Literatura no de Patente 47: Shi, E., Waters, B.: Delegating capability in predicate encryption systems. En: Aceto, L., Damºgard, I., Goldberg, LA., Halldorsson, M.M., Ingolfsdottir, A., Walukiewicz, I. (eds.) ICALP (2) 2008. LNCS, vol. 5126, páginas 560-578. Springer Heidelberg (2008)

Literatura no de Patente 48: Shi, E., Waters, B.: Delegating capability in predicate encryption systems. En: Aceto, L., Damºgard, I., Goldberg, L.A., Halldorsson, M.M., Ingolfsdottir, A., Walukiewicz, I. (eds.) ICALP (2) 2008. LNCS, vol. 5126, páginas 560-578. Springer Heidelberg (2008).

Literatura no de Patente 49: Waters, B.: Ciphertext-policy attribute-based encryption an expressive, efficient, and probably secure realization. ePrint, IACR, http://eprint.iacr.org/2008/290

Literatura no de Patente 50: Waters, B.: Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. En: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, páginas 619-636. Springer Heidelberg (2009)

Literatura no de Patente 51: Waters, B.: Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. En: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, páginas. 619-636. Springer Heidelberg (2009)

Compendio de la invención

Problema técnico

El esquema de firmas basado en atributos convencional no soporta predicados no monótonos.

Es un objeto de la presente invención proporcionar un esquema de firmas basado en atributos que soporte predicados no monótonos.

Solución al problema

Un sistema de procesamiento de firmas según la presente invención es un sistema de procesamiento de firmas que incluye un dispositivo de generación de claves, un dispositivo de firmas y un dispositivo de verificación, y sirve para ejecutar un proceso de firma que usa una base B_t y una base B^*_t para cada número entero t = 0, ..., d+1 (d es un número entero de 1 o más),

en donde el dispositivo de generación de claves incluye

una primera parte de entrada de información que toma como entrada un conjunto de atributos Γ que incluye información de identificación t e información de atributo $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t donde n_t es un número entero de 1 o más) para al menos un número entero t = 1, ..., d,

una parte de generación del elemento de clave 0 que genera un elemento de clave k^*_0 donde un valor δ predeterminado se establece como coeficiente para un vector base $b^*_{0,1}$ de una base B^*_0,

una parte de generación del elemento de clave t que genera un elemento de clave k^*_t donde $\delta x_{t,i}$ (i = 1, ..., n_t) obtenido multiplicando la información de atributo $\vec{x}_t$ por el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{t,i}$ (i = 1, ..., n_t) de la base B^*_t, que concierne a cada información de identificación t incluida en el conjunto de atributos Γ introducido por la primera parte de entrada de información,

una parte de generación del elemento de clave d+1 que genera un elemento de clave $k^*_{d+1,1}$ donde el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{d+1,1}$ de una base B^*_{d+1}, y un elemento de clave $k^*_{d+1,2}$ donde el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{d+1,2}$ de la base B^*_{d+1}, y

una parte de transmisión de clave de firma que transmite, al dispositivo de firmas, una clave de firma sk_Γ que incluye: el elemento de clave k^*_0 generado por la parte de generación del elemento de clave 0; el elemento de clave k^*_t generado por la parte de generación del elemento de clave t que concierne a cada información de identificación t incluida en el conjunto de atributos Γ; el elemento de clave $k^*_{d+1,1}$ y el elemento de clave $k^*_{d+1,2}$ que se generan por la parte de generación de elemento de clave d+1; y el conjunto de atributos Γ,

en donde el dispositivo de firmas incluye

una segunda parte de entrada de información que toma como entrada una variable ρ(i) para cada número entero i = 1, ..., L (L es un número entero de 1 o más), cuya variable ρ(i) es cualquiera de una tupla positiva $(t, \vec{v}_i)$ y una tupla negativa $\neg(t, \vec{v}_i)$ de la información de identificación t (t es cualquier número entero de t = 1, ..., d) y la información de atributo $\vec{v}_i := (v_{i,i'})$ (i' = 1, ..., n_t); una matriz M predeterminada que tiene L filas y r columnas (r es un número entero de 1 o más); y un mensaje m,

una parte de adquisición de clave de firma que adquiere la clave de firma sk_Γ transmitida por la parte de transmisión de clave de firma,

una parte de cálculo de coeficientes complementarios que, en base a la variable ρ(i) introducida por la segunda parte de entrada de información y el conjunto de atributos Γ incluido en la clave de firma sk_Γ adquirida por la parte de adquisición de clave de firma, especifica, entre los números enteros i = 1, ..., L, un conjunto I de un número entero i para el cual la variable ρ(i) es una tupla positiva $(t, \vec{v}_i)$ y con el cual un producto interno de $\vec{v}_i$ de la tupla positiva y $\vec{x}_t$ incluido en el conjunto de atributos Γ indicado por la información de identificación t de la tupla positiva llega a ser 0, y un número entero i para el cual la variable ρ(i) es una tupla negativa $\neg(t, \vec{v}_i)$ y con el cual un producto interno de $\vec{v}_i$ de la tupla negativa y $\vec{x}_t$ incluido en el conjunto de atributos Γ indicado por la información de identificación t de la tupla negativa no llega a ser 0; y calcula, concerniente a i incluido en el conjunto I especificado, un coeficiente complementario α_i con el cual un total de $\alpha_i M_i$ en base a M_i que es un elemento en una fila de orden i de la matriz M introducida por la segunda parte de entrada de información llega a ser un vector predeterminado $\vec{h}$,

una parte de generación del elemento de firma 0 que genera un elemento de firma s^*_0 que incluye el elemento de clave k^*_0 incluido en la clave de firma sk_Γ,

una parte de generación del elemento de firma i que genera, para cada número entero i = 1 ..., L, un elemento de firma s^*_i que incluye $\gamma_i k^*_t$ obtenido multiplicando el elemento de clave k^*_t incluido en la clave de firma sk_Γ por un valor γ_i, estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i$ cuando el número entero i se incluye en el conjunto I especificado por la parte de cálculo de coeficientes complementarios y la variable ρ(i) es una tupla positiva $(t, \vec{v}_i)$; estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i/(\vec{v}_i \cdot \vec{x}_t)$ cuando el número entero i está incluido en el conjunto I y la variable ρ(i) es una tupla negativa $\neg(t, \vec{v}_i)$; y estableciendo el valor γ_i para satisfacer $\gamma_i := 0$ cuando el número entero i no está incluido en el conjunto I,

una parte de generación del elemento de firma L+1 que genera un elemento de firma s^*_{L+1} que incluye una suma del elemento de clave $k^*_{d+1,1}$ incluido en la clave de firma sk_Γ y $m' \cdot k^*_{d+1,2}$ obtenido multiplicando el elemento de clave $k^*_{d+1,2}$ por un valor m' generado usando el mensaje m, y

una parte de transmisión de datos de firma que transmite, al dispositivo de verificación, datos de firma σ que incluyen: el elemento de firma s^*_0 generado por la parte de generación del elemento de firma 0; el elemento de firma s^*_i generado para cada número entero i = 1, ..., L por la parte de generación del elemento de firma i; el elemento de firma s^*_{L+1} generado por la parte de generación del elemento de firma L+1; el mensaje m; la variable ρ(i); y la matriz M, y

en donde el dispositivo de verificación incluye

una parte de adquisición de datos que adquiere los datos de firma σ transmitidos por la parte de transmisión de datos de firma,

una parte de generación del elemento de verificación 0 que genera un elemento de verificación c_0 estableciendo, como coeficiente para un vector base $b_{0,1}$ de una base B_0, $-s_0 - s_{L+1}$ calculado a partir de un valor $s_0 := \vec{h} \cdot \vec{f}$ y un valor predeterminado s_{L+1}, el valor $s_0 := \vec{h} \cdot \vec{f}$ que se genera usando un vector $\vec{f}$ que tiene r partes de elementos, y el vector $\vec{h}$,

una parte de generación del elemento de verificación i que, para cada número entero i = 1, ..., L y usando un vector de columna $\vec{s}^T := (s_1, ..., s_L)^T := M \cdot \vec{f}^T$ generado en base al vector $\vec{f}$ y la matriz M que se incluye en los datos de firma σ adquiridos por la parte de adquisición de datos, y un número predeterminado θ_i para cada

número entero i = 1, ..., L, genera un elemento de verificación c_i, cuando la variable ρ(i) es una tupla positiva (t, $\vec{v}_i$), estableciendo $s_i+\theta_i v_{i,1}$ como coeficiente para un vector base $b_{t,1}$ de la base B_t indicado por la información de identificación t de la tupla positiva y estableciendo $\theta_i v_{i,i'}$ (i' = 2, ..., n_t) como coeficiente para un vector base $b_{t,i'}$ (i' = 2, ..., n_t), y genera un elemento de verificación c_i, cuando la variable ρ(i) es una tupla negativa ¬(t, $\vec{v}_i$) estableciendo $s_i v_{i,i'}$ (i' = 1, ..., n_t) como coeficiente para el vector base $b_{t,i'}$ (i' = 1, ..., n_t) indicado por la información de identificación t de la tupla negativa,

una parte de generación del elemento de verificación L+1 que genera un elemento de verificación c_{L+1} estableciendo $s_{L+1}-\theta_{L+1}m'$ calculado a partir del valor predeterminado s_{L+1}, el valor m', y un valor predeterminado θ_{L+1} como coeficiente para un vector base $b_{d+1,1}$ de una base B_{d+1}, y estableciendo el valor predeterminado θ_{L+1} como coeficiente para un vector base $b_{d+1,2}$, y

una parte de operación de emparejamiento que verifica la autenticidad de los datos de firma σ dirigiendo una operación de emparejamiento $\Pi_{i=0}^{L+1} e(c_i, s^*_i)$ para el elemento de verificación c_0 generado por la parte de generación del elemento de verificación 0, el elemento de verificación c_i generado por la parte de generación del elemento de verificación i, el elemento de verificación c_{L+1} generado por la parte de generación del elemento de verificación L+1, y los elementos de firma s^*_0, s^*_i, y s^*_{L+1} incluidos en los datos de firma σ.

Efectos ventajosos de la invención

Un esquema de firmas basado en atributos según la presente invención soporta predicados no monótonos, y en consecuencia realiza un esquema de firmas basado en atributos que tiene aplicaciones diversificadas.

Breve descripción de los dibujos

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

La Fig. 2 es un dibujo explicativo de una matriz M_δ.

La Fig. 3 es un dibujo explicativo de s_0.

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

La Fig.5 es un diagrama de configuración de un sistema de procesamiento de firmas 10 que ejecuta un esquema de firmas basado en atributos.

La Fig.6 es un diagrama de bloques de funciones que muestra una función de un dispositivo de generación de claves 100.

La Fig.7 es un diagrama de bloques de funciones que muestra una función de un dispositivo de firmas 200.

La Fig. 8 es un diagrama de bloques de funciones que muestra una función de un dispositivo de verificación 300.

La Fig. 9 es un diagrama de flujo que muestra el proceso del algoritmo Setup.

La Fig.10 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen.

La Fig.11 es un diagrama de flujo que muestra el proceso del algoritmo Sig.

La Fig. 12 es un diagrama de flujo que muestra el proceso del algoritmo Ver.

La Fig. 13 es un dibujo explicativo de multiautoridad.

La Fig. 14 es un diagrama de configuración de un sistema de procesamiento de firmas 10 que ejecuta un esquema de firmas basado en atributos multiautoridad descentralizado.

La Fig. 15 es un diagrama de bloques de funciones que muestra una función de cada dispositivo de generación de claves 100.

La Fig. 16 es un diagrama de bloques de funciones que muestra una función de un dispositivo de firmas 200.

La Fig. 17 es un diagrama de bloques de funciones que muestra la función de un dispositivo de verificación 300.

La Fig. 18 es un diagrama de flujo que muestra el proceso del algoritmo GSetup.

La Fig. 19 es un diagrama de flujo que muestra el proceso del algoritmo ASetup.

La Fig. 20 es un diagrama de flujo que muestra el proceso del algoritmo AttrGen.

La Fig. 21 es un diagrama de flujo que muestra el proceso del algoritmo Sig.

La Fig. 22 es un diagrama de flujo que muestra el proceso del algoritmo Ver.

La Fig. 23 es un diagrama que muestra un ejemplo de la configuración de hardware del dispositivo de generación de claves 100, el dispositivo de firmas 200 y el dispositivo de verificación 300.

Descripción de realizaciones

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

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

Se explicará la notación en la siguiente descripción.

Cuando A es una variable o distribución aleatoria, la Fórmula 101 indica que y se selecciona aleatoriamente a partir de A según la distribución de A. Esto es, 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. Esto es, 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 que una máquina (algoritmo) A emite a en la entrada x.

[Fórmula 104]

$$A(x) \rightarrow a$$

Por ejemplo,

$$A(x) \rightarrow 1$$

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

[Fórmula 105]

$$\mathbb{F}_q$$

Un símbolo vectorial indica una representación vectorial sobre el campo finito F_q. Esto es, 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 en la Fórmula 109, de dos vectores $\vec{x}$ e $\vec{y}$ 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]

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

Obsérvese que X^T indica la transpuesta de la matriz M.

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

[Fórmula 110]

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

[Fórmula 111]

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

[Fórmula 112]

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

Obsérvese que para las bases B y B* indicadas en la Fórmula 113, se establece la Fórmula 114.

[Fórmula 113]

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

[Fórmula 114]

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

En la siguiente descripción, en $param_{v0}$, V0 representa V_0.

Del mismo modo, nt en F_q^{nt} representa n_t.

Del mismo modo, xt en $sk_{gid,(t,\ xt)}$ representa x_t.

Del mismo modo, cuando "$\delta_{i,j}$" se indica como un superíndice, δi,j es $\delta_{i,j}$.

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

En la siguiente descripción, un proceso de firma incluye un proceso de generación de claves, un proceso de firma y un proceso de verificación.

Realización 1.

Esta realización describe un "esquema de firmas basado en atributos".

En primer lugar, se explicará brevemente una firma basada en atributos.

En segundo lugar, se describirá un espacio que tiene una estructura matemática rica llamada "espacios vectoriales de emparejamiento dual (DPVS)" que es un espacio para implementar el esquema de firmas basado en atributos.

En tercer lugar, se describirá un concepto para implementar el esquema de firmas basado en atributos. Aquí, se describirán un "programa de extensión", "el producto interno de vectores de atributos, una estructura de acceso", y un "esquema de distribución de secreto (esquema de compartición de secreto)". También se describirán funciones de comprobación aleatoria resistentes a colisión.

En cuarto lugar, se describirá un "esquema de firmas basado en atributos" según esta realización. Inicialmente, se describirá la estructura básica del "esquema de firmas basado en atributos". Posteriormente, se describirá la estructura básica de un "sistema de procesamiento de firmas 10" que implementa el "esquema de firmas basado en atributos". Luego, se describirán en detalle el "esquema de firmas basado en atributos" y el "sistema de procesamiento de firmas 10" según esta realización.

<1. Firma basada en atributos>

El concepto de firma digital se introdujo en el documento de seminario por Diffie y Hellman en 1976. En este concepto, se genera un par que comprende una clave de firma secreta sk y una clave de verificación pública pk para el firmante, y la firma σ del mensaje m generado usando la clave de firma sk se verifica mediante la clave de verificación pk correspondiente. Por lo tanto, se identifica al firmante del mensaje (m, σ) firmado usando la clave de firma sk a través de la clave de verificación pk.

Aunque este es uno de los requisitos de las firmas digitales, no existe flexibilidad ni privacidad en la relación entre los firmantes y las demandas atestiguadas por las firmas debido a la estrecha relación entre la clave de firma sk y la clave de verificación pk.

Se han estudiado variantes versátiles y de privacidad mejorada de firmas digitales, donde la relación entre una clave de firma y una clave de verificación es más flexible o sofisticada.

En esta clase de firmas, la clave de firma y la clave de verificación se parametrizan mediante el atributo x y el predicado v, respectivamente, y el mensaje (m, σ) firmado generado mediante la clave de firma con el parámetro x, sk_x, se verifica correctamente mediante la clave pública pk y el parámetro v, si y sólo si el predicado v acepta el atributo x (cuando se contiene v(x)).

La privacidad de los firmantes en esta clase de firmas requiere que una firma para el predicado v, generado por la clave de firma sk_x no libere información con respecto al atributo x excepto que contenga v(x).

Cuando el predicado v es la igualdad con el parámetro v (es decir, se contiene v(x) si y sólo si x = v), la clase de firmas para este predicado es firmas basadas en ID (Firmas Basadas en Identidad, IBS) (véase la Literatura no de Patente 46).

Aquí obsérvese que no hay espacio para la privacidad en las firmas basadas en ID, dado que el predicado v identifica de manera única el atributo x de la clave secreta sk_x del firmante, de manera que x = v.

Las firmas de grupo también están en esta clase de firmas (véase la Literatura no de Patente 19). Las firmas de grupo son firmas con predicado v, donde se contiene v(x) si y sólo si el parámetro de predicado v es la identidad del grupo y el atributo x es una identidad de miembro del grupo v (o pk, es una clave pública que identifica el grupo v y sk_x es una clave secreta del miembro x del grupo v).

Debido al requisito de privacidad, las firmas generadas usando la clave secreta sk_x no liberan información con respecto a la identidad del miembro x, excepto que x sea miembro del grupo v.

Esta clase de firmas incluye una firma basada en atributos con un predicado más sofisticado (véanse las Literaturas no de Patente 26, 29, 30, 34 a 46, 45 y 51), donde x para la clave de firma sk_x es una tupla de atributos (x_1, ..., x_i) y v para la verificación es un predicado de estructura de acceso o umbral.

La clase más amplia de predicados en el esquema de firmas basado en atributos existente son las estructuras de acceso monótono (véanse las Literaturas no de Patente 36 y 37), donde el predicado v se especifica por un programa de extensión monótono (M, ρ) (MSP(M, ρ)) junto con una tupla de atributos (v_1, ..., v_j) y v(x) se cumple si y sólo si MSP (M, ρ) acepta el vector de valor verdadero de ($T(x_{i\_1} = v_1)$, …, $T(x_{i\_j} = v_j)$). Aquí, T(ψ) := 1 si ψ es verdadero, y T(ψ) := 1 si ψ es falso. Por ejemplo, T (x = v) := 1 si x = v, y T (x = v) := 0 si x ≠ v.

Tal predicado monótono puede expresar puertas AND, OR y Umbral.

Se explicará un ejemplo de tal predicado monótono v para una firma basada en atributos.

Un ejemplo de tal predicado monótono v es (Instituto = Univ. A) AND (TH2 ((Departamento = Biología), (Sexo = Femenino), (Edad = Cincuentas)) OR (Posición = Profesor)), donde TH2 significa la puerta de umbral con el valor umbral 2 (esto es, una puerta que requiere que se contengan dos o más condiciones).

El atributo x_A de Alicia es (Instituto = Univ. A), (Departamento = Biología), (Posición = Postdoctorado), (Edad = 30), (Sexo = Femenino), y el atributo x_B de Bob es (Instituto = Univ. A), (Departamento = Matemáticas), (Posición = Profesor), (Edad = 45), (Sexo = Masculino). Aunque sus atributos, x_A y x_B, son bastante diferentes, está claro que contienen $v(x_A)$ y $v(x_B)$, y que hay muchos otros atributos que satisfacen v.

Por lo tanto, Alice y Bob pueden generar una firma en este predicado, y debido al requisito de privacidad de la firma basada en atributos, una firma para v no libera información con respecto el atributo del firmante, es decir, Alice o Bob (u otro), excepto que el atributo del firmante satisfaga el predicado v.

Hay muchas aplicaciones de la firma basada en atributos tales como mensajería basada en atributos (ABM), autenticación basada en atributos, negociación de confianza y secretos de fugas (véanse las Literaturas no de Patente 36 y 37).

No obstante, no hay ningún esquema de firmas basado en atributos, incluso uno con una seguridad baja, para un predicado no monótono. Un predicado no monótono puede expresar una puerta NOT, como con puertas AND, OR y de Umbral.

Más específicamente, con un predicado monótono, aunque se puede establecer una condición positiva, tal como (Instituto = Univ. A), no se puede establecer una condición negativa, tal como (Instituto ≠ Univ. A) (es decir, No(Instituto = Univ. A)). En contraste con esto, con un predicado no monótono, se puede establecer una condición negativa.

Si hay muchas universidades además de Univ. A, es difícil establecer una condición negativa de otra que no sea Univ. A usando solamente una condición positiva (la descripción llega a ser complicada). Esto indica la utilidad de los predicados no monótonos.

<2. Espacios vectoriales de emparejamiento dual>

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

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

En la siguiente descripción, permitamos que la Fórmula 115 sea un algoritmo que tome como entrada 1^λ y emita los valores de un parámetro $param_G := (q, G, G_T, g, e)$ de grupos de emparejamiento bilineales con un parámetro de seguridad λ.

[Fórmula 115]

$\mathcal{G}_{bpg}$

Se describirán ahora espacios vectoriales de emparejamiento dual.

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

[Fórmula 116]

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

[Fórmula 117]

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

Operación (1): Emparejamiento bilineal no degenerado

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

[Fórmula 118]

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

donde

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

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

Operación (2): Mapas de distorsión

La transformación lineal $\Phi_{i,j}$ en el espacio V indicada en la Fórmula 119 puede lograr la Fórmula 120.

[Fórmula 119]

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

[Fórmula 120]

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

Obsérvese que

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

La transformación lineal $\Phi_{i,j}$ se denominará mapas de distorsión.

En la siguiente descripción, permitamos que la Fórmula 121 sea un algoritmo que tome como entrada, 1^λ ($\lambda \in$ número natural), $N \in$ número natural, y los valores del parámetro $param_G := (q, G, G_T, g, e)$ de grupos de emparejamiento bilineales, y emite los valores de un parámetro $param_V := (q, V, G_T, A, e)$ de espacios vectoriales de emparejamiento dual que tienen un parámetro de seguridad λ, y que forman espacio N-dimensional V.

[Fórmula 121]

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

Se describirá un caso donde se construyen espacios vectoriales de emparejamiento dual a partir de los grupos de emparejamiento bilineal simétricos descritos anteriormente. Los espacios vectoriales de emparejamiento dual se pueden construir también a partir de grupos de emparejamiento bilineal asimétricos. La siguiente descripción se

puede aplicar fácilmente a un caso donde se construyen espacios vectoriales de emparejamiento dual a partir de grupos de emparejamiento bilineal asimétricos.

<3. Concepto para implementar un esquema de firmas basado en atributos>

<3-1. Programa de extensión>

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

Permitamos que $\{p_1, \ldots, p_n\}$ sea un conjunto de variables. M^ := (M, ρ) es una matriz etiquetada donde la matriz M es una matriz (L filas x r columnas) sobre F_q, y ρ es una etiqueta de cada columna de la matriz M y está relacionada con uno de los literales $\{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$. Una etiqueta ρ_i (i = 1, ..., L) de cada fila de M está relacionada con uno de los literales, esto es, $\rho : \{1, ..., L\} \rightarrow \{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$.

Para cada secuencia de entrada $\delta \in \{0, 1\}^n$, se define una submatriz M_δ de la matriz M. La matriz M_δ es una submatriz que consiste en las filas de la matriz M, cuyas etiquetas ρ se relacionan con el valor "1" mediante la secuencia de entrada δ. Esto es, la matriz M_δ es una submatriz que consiste en las filas de la matriz M que están relacionadas con p_i con las cuales $\delta_i = 1$ y las filas de la matriz M que están relacionadas con $\neg p_i$ con las cuales $\delta_i = 0$.

La Fig. 2 es un dibujo explicativo de la matriz M_δ. Obsérvese que en la Fig. 2, n = 7, L = 6 y r = 5. Es decir, el conjunto de variables es $\{p_1, \ldots, p_7\}$, y la matriz M es una matriz (6 filas x 5 columnas). En la Fig. 2, suponemos que las etiquetas ρ están relacionadas de manera tal 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 $\neg p_5$.

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

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

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

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

El programa de extensión M^ acepta una secuencia de entrada δ si y sólo si $1^{\rightarrow} \in$ span $<M_\delta>$, y rechaza la secuencia de entrada δ de otro modo. Esto es, el programa de extensión M^ acepta la secuencia de entrada δ si y sólo si la combinación lineal de las filas de la matriz M_δ que se obtienen de la matriz M^ mediante la secuencia de entrada δ da $1^{\rightarrow}$. $1^{\rightarrow}$ es un vector de fila que tiene un valor de "1" "en cada elemento.

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

El programa de extensión se denomina monótono si sus etiquetas ρ se relacionan solamente con los literales positivos $\{p_1, \ldots, p_n\}$. El programa de extensión se llama no monótono si sus etiquetas ρ se relacionan con los literales $\{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$. Supongamos que el programa de extensión es no monótono. Una estructura de acceso (estructura de acceso no monótona) se constituye usando el programa de extensión no monótono.

Debido a que el programa de extensión no es monótono, sino no monótono, como se ha descrito anteriormente, se amplía la aplicación del esquema de firmas basado en atributos constituido usando el programa de extensión.

<3-2. Producto interno de los vectores de atributo y la estructura de acceso>

El mapa γ(j) descrito anteriormente se calculará usando el producto interno de los vectores de atributos. Esto es, qué fila de la matriz M ha de ser incluida en la matriz M_δ se determinará usando el producto interno de los vectores de atributos.

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

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

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

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

Cuando Γ se da a la estructura de acceso S, el mapa γ : {1, ..., L} → {0, 1} para el programa de extensión M^ := (M, ρ) se define como sigue. Para cada número entero i = 1, ..., L, el conjunto γ(j) = 1 si [ρ(i) = (t, $v^{\rightarrow}_i$)] ^ [(t, $x^{\rightarrow}_t$)] ∈ Γ ^ [$v^{\rightarrow}_i \cdot x^{\rightarrow}_t = 0$] o [ρ(i) = ¬(t, $v^{\rightarrow}_i$)] ^ [(t, $x^{\rightarrow}_t$)] ∈ Γ] ^ [$v^{\rightarrow}_i \cdot x^{\rightarrow}_t \neq 0$]. Establecemos γ(j) = 0 de otro modo.

Esto es, el mapa γ se calcula en base al producto interno de los vectores de atributo $v^{\rightarrow}$·y $x^{\rightarrow}$. Como se ha descrito anteriormente, qué fila de la matriz M ha de ser incluida en la matriz M_δ se determina por el mapa γ. Más específicamente, qué fila de la matriz M ha de ser incluida en la M_δ se determina por el producto interno de los vectores de atributo $v^{\rightarrow}$ y $x^{\rightarrow}$. La estructura de acceso S := (M, ρ) acepta Γ si y sólo si $1^{\rightarrow} \in$ span $\langle (M_i)_{\gamma(i)=1} \rangle$.

Una forma más simple de las relaciones de producto interno en las estructuras de acceso mencionadas anteriormente se obtiene cuando $n_t = 2$ para todo $t \in \{1, ..., d\}$ y $x^{\rightarrow} := (1, x)$ y $v^{\rightarrow} := (v, -1)$.

En este caso, (t, $x^{\rightarrow}_t$) := (t, (1, x)) y (t, $v^{\rightarrow}_i$) := (t, (v_i, -1)), que se simplificará como (t, x_t) y (t, v_i). Entonces, la estructura de acceso S es S := (M, ρ) de manera que ρ : {1, ..., L} → {(t, v), (t', v'), ... ¬(t, v), ¬(t', v'), ...} (v, v', ... ∈ F_q), y el conjunto de atributos Γ es Γ := {(t, x_t) | $x_t \in F_q$, $1 \leq t \leq d$}.

Cuando Γ se da a la estructura de acceso S, el mapa γ : {1, ..., L} → {0, 1} para el programa de extensión M^ := (M, ρ) se define como sigue: Para cada número entero i = 1, ..., L, establecemos γ(j) = 1 si [ρ(i) = (t, v_i)] ^ [(t, x_t) ∈ Γ] ^ [$v_i = x_t$] o [ρ(i) = ¬(t, v_i)] ^ [(t, x_t) ∈ Γ] ^ [$v_i \neq x_t$]. Establecemos γ(j) = 0 de otro modo.

<3-3. Esquema de distribución secreta>

Se describirá un esquema de distribución secreta para la estructura de acceso S := (M, ρ).

El esquema de distribución secreta está distribuyendo información secreta para presentarla información distribuida sin sentido. Por ejemplo, la información secreta s se permite que sea distribuida entre 10 paquetes para generar 10 partes de información distribuida. Cada una de las 10 partes de información distribuida no tiene información sobre la información secreta s. Por lo tanto, incluso cuando se obtiene una cierta parte de información distribuida, no se puede obtener información sobre la información secreta s. Por otra parte, si se obtienen todas de las 10 partes de información distribuida, se puede recuperar la información secreta s.

Otro esquema de distribución secreta también está disponible según el cual, incluso cuando no se puedan obtener todas de las 10 partes de información distribuida, si se pueden obtener una o más, pero no todas, (por ejemplo, 8 partes) de información distribuida, entonces se puede recuperar la información secreta s. Un caso como éste donde la información secreta s se puede recuperar usando 8 partes de entre las 10 partes de información distribuida se llamará 8 de entre 10. Es decir, un caso donde la información secreta s se puede recuperar usando t partes de entre las n partes de información distribuida se llamará t de entre n. Esta t se llamará umbral.

Otro esquema de distribución secreta más está disponible según el cual cuando se generan 10 partes de información distribuida d_1, …, d_{10}, la información secreta s se puede recuperar si se dan 8 partes de información distribuida d_1, …, d_8, pero no se puede si se dan 8 partes de información distribuida d_3, …, d_{10}. Esto es, este es un esquema de distribución secreta con el que se puede recuperar o no la información secreta s se controla no solamente por el número de partes de información distribuida obtenidas, sino también dependiendo de la combinación de la información distribuida.

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

Permitamos que una matriz M sea una matriz (L filas x r columnas). Permitamos que $f^{\rightarrow}$ sea un vector de columna indicado en la Fórmula 122.

[Fórmula 122]

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

Permitamos que s_0 indicado en la Fórmula 123 sea la información secreta a ser compartida.

[Fórmula 123]

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

Permitamos que $s^{\rightarrow T}$ indicado en la Fórmula 124 sea un vector de L partes de información distribuida de s_0.

[Fórmula 124]

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

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

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

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

Obsérvese la Fórmula 125.

[Fórmula 125]

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

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

Con el esquema de firmas basado en atributos según esta y las siguientes realizaciones, se construye una estructura de acceso aplicando el predicado de producto interno y el esquema de distribución secreta al programa de extensión, como se ha descrito anteriormente. Por lo tanto, el control de acceso se puede diseñar de manera flexible diseñando la matriz M en el programa de extensión y la información de atributo x y la información de atributo v (información de predicado) en el predicado de producto interno. Esto es, el control de acceso se puede diseñar de manera muy flexible. El diseño de la matriz M responde al diseño de condiciones de manera que el umbral del esquema de distribución secreta.

En particular, la estructura de acceso en el esquema de firmas basado en atributos según esta y las siguientes realizaciones constituye una estructura de acceso no monótona que usa un programa de extensión no monótono. Esto es, el esquema de firmas basado en atributos según esta y las siguientes realizaciones es un esquema de firmas con predicados no monótonos. De esta manera, la flexibilidad en el diseño de control de acceso mejora aún más.

<3-4. Función de comprobación aleatoria con resistencia a colisión>

Una función de comprobación aleatoria con resistencia a colisión es una función de comprobación aleatoria que es difícil de encontrar en dos entradas que comprueben aleatoriamente para la misma salida.

Permitamos que un número natural λ sea un parámetro de seguridad. Una familia de funciones de comprobación aleatoria resistente a colisión H asociada con el algoritmo G_{bpg}, y un polinomio poly(λ) especifican dos elementos:

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

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

Permitamos que ε sea una máquina de polinomio de tiempo probabilístico. Para todo λ, se define la Fórmula 126:

[Fórmula 126]

$$\mathrm{Adv}_{\varepsilon}^{\mathrm{H,CR}}(\lambda) := \Pr\left[(d_1, d_2) \in D^2 \wedge d_1 \neq d_2 \wedge \mathrm{H}_{\mathrm{hk}}^{\lambda,\mathrm{D}}(d_1) = \mathrm{H}_{\mathrm{hk}}^{\lambda,\mathrm{D}}(d_2)\right]$$

donde

$$D := \{0,1\}^{poly(\lambda)}$$

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

$$(d_1, d_2) \xleftarrow{R} \varepsilon(1^{\lambda}, hk, D)$$

H es una familia de funciones de comprobación aleatoria resistente a colisión si para cualquier polinomio de tiempo probabilístico ε adversario, $Adv_{\varepsilon}^{H,CR}(\lambda)$ es despreciable.

<4. Estructura de esquema de firmas basado en atributos>

<4-1. Estructura básica de esquema de firmas basado en atributos>

El esquema de firmas basado en atributos consta de cuatro algoritmos: Setup, KeyGen, Sig y Ver.

(Setup)

Un algoritmo Setup es un algoritmo aleatorizado que toma como entrada un parámetro de seguridad λ y un formato de atributo $\vec{n} := ((d; n_t, u_t, w_t, z_t (t = 1, ..., d))$, y emite un parámetro público pk y una clave maestra sk.

(KeyGen)

Un algoritmo KeyGen es un algoritmo aleatorizado que toma como entrada un conjunto de atributos $\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in F_q^{nt} \setminus \{\vec{0}\}, 1 \leq t \leq d\}$, el parámetro público pk y la clave maestra sk, y emite una clave de firma sk_{Γ}.

(Sig)

Un algoritmo Sig es un algoritmo aleatorizado que toma como entrada un mensaje m, una estructura de acceso S := (M, ρ) que acepta el conjunto de atributos Γ, la clave de firma sk_{Γ} y el parámetro público pk, y emite datos de firma σ incluyendo una firma $\vec{s}^*$, el mensaje m, y la estructura de acceso S.

(Ver)

Un algoritmo Ver es un algoritmo que toma como entrada los datos de firma σ y el parámetro público pk, y emite un valor booleano 1 (aceptar) o 0 (rechazar).

Con el esquema de firmas basado en atributos, para cada parámetro público pk y clave maestra sk indicados en Fórmula 127, cada mensaje m, cada conjunto de atributos Γ, cada clave de firma sk_{Γ} indicados en Fórmula 128, cada estructura de acceso S que acepta el conjunto de atributos Γ, y cada uno de los datos de firma σ indicados en Fórmula 129, 1 = Ver(pk, m, S, σ) se mantiene con probabilidad 1.

[Fórmula 127]

$$(pk, sk) \xleftarrow{R} Setup(1^{\lambda}, \vec{n})$$

[Fórmula 128]

$$sk_{\Gamma} \xleftarrow{R} KeyGen(pk, sk, \Gamma)$$

[Fórmula 129]

$$\sigma \xleftarrow{R} Sig(pk, sk_{\Gamma}, m, \mathbb{S})$$

<4-2. Sistema de procesamiento de firmas 10>

Se describirá un sistema de procesamiento de firmas 10 que ejecuta los algoritmos del esquema de firmas basado en atributos descrito anteriormente.

La Fig. 5 es un diagrama de configuración del sistema de procesamiento de firmas 10 que ejecuta el esquema de firmas basado en atributos.

El sistema de procesamiento de firmas 10 está dotado con un dispositivo de generación de claves 100, un dispositivo de firmas 200 y un dispositivo de verificación 300.

El dispositivo de generación de claves 100 ejecuta el algoritmo Setup tomando como entrada un parámetro de seguridad λ y un formato de atributo $n^{\rightarrow} := ((d; n_t, u_t, w_t, z_t\ (t = 1, ..., d))$, y genera un parámetro público pk y una clave maestra sk. El dispositivo de generación de claves 100 hace público el parámetro público pk generado. El dispositivo de generación de claves 100 también ejecuta el algoritmo KeyGen tomando como entrada el conjunto de atributos $\Gamma := \{(t, x^{\rightarrow}_t) \mid x^{\rightarrow}_t \in F_q^{nt} \setminus \{0^{\rightarrow}\}, 1 \leq t \leq d\}$, el parámetro público pk y la clave maestra sk, y genera una clave de firma sk_Γ y la distribuye al dispositivo de firmas 200 en secreto.

El dispositivo de firmas 200 ejecuta el algoritmo Sig tomando como entrada un mensaje m, una estructura de acceso S := (M, ρ) que acepta el conjunto de atributos Γ, la clave de firma sk_Γ y el parámetro público pk, y genera datos de firma σ que incluyen una firma $s^{\rightarrow}*$, el mensaje m, y la estructura de acceso S. El dispositivo de firmas 200 transmite los datos de firma σ generados al dispositivo de verificación 300.

El dispositivo de verificación 300 ejecuta el algoritmo Ver tomando como entrada los datos de firma σ y el parámetro público pk, y emite el valor booleano 1 (aceptar) o 0 (rechazar).

<4-3. Esquema de firmas basado en atributos y sistema de procesamiento de firmas 10 en detalle>

El esquema de firmas basado en atributos, y la función y operación del sistema de procesamiento de firmas 10 que ejecuta el esquema de firmas basado en atributos se describirán con referencia a las Fig. 6 a 12.

La Fig. 6 es un diagrama de bloques de funciones que muestra la función del dispositivo de generación de claves 100. La Fig.7 es un diagrama de bloques de funciones que muestra la función del dispositivo de firmas 200. La Fig. 8 es un diagrama de bloques de funciones que muestra la función del dispositivo de verificación 300.

Las Fig. 9 y 10 son diagramas de flujo que muestran la operación del dispositivo de generación de claves 100. Obsérvese que la Fig. 9 es un diagrama de flujo que muestra el proceso del algoritmo Setup, y que la Fig. 10 es un diagrama de flujo que muestra el proceso del algoritmo KeyGen. La Fig. 11 es un diagrama de flujo que muestra la operación del dispositivo de firmas 200 y el proceso del algoritmo Sig. La Fig. 12 es un diagrama de flujo que muestra la operación del dispositivo de verificación 300 y el proceso del algoritmo Ver.

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

Como se muestra en la Fig. 6, el dispositivo de generación de claves 100 está dotado con una parte de generación de clave maestra 110, una parte de almacenamiento de clave maestra 120, una parte de entrada de información 130 (primera parte de entrada de información), una parte de generación de clave de firma 140 y una parte de distribución de clave 150 (parte de transmisión de clave de firma).

La parte de generación de clave de firma 140 está dotada con una parte de generación de número aleatorio 141, una parte de generación del elemento de clave 0 142, una parte de generación de elemento de clave t 143, y una parte de generación de elemento de clave d+1 144.

En la siguiente descripción, $H := (KH_\lambda, H_{hk}^{\lambda,D})$ es una familia de funciones de comprobación aleatoria resistente a colisión descrita anteriormente.

El proceso del algoritmo Setup ejecutado por el dispositivo de generación de claves 100 se describirá primero con referencia a la Fig. 9.

(S 101: Paso de generación de base ortogonal)

La parte de generación de clave maestra 110 calcula la Fórmula 130 con el dispositivo de procesamiento para generar aleatoriamente el $param_{n^{\rightarrow}}$, y las bases B_t y B^*_t para cada número entero t = 0, ..., d+1.

[Fórmula 130]

$$(1)\ \text{input}\ \ 1^\lambda, \vec{n} := (d; n_t, u_t, w_t, z_t)\ \ (t = 0, ..., d+1)$$

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

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

$N_t := n_t + u_t + w_t + z_t$ *para* $t = 0, ..., d+1$

Para cada t de t = 0, ..., d+1, se ejecutan los procesos (4) a (8).

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

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

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

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

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

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

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

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

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

Esto es, la parte de generación de clave maestra 110 ejecuta los siguientes procesos.

(1) Con el dispositivo de entrada, la parte de generación de clave maestra 110 toma como entrada un parámetro de seguridad λ (1^{λ}) y el formato de atributo $\vec{n} := ((d; n_t, u_t, w_t, z_t (t = 1, ..., d+1))$, donde d es un número entero de 1 o más, y n_t es 1 para t = 0, un número entero de 1 o más para cada número entero t = 1, ..., d, y 2 para t = d+1. Cada u_t, w_t y z_t es un número entero de 1 o más para cada número entero t = 0, ..., d+1.

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

(3) Con el dispositivo de procesamiento, la parte de generación de clave maestra 110 genera un número aleatorio ψ, y establece $n_t + u_t + w_t + z_t$ en N_t para cada número entero t = 0, ..., d+1.

Posteriormente, la parte de generación de clave maestra 110 ejecuta los procesos de los siguientes (4) a (8) para cada número entero t = 0, ..., d+1.

(4) Con el dispositivo de procesamiento, la parte de generación de clave maestra 110 ejecuta el algoritmo G_{dpvs} tomando como entrada el parámetro de seguridad λ (1^{λ}) introducido en (1), N_t establecido en (3), y los valores de $\text{param}_G := (q, G, G_T, g, e)$ generados en (2), y genera los valores del parámetro $\text{param}_{vt} := (q, V_t, G_T, A_t, e)$ de los espacios vectoriales de emparejamiento dual.

(5) Con el dispositivo de procesamiento, la parte de generación de clave maestra 110 toma como entrada N_t establecido en (3) y F_q, y genera la transformación lineal $X_t := (\chi_{t,i,j})_{i,j}$ aleatoriamente. Obsérvese que GL representa Lineal General. Esto es, GL es un grupo lineal general, un conjunto de matrices cuadradas en las cuales el determinante no es 0, y un grupo con respecto a la multiplicación. Obsérvese que $(\chi_{t,i,j})_{i,j}$ significa una matriz que concierne a los sufijos i y j de la matriz $\chi_{t,i,j}$ donde i, j = 1, ..., n_t.

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

(7) Con el dispositivo de procesamiento y en base a la transformación lineal X_t generada en (5), la parte de generación de clave maestra 110 genera la base B_t a partir de la base canónica A_t generada en (4).

(8) Con el dispositivo de procesamiento y en base a $(v_{t,i,j})_{i,j}$ generada en (6), la parte de generación de clave maestra 110 genera la base B^*_t a partir de la base canónica A_t generada en (4).

(9) Con el dispositivo de procesamiento, la parte de generación de clave maestra 110 establece $e(g, g)^{\psi}$ en g_T. La parte de generación de clave maestra 110 también establece $\{param_{vt}\}_{t = 0, ..., d+1}$ generado en (4), y g_T, en $param_{n\rightarrow}$. Obsérvese que $g_T = e(b_{t,i}, b^*_{t,i})$ para cada número entero t = 0, ..., d+1 y cada número entero i = 1, ..., N_t.

En resumen, en (S101), la parte de generación de clave maestra 110 ejecuta el algoritmo G_{ob} indicado en la Fórmula 131, y genera $param_{n\rightarrow}$, y las bases B_t y B^*_t para cada número entero t = 0, ..., d+1.

[Fórmula 131]

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

(S102: Paso de generación de clave de comprobación aleatoria)

Con el dispositivo de procesamiento, la parte de generación de clave maestra 110 calcula la Fórmula 132, para generar aleatoriamente una clave de comprobación aleatoria hk.

[Fórmula 132]

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

(S103: Paso de generación de parámetro público)

Con el dispositivo de procesamiento, la parte de generación de clave maestra 110 genera una subbase $B^\wedge_0$ de la base B_0, una subbase $B^\wedge_t$ de la base B_t para cada número entero t = 1, ..., d, y una subbase $B^\wedge_{d+1}$ de la base B_{d+1}, como se indica en Fórmula 133.

[Fórmula 133]

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

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

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

Con el dispositivo de procesamiento, la parte de generación de clave maestra 110 genera una subbase $B^{\wedge *}_t$, de la base B^*_t, para cada número entero t = 1, ..., d, y una subbase $B^{\wedge *}_{d+1}$ de la base B_{d+1}, como se indica en la Fórmula 134.

[Fórmula 134]

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

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

La parte de generación de clave maestra 110 trata las subbases generadas $B^\wedge_d$ (t = 0, ..., d+1) y $B^{\wedge *}_t$ (t = 1, ..., d+1), el parámetro de seguridad λ (1^λ) introducido en (S101), $param_{n\rightarrow}$ generado en (S101), la clave de comprobación aleatoria hk generada en (S102), y los vectores base $b^*_{0,1+u0+1}$, ..., $b^*_{0,1+u0+w0}$ (donde u0 y w0 representan u_0 y w_0) en combinación, como el parámetro público pk.

(S104: Paso de generación de clave maestra)

La parte de generación de clave maestra 110 trata un vector base $b^*_{0,}1$ de la base B^*_0, como la clave maestra sk.

(S105: Paso de almacenamiento de clave maestra)

La parte de almacenamiento de clave maestra 120 almacena el parámetro público pk generado en (S103), en el dispositivo de almacenamiento. La parte de almacenamiento de clave maestra 120 también almacena la clave maestra sk generada en (S104), en el dispositivo de almacenamiento.

En resumen, desde (S101) hasta (S104), el dispositivo de generación de claves 100 genera el parámetro público pk y la clave maestra sk ejecutando el algoritmo Setup indicado en la Fórmula 135. Entonces, en (S105), el dispositivo de generación de claves 100 almacena el parámetro público pk y la clave maestra sk generados, en el dispositivo de almacenamiento.

Obsérvese que el parámetro público se hace público a través de, por ejemplo, una red, de modo que el dispositivo de firmas 200 y el dispositivo de verificación 300 pueden adquirirlo.

[Fórmula 135]

$$\mathsf{Setup}(1^{\lambda}, \vec{n} := (d; n_t, u_t, w_t, z_t)\ (t = 0,...,d+1))$$

$$\mathsf{hk} \xleftarrow{R} \mathsf{KH}_{\lambda},\ n_0 := 1,\ n_{d+1} := 2,$$

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

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

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

$$\mathsf{sk} := b_{0,1}^*,$$

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

$$b_{0,1+u_0+1}^*,...,b_{0,1+u_0+w_0}^*).$$

devolver sk, pk.

El proceso del algoritmo KeyGen ejecutado por el dispositivo de generación de claves 100 se describirá con referencia a la Fig. 10.

(S201: Paso de entrada de información)

Con el dispositivo de entrada, la parte de entrada de información 130 toma como entrada un conjunto de atributos $\Gamma := \{(t, \vec{x}_t := (x_{t,i})\ (i = 1, \ldots, n_t)) | 1 \leq t \leq d\}$. Obsérvese que t no necesita ser todos los números enteros t dentro del intervalo de $1 \leq t \leq d$, sino que puede ser al menos uno de los números enteros t dentro del intervalo de $1 \leq t \leq d$.

(S202: Paso de generación de número aleatorio]

Con el dispositivo de procesamiento, la parte de generación de número aleatorio 141 genera un número aleatorio δ, y los números aleatorios Φ_0, $\Phi_{t,\tau}$, $\Phi_{d+1,1,\tau}$, y $\Phi_{d+1,2,\tau}$ ($t = 1, ..., d$; $\tau = 1, ..., w_t$), como se indica en la Fórmula 136.

[Fórmula 136]

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

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

$$\vec{\varphi}_t := (\varphi_{t,1},...,\varphi_{t,w_t}) \xleftarrow{U} \mathbb{F}_q^{w_t} \text{ para } t = 1,...,d,$$

$$\vec{\varphi}_{d+1,1} := (\varphi_{d+1,1,1},...,\varphi_{d+1,1,w_{d+1}}), \vec{\varphi}_{d+1,2} := (\varphi_{d+1,2,1},...,\varphi_{d+1,2,w_{d+1}})$$

$$\xleftarrow{U} \mathbb{F}_q^{w_{d+1}}$$

(S203: Paso de generación del elemento de clave 0)

Con el dispositivo de procesamiento, la parte de generación del elemento de clave 0 142 genera un elemento de clave k^*_0, que es un elemento de la clave de firma sk_Γ, como se indica en la Fórmula 137.

[Fórmula 137]

$$k_0^* := (\delta, \overbrace{0^{u_0}}^{u_0}, \overbrace{\varphi_{0,1},\ldots,\varphi_{0,w_0}}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*}$$

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 137 significa que el coeficiente para el vector base de una base B^*_0 se establece como se describe a continuación. Con el propósito de una representación simple, un vector bases $b^*_{0,i}$ se especifica solamente por su parte i. Por ejemplo, un vector base 1 significa un vector base $b^*_{0,1}$. Los vectores base 1, ..., 3 significan vectores base $b^*_{0,1}$, ..., $b^*_{0,3}$, respectivamente.

El número aleatorio δ se establece como el coeficiente para el vector base 1 de la base B^*_0. 0 se establece como el coeficiente para los vectores base 1+1, ..., $1+u_0$. Los números aleatorios $\Phi_{0,1}$, …, $\Phi_{0,w0}$ (donde w0 representa w_0) se establecen cada uno como el coeficiente para los vectores base $1+u_0+1$, …, $1+u_0+w_0$. 0 se establece como el coeficiente para los vectores base $1+u_0+w_0+1$, …, $1+u_0+w_0+z_0$.

(S204: paso de generación del elemento de clave t)

Con el dispositivo de procesamiento, la parte de generación de elemento del clave t 143 genera un elemento de clave k*, que es un elemento de la clave de firma sk_Γ, para cada número entero t de $(t, x\rightarrow_t)$ incluido en el conjunto de atributos Γ, como se indica en la Fórmula 138.

[Fórmula 138]

$$k_t^* := (\overbrace{\delta(x_{t,1},\ldots,x_{t,n_t})}^{n_t}, \overbrace{0^{u_t}}^{u_t}, \overbrace{\varphi_{t,1},\ldots,\varphi_{t,w_t}}^{w_t}, \overbrace{0^{z_t}}^{z_t})_{\mathbb{B}_t^*} \text{ para } (t, \vec{x}_t) \in \Gamma$$

Más específicamente, como lo hace la Fórmula 137, la Fórmula 138 significa que el coeficiente para el vector base de una base B^*_t se establece como se describe a continuación. Con el propósito de una representación simple, un vector base $b^*_{t,i}$ se especifica solamente por su parte i. Por ejemplo, un vector base 1 significa un vector base $b^*_{t,1}$. Los vectores base 1, ..., 3 significan vectores base $b^*_{t,1}$, ..., $b^*_{t,3}$, respectivamente.

$\delta x_{t,1}$, ..., $\delta x_{t,nt}$, (donde nt representa n_t) se establecen cada uno como el coeficiente para los vectores base 1, ..., n_t. 0 se establece como el coeficiente para los vectores base n_t+1, ... , n_t+u_t. Los números aleatorios $\Phi_{t,1}$, …, $\Phi_{t,wt}$ (donde wt representa w_t) se establecen cada uno como el coeficiente para los vectores base n_t+u_t+1, ..., $n_t+u_t+w_t$. 0 se establece como el coeficiente para los vectores base $n_t+u_t+w_t+1$, ..., $n_t+u_t+w_t+z_t$.

(S205: Paso de generación del elemento de clave d+1)

Con el dispositivo de procesamiento, la parte de generación del elemento de clave d+1 144 genera un elemento de clave $k^*_{d+1,1}$ y un elemento de clave $k^*_{d+1,2}$, que son elementos de la clave de firma sk_Γ, como se indica en la Fórmula 139.

[Fórmula 139]

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

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

Esto es, como lo hace la Fórmula 137, la Fórmula 139 significa que el coeficiente para el vector base de la base B^*_{d+1} se establece como se describe a continuación. Con el propósito de una representación simple, un vector base $b^*_{d+1,i}$ se especifica solamente por su parte i. Por ejemplo, un vector base 1 significa un vector base $b^*_{d+1,1}$. Los vectores base 1, ..., 3 significan vectores base $b^*_{d+1,1}$, ..., $b^*_{d+1,3}$, respectivamente.

Primero, con respecto al elemento de clave $k^*_{d+1,1}$, el número aleatorio δ se establece como el coeficiente para el vector base 1. 0 se establece como el coeficiente para el vector base 2. 0 se establece como el coeficiente para los vectores base 2+1, ..., $2+u_{d+1}$. Los números aleatorios $\Phi_{d+1,1,1}$, …, $\Phi_{d+1,1,wd+1}$ (donde wd+1 representa w_{d+1}) se

establecen cada uno como el coeficiente para los vectores base $2+u_{d+1}+1$, ..., $2+u_{d+1}+w_{d+1}$. 0 se establece como el coeficiente para los vectores base $2+u_{d+1}+w_{d+1}+1$, ..., $2+u_{d+1}+w_{d+1}+z_{d+1}$.

Con respecto al elemento de clave $k^*_{d+1,2}$, 0 se establece como el coeficiente para el vector base 1. El número aleatorio δ se establece como el coeficiente para el vector base 2. 0 se establece como el coeficiente para los vectores base 2+1, ..., $2+u_{d+1}$. Los números aleatorios $\Phi_{d+1,2,1}$, …, $\Phi_{d+1,2,wd+1}$ (donde wd+1 representa w_{d+1}) se establecen cada uno como el coeficiente para los vectores base $2+u_{d+1}+1$, ..., $2+u_{d+1}+w_{d+1}$. 0 se establece como el coeficiente para los vectores base $2+u_{d+1}+w_{d+1}+1$, ..., $2+u_{d+1}+w_{d+1}+z_{d+1}$.

(S206: Paso de distribución de clave)

Por ejemplo, con el dispositivo de comunicación, la parte de distribución de clave 150 distribuye la clave de firma sk_Γ, constituida por, como elementos, el conjunto de atributos Γ, el elemento de clave k^*_0, el elemento de clave k^*_t (t en (t, $\vec{x}_t$) incluido en el conjunto de atributos Γ), el elemento de clave $k^*_{d+1,1}$, y el elemento de clave $k^*_{d+1,2}$, al dispositivo de firmas 200 en secreto a través de la red. Como cuestión de rutina, la clave de firma sk_Γ se puede distribuir al dispositivo de firmas 200 por otro método.

En resumen, desde (S201) hasta (S205), el dispositivo de generación de claves 100 genera la clave de firma sk_Γ ejecutando el algoritmo KeyGen indicado en la Fórmula 140. En (S206), el dispositivo de generación de claves 100 distribuye la clave de firma sk_Γ generada al dispositivo de firmas 200.

[Fórmula 140]

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

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

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

$$\vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t} \quad \text{para } t = 1,\ldots,d,$$

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

$$k_0^* := (\delta, \overbrace{0^{u_0}}^{u_0}, \overbrace{\varphi_{0,1},\ldots,\varphi_{0,w_0}}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*},$$

$$k_t^* := (\overbrace{\delta(x_{t,1},\ldots,x_{t,n_t})}^{n_t}, \overbrace{0^{u_t}}^{u_t}, \overbrace{\varphi_{t,1},\ldots,\varphi_{t,w_t}}^{w_t}, \overbrace{0^{z_t}}^{z_t})_{\mathbb{B}_t^*}$$

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

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

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

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

$$\text{devolver } \mathsf{sk}_\Gamma := (\Gamma, \{k_t^*\}_{t \in T}).$$

Se describirán la función y la operación del dispositivo de firmas 200.

Como se muestra en la Fig. 7, el dispositivo de firmas 200 está dotado con una parte de adquisición de clave de firma 210, una parte de entrada de información 220 (segunda parte de entrada de información), una parte de cálculo de programa de extensión 230, una parte de cálculo de coeficiente complementario 240, una parte de generación de datos de firma 250, y una parte de transmisión de datos de firma 260 (parte de salida de datos de firma).

La parte de entrada de información 220 está dotada con una parte de entrada de información de predicado 221 y una parte de entrada de mensaje 222. La parte de generación de datos de firma 250 está dotada con una parte de

generación de número aleatorio 251, una parte de generación del elemento de firma 0 252, una parte de generación del elemento de firma i 253, y una parte de generación del elemento de firma L+1 254.

El proceso del algoritmo Sig ejecutado por el dispositivo de firmas 200 se describirá con referencia a la Fig. 11.

(S301: Paso de adquisición de clave de firma)

Por ejemplo, con el dispositivo de comunicación, la parte de adquisición de clave de firma 210 adquiere la clave de firma sk_Γ generada por el dispositivo de generación de claves 100, a través de la red. La parte de adquisición de clave de firma 210 también adquiere el parámetro público pk generado por el dispositivo de generación de claves 100.

(S302: Paso de entrada de información]

Con el dispositivo de entrada, la parte de entrada de información de predicado 221 toma como entrada la estructura de acceso S := (M, ρ). La matriz M es una matriz de L filas x r columnas. L y r son cada uno un número entero de 1 o más.

Con el dispositivo de entrada, la parte de entrada de mensaje 220 toma como entrada el mensaje m a ser firmado.

La matriz M de la estructura de acceso S ha de ser establecida dependiendo de la condición del sistema a ser realizado.

(S303: Paso de cálculo de programa de extensión)

Con el dispositivo de procesamiento, la parte de cálculo de programa de extensión 230 comprueba si la estructura de acceso S introducida en (S302) acepta o no el conjunto de atributos Γ incluido en la clave de firma sk_Γ adquirida en (S301).

El método de comprobación de si la estructura de acceso acepta o no el conjunto de atributos es el mismo que el descrito en “3. Concepto para implementar cifrado funcional”.

La parte de cálculo de programa de extensión 230 avanza el proceso a (S304) si la estructura de acceso S acepta el conjunto de atributos Γ (aceptar en S303). Si la estructura de acceso S rechaza el conjunto de atributos Γ (rechazar en S303), la parte de cálculo de programa de extensión 230 termina el proceso.

(S304: Paso de cálculo de coeficiente complementario)

Con el dispositivo de procesamiento, la parte de cálculo de coeficiente complementario 430 calcula I y una constante (coeficiente complementario) α_i para cada número entero incluido en I, cuyo I y α_i que satisfacen la Fórmula 141.

[Fórmula 141]

$$\sum_{i\in I}\alpha_i M_i := \vec{1}$$

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

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

Obsérvese que M_i significa la fila de orden i de la matriz M.

(S305: Paso de generación de número aleatorio)

Con el dispositivo de procesamiento, la parte de generación de número aleatorio 251 genera un número aleatorio ξ y un número aleatorio β_i (i = 1, ..., L), como se indica en la Fórmula 142.

[Fórmula 142]

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

$$(\beta_i) \xleftarrow{U} \{(\beta_1,...,\beta_L) \Big| \sum_{i=1}^{L} \beta_i M_i = \vec{0}\}$$

(S306: Paso de generación del elemento de firma 0)

Con el dispositivo de procesamiento, la parte de generación del elemento de firma 0 252 genera s^*_0 que es un elemento de los datos de firma σ, como se indica en la Fórmula 143.

[Fórmula 143]

$$s_0^* := \xi k_0^* + r_0^*$$

Obsérvese que r^*_0 está definido por la Fórmula 144 (véanse las Fórmulas 110 hasta 112 y sus explicaciones).

[Fórmula 144]

$$r_0^* \xleftarrow{U} \mathrm{span}\left\langle b_{0,1+u_0+1}^*, \ldots, b_{0,1+u_0+w_0}^* \right\rangle$$

(S307: Paso de generación del elemento de firma i)

Con el dispositivo de procesamiento, la parte de generación del elemento de firma i 253 genera un elemento de firma s^*_i que es un elemento de los datos de firma σ, para cada número entero i = 1, ..., L, como se indica en la Fórmula 145.

[Fórmula 145]

$$s_i^* := \gamma_i \cdot \xi k_t^* + \sum_{l=1}^{n_t} y_{i,l} \cdot b_{t,l}^* + r_i^* \quad \text{para } 1 \le i \le L$$

Obsérvese que r^*_i se define por la Fórmula 146 (véanse las Fórmulas 110 hasta 112 y sus explicaciones).

[Fórmula 146]

$$r_i^* \xleftarrow{U} \mathrm{span}\left\langle b_{t,n_t+u_t+1}^*, \ldots, b_{t,n_t+u_t+w_t}^* \right\rangle$$

También, γ_i e $\vec{y}_i := (y_{i,i'})$ (i' = 1, ..., n_t) se definen por la Fórmula 147.

[Fórmula 147]

$$\begin{aligned}
&\text{si } i \in I \wedge \rho(i) = (t, \vec{v}_i), \quad \gamma_i := \alpha_i,\ \vec{y}_i \xleftarrow{U} \{\vec{y}_i \mid \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},\\
&\text{si } i \in I \wedge \rho(i) = \neg(t, \vec{v}_i), \quad \gamma_i := \frac{\alpha_i}{\vec{v}_i \cdot \vec{x}_t},\\
&\qquad\qquad \vec{y}_i \xleftarrow{U} \{\vec{y}_i \mid \vec{y}_i \cdot \vec{v}_i = \beta_i\},\\
&\text{si } i \notin I \wedge \rho(i) = (t, \vec{v}_i), \quad \gamma_i := 0,\ \vec{y}_i \xleftarrow{U} \{\vec{y}_i \mid \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},\\
&\text{si } i \notin I \wedge \rho(i) = \neg(t, \vec{v}_i), \quad \gamma_i := 0,\\
&\qquad\qquad \vec{y}_i \xleftarrow{U} \{\vec{y}_i \mid \vec{y}_i \cdot \vec{v}_i = \beta_i\}
\end{aligned}$$

(S308: Paso de generación del elemento de firma L+1)

Con el dispositivo de procesamiento, la parte de generación del elemento de firma L+1 254 genera un elemento de firma s^*_{L+1}, que es un elemento de los datos de firma σ, como se indica en la Fórmula 148.

[Fórmula 148]

$$s^*_{L+1} := \xi(k^*_{d+1,1} + \mathsf{H}^{\lambda,D}_{hk}(m \| \mathbb{S}) \cdot k^*_{d+1,2}) + r^*_{L+1}$$

Obsérvese que r^*_{L+1} se define por la Fórmula 149 (véanse las Fórmulas 110 hasta 112 y sus explicaciones).

[Fórmula 149]

$$r^*_{L+1} \xleftarrow{U} \mathrm{span}\left\langle b^*_{d+1,2+u_{d+1}+1}, \ldots, b^*_{d+1,2+u_{d+1}+w_{d+1}} \right\rangle$$

(S309: Paso de transmisión de datos)

Por ejemplo, con el dispositivo de comunicación, la parte de transmisión de datos de firma 260 transmite los datos de firma σ, incluyendo el elemento de firma s^*_0, el elemento de firma s^*_i (i = 1, ..., L), el elemento de firma s^*_{L+1}, el mensaje m, y la estructura de acceso S := (M, ρ), al dispositivo de verificación 300 a través de la red. Como cuestión de rutina, los datos de firma σ se pueden transmitir al dispositivo de verificación 300 por otro método.

En resumen, desde (S301) hasta (S308), el dispositivo de firmas 200 genera los datos de firma σ ejecutando el algoritmo Sig indicado en la Fórmula 150. En (S309), el dispositivo de firmas 200 distribuye los datos de firma σ generados al dispositivo de verificación 300.

[Fórmula 150]

$$\mathrm{Sig}(\mathrm{pk}, \mathrm{sk}_\Gamma, m, \mathbb{S} := (M, \rho))$$

si $\mathbb{S} := (M, \rho)$ acepta $\Gamma := \{(t, \vec{x}_t)\}$,

entonces calcular I y $\{\alpha_i\}_{i \in I}$ de manera que

$$\sum_{i \in I} \alpha_i M_i := \vec{1}$$

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

$$\xi \xleftarrow{U} \mathbb{F}_q^\times, \quad (\beta_i) \xleftarrow{U} \{(\beta_1, \ldots, \beta_L) \mid \textstyle\sum_{i=1}^{L} \beta_i M_i = \vec{0}\},$$

$$s^*_0 := \xi k^*_0 + r^*_0, \quad \text{donde } r^*_0 \xleftarrow{U} \mathrm{span}\left\langle b^*_{0,1+u_0+1}, \ldots, b^*_{0,1+u_0+w_0} \right\rangle,$$

$$s^*_i := \gamma_i \cdot \xi k^*_t + \textstyle\sum_{\iota=1}^{n_t} y_{i,\iota} \cdot b^*_{t,\iota} + r^*_i, \text{ para } 1 \le i \le L,$$

$$\text{donde } r^*_i \xleftarrow{U} \mathrm{span}\left\langle b^*_{t,n_t+u_t+1}, \ldots, b^*_{t,n_t+u_t+w_t} \right\rangle,$$

$$\text{y } \gamma_i, \vec{y}_i := (y_{i,1}, \ldots, y_{i,n_t}) \text{ se definen como}$$

$$\text{si } i \in I \wedge \rho(i) = (t, \vec{v}_i), \quad \gamma_i := \alpha_i, \quad \vec{y}_i \xleftarrow{U} \{\vec{y}_i \mid \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},$$

$$\text{si } i \in I \wedge \rho(i) = \neg(t, \vec{v}_i), \quad \gamma_i := \frac{\alpha_i}{\vec{v}_i \cdot \vec{x}_t},$$

$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

$$\text{si } i \notin I \wedge \rho(i) = (t, \vec{v}_i),\ \ \gamma_i := 0,\ \ \vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},$$

$$\text{si } i \notin I \wedge \rho(i) = \neg(t, \vec{v}_i),\ \ \gamma_i := 0,$$

$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

$$s^*_{L+1} := \xi(k^*_{d+1,1} + \mathsf{H}^{\lambda,\mathsf{D}}_{\mathsf{hk}}(m \| \mathbb{S}) \cdot k^*_{d+1,2}) + r^*_{L+1},$$

$$\text{donde } r^*_{L+1} \xleftarrow{U} \text{span}\left\langle b^*_{d+1,2+u_{d+1}+1}, \ldots, b^*_{d+1,2+u_{d+1}+w_{d+1}} \right\rangle,$$

$$\text{devolver } \vec{s}^* := (s^*_0, \ldots, s^*_{L+1}).$$

Se describirán la función y la operación del dispositivo de verificación 300.

Como se muestra en la Fig. 8, el dispositivo de verificación 300 está dotado con una parte de adquisición de parámetro público 310, una parte de recepción de datos 320, una parte de generación de clave de verificación 330, y una parte de operación de emparejamiento 340.

La parte de generación de clave de verificación 330 está dotada con una parte de generación de número aleatorio 331, una parte de generación de vector f 332, una parte de generación de vector s 333, una parte de generación del elemento de verificación 0 334, una parte de generación del elemento de verificación i 335, y una parte de generación del elemento de verificación L+1 336.

El proceso del algoritmo Ver ejecutado por el dispositivo de verificación 300 se describirá con referencia a la Fig. 12.

(S401: Paso de adquisición de parámetro público)

Por ejemplo, con el dispositivo de comunicación, la parte de adquisición de parámetro público 310 adquiere el parámetro público pk generado por el dispositivo de generación de claves 100, a través de la red.

(S402: Paso de recepción de datos de firma)

Por ejemplo, con el dispositivo de comunicación, la parte de recepción de datos 320 recibe los datos de firma σ transmitidos por el dispositivo de firmas 200, a través de la red.

(S403: Paso de generación de vector f)

Con el dispositivo de procesamiento, la parte de generación de vector f 332 genera un vector $\vec{f}$ que tiene r partes de elementos, aleatoriamente como se indica en la Fórmula 151.

[Fórmula 151]

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

(S404: Paso de generación de vector s)

Con el dispositivo de procesamiento, la parte de generación de vector s 333 genera un vector $\vec{s}^{\mathrm{T}}$, en base a la matriz M (L filas x r columnas) de la estructura de acceso S incluida en los datos de firma σ recibidos en (S402) y el vector $\vec{f}$ generado en (S403) y que tiene r partes de elementos, como se indica en la Fórmula 152.

[Fórmula 152]

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

Con el dispositivo de procesamiento, la parte de generación de vector s 333 genera un valor s_0 basado en el vector $\vec{f}$ generado en (S403), como se indica en la Fórmula 153. Obsérvese que $\vec{1}$ es un vector que tiene un valor 1 en todos sus elementos.

[Fórmula 153]

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

(S405: Paso de generación de número aleatorio)

Con el dispositivo de procesamiento, la parte de generación de número aleatorio 331 genera un número aleatorio $\eta_{0,i}$ para cada número entero i = 1, ..., z_0, un número aleatorio $\eta_{L+1,i}$ para cada número entero i = 1, ..., z_{d+1}, un número aleatorio θ_{L+1}, y un número aleatorio s_{L+1}, como se indica en la Fórmula 154.

[Fórmula 154]

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

$$\eta_{L+1} := (\eta_{L+1,1},\ldots,\eta_{L+1,z_{d+1}}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{z_{d+1}},$$

$$\theta_{L+1}, s_{L+1} \xleftarrow{\mathrm{U}} \mathbb{F}_q$$

(S406: Paso de generación del elemento de verificación 0)

Con el dispositivo de procesamiento, la parte de generación del elemento de verificación 0 334 genera un elemento de verificación c_0, que es un elemento de la clave de verificación, como se indica en la Fórmula 155.

[Fórmula 155]

$$c_0 := (-s_0 - s_{L+1}, \overbrace{0^{u_0}}^{u_0}, \overbrace{0^{w_0}}^{w_0}, \overbrace{\eta_{0,1},\ldots,\eta_{0,z_0}}^{z_0})_{\mathbb{B}_0}$$

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 155 significa que el coeficiente para el vector base de la base B_0 se establece como se describe a continuación. Con el propósito de una representación simple, un vector base $b_{0,i}$ se especifica solamente por su parte i. Por ejemplo, un vector base 1 significa un vector base $b_{0,1}$. Los vectores base 1, ..., 3 significan los vectores base $b_{0,1}$, ..., $b_{0,3}$, respectivamente.

$-s_0-s_{L+1}$ se establece como el coeficiente para el vector base 1 de la base B_0. 0 se establece como el coeficiente para los vectores base 1+1, ..., $1+u_0+w_0$. Los números aleatorios $\eta_{0,1}$, $\eta_{0,z0}$ (donde z0 representa z_0) se establecen cada uno como el coeficiente para los vectores base $1+u_0+w_0+1$, ..., $1+u_0+w_0+z_0$ (donde z0 representa z_0).

(S407: Paso de generación del elemento de verificación i)

Con el dispositivo de procesamiento, la parte de generación del elemento de verificación i 335 genera un elemento de verificación c_i, que es un elemento de la clave de verificación, para cada número entero i = 1, ..., L, como se indica en la Fórmula 156.

[Fórmula 156]

$$\text{si } \rho(i) = (t, \vec{v}_i := (v_{i,1},\ldots,v_{i,n_t}) \in \mathbb{F}_q^{n_t}),$$

$$\theta_i \xleftarrow{\mathrm{U}} \mathbb{F}_q, \vec{\eta}_i := (\eta_{i,1},\ldots,\eta_{i,z_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{z_t},$$

$$c_i := (\overbrace{s_i + \theta_i v_{i,1}, \theta_i v_{i,2},\ldots,\theta_i v_{i,n_t}}^{n_t}, \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1},\ldots,\eta_{i,z_t}}^{z_t})_{\mathbb{B}_t},$$

$$\text{si } \rho(i) = \neg(t, \vec{v}_i := (v_{i,1},\ldots,v_{i,n_t}) \in \mathbb{F}_q^{n_t}),$$

$$\vec{\eta}_i := (\eta_{i,1},\ldots,\eta_{i,z_t}) \xleftarrow{U} \mathbb{F}_q^{z_t},$$

$$c_i := (\overbrace{s_i\ (v_{i,1},\ldots,v_{i,n_t})}^{n_t},\ \overbrace{0^{u_t}}^{u_t},\ \overbrace{0^{w_t}}^{w_t},\ \overbrace{\eta_{i,1},\ldots,\eta_{i,z_t}}^{z_t})\mathbb{B}_t$$

En resumen, como lo hace la Fórmula 155, la Fórmula 156 significa que el coeficiente para el vector base de la base B_t se establece como se describe a continuación. Con el propósito de una representación simple, un vector base $b_{t,i}$ se especifica solamente por su parte i. Por ejemplo, un vector base 1 significa un vector base $b_{t,1}$. Los vectores base 1, ..., 3 significan vectores base $b_{t,1}$, ..., $b_{t,3}$, respectivamente.

Cuando ρ(i) es una tupla positiva (t, $v^{\rightarrow}_i$), $s_i + \theta_i v_{i,1}$ se establece como el coeficiente para el vector base 1. $\theta_i v_{i,2}$, …. $\theta_i v_{i,nt}$ (donde nt representa n_t) se establecen cada uno como el coeficiente para los vectores base 2, ..., n_t. 0 se establece como el coeficiente para los vectores base n_t+1, ..., $n_t+u_t+w_t$. $\eta_{i,1}$, …, $\eta_{i,zt}$ (donde zt representa z_t) se establecen cada uno como el coeficiente para los vectores base $\eta_t+u_t+w_t$+1, …, $\eta_t+u_t+w_t+z_t$.

Cuando ρ(i) es una tupla negativa ¬(t, $v^{\rightarrow}_i$), $s_i v_{i,1}$, …, $\theta_i v_{i,nt}$ (donde nt representa n_t) se establecen cada uno como el coeficiente para los vectores base 1, ..., n_t. $-s_i$ se establece como el coeficiente para los vectores base 2. 0 se establece como el coeficiente para los vectores base n_t+1, ..., $n_t+u_t+w_t$. $\eta_{i,1}$, …, $\eta_{i,zt}$ (donde zt representa z_t) se establecen cada uno como el coeficiente para los vectores base $n_t+u_t+w_t$+1, …, $n_t+u_t+w_t+z_t$.

Obsérvese que θ_i y $\eta_{i,i'}$(i' = 1, ..., z_t) son números aleatorios uniformes generados por la parte de generación de número aleatorio 233.

(S408: Paso de generación del elemento de firma L+1)

Con el dispositivo de procesamiento, la parte de generación del elemento de verificación L+1 336 genera un elemento de verificación c_{L+1}, que es un elemento de la clave de verificación, como se indica en la Fórmula 157.

[Fórmula 157]

$$c_{L+1} := (\overbrace{s_{L+1} - \theta_{L+1}\mathrm{H}^{\lambda,D}_{hk}(m\|\ \mathbb{S}), \theta_{L+1}}^{2},\ \overbrace{0^{u_{d+1}}}^{u_{d+1}},\ \overbrace{0^{w_{d+1}}}^{w_{d+1}},\ \overbrace{\eta_{L+1,1},\ldots,\eta_{L+1,z_{d+1}}}^{z_{d+1}})\mathbb{B}_{d+1}$$

En resumen, como lo hace la Fórmula 155, la Fórmula 157 significa que el coeficiente para el vector base de la base B_{d+1} se establece como se describe a continuación. Con el propósito de una representación simple, un vector base $b_{d+1,i}$ se especifica solamente por su parte i. Por ejemplo, un vector base 1 significa un vector base $b_{d+1,1}$. Los vectores base 1, ..., 3 significan vectores base $b_{d+1,1}$, ..., $b_{d+1,3}$, respectivamente.

$s_{L+1}-\theta_{L+1} \cdot H_{hk}^{\lambda,D}(m||S)$ se establece como el coeficiente para el vector base 1. θ_{L+1} se establece como el coeficiente para el vector base 2. 0 se establece como el coeficiente para los vectores base 2+1, ..., $2+u_{d+1}+w_{d+1}$. Los números aleatorios $\eta_{L+1,1}$, ..., $\eta_{L+1,zd+1}$ (donde zd+1 representa z_{d+1}) se configuran cada uno como el coeficiente para los vectores base $2+u_{d+1}+w_{d+1}$+1, ..., $2+u_{d+1}+w_{d+1}+z_{d+1}$.

(S409: Primer paso de operación de emparejamiento)

Con el dispositivo de procesamiento, la parte de operación de emparejamiento 340 conduce a una operación de emparejamiento $e(b_{0,1}, s^*_0)$.

Si el resultado del cálculo de la operación de emparejamiento $e(b_{0,1}, s^*_0)$ es el valor 1, la parte de operación de emparejamiento 340 emite el valor 0 que indica el fallo de la verificación de firma, y termina el proceso. Si el resultado del cálculo de la operación de emparejamiento $e(b_{0,1}, s^*_0)$ no es el valor 1, la parte de operación de emparejamiento 340 avanza el proceso a S410.

(S410: Segundo paso de operación de emparejamiento)

Con el dispositivo de procesamiento, la parte de operación de emparejamiento 340 dirige una operación de emparejamiento indicada en la Fórmula 158.

[Fórmula 158]

$$\prod_{i=0}^{L+1} e(c_i, s_i^*)$$

Si el resultado del cálculo de la operación de emparejamiento indicada en la Fórmula 158 es el valor 1, la parte de operación de emparejamiento 340 emite el valor 1 que indica el éxito de la verificación de firma; y, de otro modo, el valor 0 que indica el fallo de la verificación de firma.

Si el dato de firma σ es auténtico, como consecuencia del cálculo de la fórmula 158, se obtiene el valor 1, como se indica en la Fórmula 159.

[Fórmula 159]

$$\begin{aligned}
&\prod_{i=0}^{L+1} e(c_i, s_i^*) \\
&= e(c_0, k_0^*)^{\xi} \cdot \prod_{i \in I} e(c_i, k_t^*)^{\gamma_i \xi} \cdot \prod_{i=1}^{L} \prod_{t=1}^{n_t} e(c_i, b_{t,t}^*)^{y_{i,t}} \cdot e(c_{L+1}, s_{L+1}^*) \\
&= g_T^{\xi\delta(-s_0 - s_{L+1})} \cdot \prod_{i \in I} g_T^{\xi\delta\alpha_i s_i} \prod_{i=1}^{L} g_T^{\beta_i s_i} \cdot g_T^{\xi\delta s_{L+1}} \\
&= g_T^{\xi\delta(-s_0 - s_{L+1})} \cdot g_T^{\xi\delta s_0} \cdot g_T^{\xi\delta s_{L+1}} = 1.
\end{aligned}$$

En resumen, desde (S401) hasta (S410), el dispositivo de verificación 300 verifica los datos de firma σ ejecutando el algoritmo Ver indicado en la Fórmula 160.

[Fórmula 160]

$$\begin{aligned}
&\mathrm{Ver}(\mathrm{pk}, m, \mathbb{S} := (M, \rho), \vec{s}^*) \\
&\quad \vec{f} \xleftarrow{\mathrm{U}} \mathbb{F}_q^r, \ \vec{s}^{\mathrm{T}} := (s_1, \ldots, s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, \ s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}, \\
&\quad \vec{\eta}_0 \xleftarrow{\mathrm{U}} \mathbb{F}_q^{z_0}, \ \eta_{L+1} \xleftarrow{\mathrm{U}} \mathbb{F}_q^{z_{d+1}}, \ \theta_{L+1}, s_{L+1} \xleftarrow{\mathrm{U}} \mathbb{F}_q, \\
&\quad c_0 := (-s_0 - s_{L+1}, \overbrace{0^{u_0}}^{u_0}, \overbrace{0^{w_0}}^{w_0}, \overbrace{\eta_{0,1}, \ldots, \eta_{0,z_0}}^{z_0})_{\mathbb{B}_0}, \\
&\quad \text{para } 1 \le i \le L, \\
&\qquad \text{si } \rho(i) = (t, \vec{v}_i := (v_{i,1}, \ldots, v_{i,n_t}) \in \mathbb{F}_q^{n_t}), \\
&\qquad \text{si } s_i^* \notin \mathbb{V}_t \text{ devolver } 0, \\
&\qquad \text{de otro modo } \theta_i \xleftarrow{\mathrm{U}} \mathbb{F}_q, \vec{\eta}_i \xleftarrow{\mathrm{U}} \mathbb{F}_q^{z_t}, \\
&\qquad\quad c_i := (\overbrace{s_i + \theta_i v_{i,1}, \theta_i v_{i,2}, \ldots, \theta_i v_{i,n_t}}^{n_t}, \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1}, \ldots, \eta_{i,z_t}}^{z_t})_{\mathbb{B}_t},
\end{aligned}$$

si $\rho(i) = \neg(t, \vec{v}_i := (v_{i,1}, ..., v_{i,n_t}) \in \mathbb{F}_q^{n_t})$,

si $s_i^* \notin \mathbb{V}_t$ devolver 0,

de otro modo $\vec{\eta}_i \xleftarrow{U} \mathbb{F}_q^{z_t}$,

$$c_i := (s_i (v_{i,1}, ..., v_{i,n_t}), \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1}, ..., \eta_{i,z_t}}^{z_t})_{\mathbb{B}_t}$$

$$c_{L+1} := (\overbrace{s_{L+1} - \theta_{L+1} \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m \| \mathbb{S}), \theta_{L+1}}^{2}, \overbrace{0^{u_{d+1}}}^{u_{d+1}},$$

$$\overbrace{0^{w_{d+1}}}^{w_{d+1}}, \overbrace{\eta_{L+1,1}, ..., \eta_{L+1,z_{d+1}}}^{z_{d+1}})_{\mathbb{B}_{d+1}}$$

devolver 0 si $e(b_{0,1}, s_0^*) = 1$,

devolver 1 si $\prod_{i=0}^{L+1} e(c_i, s_i^*) = 1$, devolver 0 de otro modo.

Como se ha descrito anteriormente, el sistema de procesamiento de firmas 10 según la Realización 1 implementa el esquema de firmas basado en atributos que usa la estructura de acceso S construida usando el programa de extensión, el predicado de producto interno y la distribución secreta. En particular, como el sistema de procesamiento de firmas 10 según la Realización 1 usa un programa de extensión no monótono, implementa un esquema de firmas basado en atributos con un predicado no monótono.

El esquema de firmas basado en atributos implementado por el sistema de procesamiento de firmas 10 según la Realización 1 es altamente seguro y satisface los requisitos de privacidad. Ser altamente seguro significa que la firma no es probable que se falsifique por otros.

La operación de emparejamiento $e(b_{0,1}, s^*_0)$ en (S409) es comprobar que los datos de firma σ no son datos de firma generados sin usar el vector base $b^*_{0,1}$ que es secreto (que es la clave maestra sk).

La operación de emparejamiento $e(b_{0,1}, s^*_0)$ es una operación para comprobar si el elemento de firma s^*_0 incluye el vector base $b^*_{0,1}$, esto es, si se establece un valor distinto de 0 como el coeficiente para el vector base $b^*_{0,1}$. Si la operación de emparejamiento $e(b_{0,1}, s^*_0) = 1$, entonces en el elemento de firma s^*_0, 0 se establece como el coeficiente para el vector base $b^*_{0,1}$, lo que significa que los datos de firma σ son datos de firma generados sin usar el vector base $b^*_{0,1}$. Por lo tanto, en este caso, los datos de firma σ se determinan como falsos.

En la descripción anterior, las dimensiones u_t, w_t y z_t (t = 0, ..., d+1) se proporcionan para mejorar la seguridad. Por lo tanto, si u_t, w_t y z_t (t = 0, ..., d+1) se establecen cada uno a 0, las dimensiones u_t, w_t y z_t (t = 0, ..., d+1) no necesitan ser proporcionadas, aunque la seguridad se puede degradar.

En la descripción anterior, en (S101), $n_t+u_t+w_t+z_t$ se establece en N_t. Alternativamente, $n_t+u_t+w_t+z_t$ se puede sustituir por $n_t+ n_t+ n_t+1$, y 3 n_t +1 se puede establecer en N_t. Obsérvese que n_0 es 1 y que n_t (t = 1, ..., d+1) es 2.

En este caso, el algoritmo Setup indicado en la Fórmula 135 se reescribe como se indica en la Fórmula 161. Obsérvese que G_{ob} se escribe como se indica en la Fórmula 162.

[Fórmula 161]

$$\mathsf{Setup}(1^{\lambda}, \vec{n} := (d; 2,\ldots,2))$$

$$\mathsf{hk} \xleftarrow{\mathsf{R}} \mathsf{KH}_{\lambda},\ \ n_0 := 1,\ \ n_{d+1} := 2,$$

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

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

$$\hat{\mathbb{B}}_t := (b_{t,1}, b_{t,2}, b_{t,7}) \text{ para } t = 1,\ldots,d+1,$$

$$\hat{\mathbb{B}}_t^* := (b_{t,1}^*, b_{t,2}^*, b_{t,5}^*, b_{t,6}^*) \text{ para } t = 1,\ldots,d+1,$$

$$\mathsf{sk} := b_{0,1}^*,$$

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

devolver sk, pk.

[Fórmula 162]

$$\mathcal{G}_{\mathsf{ob}}(1^{\lambda}, \vec{n} := (d; 2,\ldots,2)):$$

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

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

$$n_0 := 1,\ n_{d+1} := 2,\ N_t := 3n_t + \text{para } t = 0,\ldots,d+1,$$

Para $t = 0,\ldots,d+1$,

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

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

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

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

$$g_T := e(g,g)^{\psi},\ \ \mathsf{param}_{\vec{n}}^{-} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,\ldots,d+1}, g_T)$$

devolver $(\mathsf{param}_{\vec{n}}^{-}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,\ldots,d+1})$.

El algoritmo KeyGen indicado en la Fórmula 140 se reescribe como se indica en Fórmula 163.

[Fórmula 163]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},\Gamma \coloneqq \{(t,x_t)\,|\,1 \le t \le d\})$$

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

$$\varphi_0,\varphi_{t,t},\varphi_{d+1,1,t},\varphi_{d+1,2,t} \xleftarrow{\cup} \mathbb{F}_q \text{ para } t=1,\ldots,d;\ t=1,2$$

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

$$k_t^* \coloneqq (\overbrace{\delta(1,x_t)}^{2},\overbrace{0,\ 0,}^{2}\overbrace{\quad\varphi_{t,1},\quad\varphi_{t,2},\quad}^{2}\overbrace{0}^{1})_{\mathbb{B}_t^*} \text{ para } (t,x_t)\in\Gamma,$$

$$k_{d+1,1}^* \coloneqq (\overbrace{\delta(1,\ 0),}^{2}\overbrace{0,\ 0,}^{2}\overbrace{\varphi_{d+1,1,1},\varphi_{d+1,1,2},}^{2}\overbrace{0}^{1})_{\mathbb{B}_{d+1}^*},$$

$$k_{d+1,2}^* \coloneqq (\overbrace{\delta(0,\ 1),}^{2}\overbrace{0,\ 0,}^{2}\overbrace{\varphi_{d+1,2,1},\varphi_{d+1,2,2},}^{2}\overbrace{0}^{1})_{\mathbb{B}_{d+1}^*},$$

$$T \coloneqq \{0,(d+1,1),(d+1,2)\} \cup \{t\,|\,1 \le t \le d,(t,x_t)\in\Gamma\},$$

devolver $\mathsf{sk}_\Gamma \coloneqq (\Gamma,\{k_t^*\}_{t\in T})$.

El algoritmo Sig indicado en la Fórmula 150 se reescribe como se indica en la Fórmula 164.

[Fórmula 164]

$\mathsf{Sig}(\mathsf{pk}, \mathsf{sk}_{\Gamma}, m, \mathbb{S} := (M, \rho))$

Si $\mathbb{S} := (M, \rho)$ acepta $\Gamma := \{(t, x_t)\}$,

entonces calcular I y $\{\alpha_i\}_{i \in I}$ de manera que

$$\sum_{i \in I} \alpha_i M_i := \vec{1}$$

e $I \subseteq \{i \in \{1, ..., L\} | [\rho(i) = (t, v_i) \wedge (t, x_t) \in \Gamma \wedge v_i = x_t]$

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

$$\xi \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times}, \quad (\beta_i) \xleftarrow{\mathsf{U}} \{(\beta_1, ..., \beta_L) \Big| \sum_{i=1}^{L} \beta_i M_i = \vec{0}\},$$

$$s_0^* := \xi k_0^* + r_0^*, \text{ donde } r_0^* \xleftarrow{\mathsf{U}} \mathsf{span}\langle b_{0,3}^* \rangle,$$

$$s_i^* := \gamma_i \cdot \xi k_t^* + \sum_{t=1}^{2} y_{i,t} \cdot b_{t,t}^* + r_i^*, \text{ para } 1 \leq i \leq L,$$

donde $r_i^* \xleftarrow{\mathsf{U}} \mathsf{span}\langle b_{t,5}^*, b_{t,6}^* \rangle$,

y $\gamma_i, \vec{y}_i := (y_{i,1}, y_{i,2})$ se definen como

si $i \in I \wedge \rho(i) = (t, v_i)$, $\quad \gamma_i := \alpha_i, \quad \vec{y}_i := \beta_i (1, v_i)$,

si $i \in I \wedge \rho(i) = \neg(t, v_i)$, $\gamma_i := \dfrac{\alpha_i}{v_i - x_t}$,

$$\vec{y}_i := \frac{\beta_i}{v_i - y_i}(1, y_i) \ (y_i \xleftarrow{\mathsf{U}} \mathbb{F}_q \setminus \{v_i\}),$$

si $i \notin I \wedge \rho(i) = (t, v_i)$, $\quad \gamma_i := 0, \quad \vec{y}_i := \beta_i (1, v_i)$,

si $i \notin I \wedge \rho(i) = \neg(t, v_i)$, $\gamma_i := 0$,

$$\vec{y}_i := \frac{\beta_i}{v_i - y_i}(1, y_i) \ (y_i \xleftarrow{\mathsf{U}} \mathbb{F}_q \setminus \{v_i\}),$$

$$s_{L+1}^* := \xi (k_{d+1,1}^* + \mathsf{H}_{\mathsf{hk}}^{\lambda, \mathsf{D}}(m \| \mathbb{S}) \cdot k_{d+1,2}^*) + r_{L+1}^*,$$

donde $r_{L+1}^* \xleftarrow{\mathsf{U}} \mathsf{span}\langle b_{d+1,5}^*, b_{d+1,6}^* \rangle$,

devolver $\vec{s}^* := (s_0^*, ..., s_{L+1}^*)$.

El algoritmo Ver indicado en la Fórmula 159 se reescribe como se indica en la Fórmula 165.

[Fórmula 165]

$$\mathrm{Ver}(\mathsf{pk}, m, \mathbb{S} := (M, \rho), \vec{s}^{*})$$

$$\vec{f} \xleftarrow{\mathrm{U}} \mathbb{F}_q^r, \quad \vec{s}^{\mathrm{T}} := (s_1, ..., s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, \quad s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}},$$

$$\eta_0, \eta_{L+1}, \theta_{L+1}, s_{L+1} \xleftarrow{\mathrm{U}} \mathbb{F}_q,$$

$$c_0 := (-s_0 - s_{L+1}, 0, 0, \eta_0)_{\mathbb{B}_0},$$

para $1 \le i \le L$,

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

devolver 0 si $s_i^{*} \notin \mathbb{V}_t$, de otro modo $\theta_i, \eta_i \xleftarrow{\mathrm{U}} \mathbb{F}_q$,

$$c_i := (\overbrace{s_i + \theta_i v_i, -\theta_i}^{2}, \overbrace{0,\ 0,}^{2} \overbrace{0,\ 0,}^{2} \overbrace{\eta_i}^{1})_{\mathbb{B}_t},$$

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

devolver 0 si $s_i^{*} \notin \mathbb{V}_t$, de otro modo $\eta_i \xleftarrow{\mathrm{U}} \mathbb{F}_q$,

$$c_i := (\overbrace{s_i(v_i, -1)}^{2}, \overbrace{0,\ 0,}^{2} \overbrace{0,\ 0,}^{2} \overbrace{\eta_i}^{1})_{\mathbb{B}_t},$$

$$c_{L+1} := (\overbrace{s_{L+1} - \theta_{L+1} \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m \| \mathbb{S}), \theta_{L+1}}^{2}, \overbrace{0,\ 0,}^{2} \overbrace{0,\ 0,}^{2} \overbrace{\eta_{L+1}}^{1})_{\mathbb{B}_{d+1}},$$

devolver 0 si $e(b_{0,1}, s_0^{*}) = 1$,

devolver 1 si $\prod_{i=0}^{L+1} e(c_i, s_i^{*}) = 1$, devolver 0 de otro modo.

El algoritmo Setup se puede ejecutar solamente una vez en la configuración del sistema de procesamiento de firmas 10, y no necesita ser ejecutado cada vez que ha de ser generada una clave de firma. En la descripción anterior, el algoritmo Setup y el algoritmo KeyGen se ejecutan por el dispositivo de generación de claves 100. Alternativamente, el algoritmo Setup y el algoritmo KeyGen se pueden ejecutar por diferentes dispositivos.

Realización 2.

Esta realización describe el “esquema de firmas basado en atributos multiautoridad descentralizada”.

En primer lugar, se explicará la noción de “multiautoridad descentralizada”.

En segundo lugar, se explicará el “esquema de firmas basado en atributos multiautoridad descentralizada” según esta realización. Inicialmente, se explicará la estructura básica del “esquema de firmas basado en atributos multiautoridad descentralizada”. Luego, se explicará la estructura básica del “sistema de procesamiento de firmas 10” que implementa el “esquema de firmas basado en atributos multiautoridad descentralizada”. Después de eso, se explicarán en detalle el “esquema de firmas basado en atributos multiautoridad descentralizada” y el “sistema de procesamiento de firmas 10”.

<1. La noción de multiautoridad descentralizada>

Inicialmente, se explicará la “multiautoridad”. Multiautoridad significa la presencia de una pluralidad de autoridades que generan la clave de firma.

En un sistema general de procesamiento de firmas, la seguridad de todo el sistema depende de una cierta parte (autoridad). Por ejemplo, en el sistema de procesamiento de firmas 10 descrito en la Realización 1, la seguridad de

todo el sistema depende del dispositivo de generación de claves 100 que genera la clave maestra sk. Si se viola la seguridad del dispositivo de generación de claves 100 o se filtra la clave maestra sk, todo el sistema de procesamiento de firmas 10 ya no funciona más.

Con el esquema de multiautoridad, no obstante, incluso si se viola la seguridad de alguna autoridad o se filtra la clave secreta (clave maestra) de alguna autoridad, solamente parte del sistema de procesamiento de firmas deja de funcionar, y la parte restante del sistema puede funcionar normalmente.

La Fig. 13 es un dibujo explicativo de la multiautoridad.

En la Fig. 13, una oficina pública gestiona atributos tales como la dirección, el número de teléfono y la edad. La policía gestiona atributos tales como el tipo de carnet de conducir. Una empresa A gestiona atributos tales como la posición en la empresa A y el departamento correspondiente en la empresa A. Una clave de firma 1 para indicar los atributos gestionados por la oficina pública se emite por la oficina pública. Una clave de firma 2 para indicar los atributos gestionados por la policía se emite por la policía. Una clave de firma 3 para indicar los atributos gestionados por la empresa A se emite por la empresa A.

El firmante que firma genera datos de firma usando una clave de firma formada juntando las claves de firma 1, 2 y 3 emitidas por las autoridades respectivas, tales como la oficina pública, la policía y la empresa A. Esto es, cuando se ve desde el firmante, una clave de firma formada juntando las claves de firma emitidas por las autoridades respectivas es la clave de firma única emitida por él mismo o por ella misma.

Por ejemplo, en un caso donde se filtra la clave maestra de la empresa A, aunque el sistema de procesamiento de firmas no funciona con respecto a los atributos en la empresa A, funciona con respecto a los atributos gestionados por las otras autoridades. Esto es, si se verifican los datos de firma, aunque no se puede confiar en los atributos gestionados por la empresa A, se pueden confiar en los otros atributos.

Como se ve a partir del ejemplo de Fig. 13, según la firma basada en atributos, es normal que esté presente una pluralidad de autoridades, y que cada autoridad gestione una cierta categoría (subespacio) o intervalo de definición en los atributos y emita (una parte de) una clave de firma con respecto al atributo del usuario en esta categoría.

Se explicará la noción de “descentralizada”. Ser descentralizada significa que cualquier parte puede servir como autoridad y emitir (una parte de) la clave de firma sin interactuar con las otras partes, y que cada usuario puede adquirir (una parte de) la clave de firma sin interactuar con las otras partes.

Por ejemplo, si existe una autoridad central, el sistema no está descentralizado. Una autoridad central es una autoridad superior a las otras autoridades. Si se viola la seguridad de la autoridad central, se violará la seguridad de todas las autoridades.

<2. Estructura de esquema de firmas basado en atributos multiautoridad descentralizada>

<2-1. Estructura básica de esquema de firmas basado en atributos multiautoridad descentralizada>

Un esquema de firmas basado en atributos multiautoridad descentralizada consta de cuatro algoritmos: GSetup, ASetup, AttrGen, Sig y Ver.

(GSetup)

Un algoritmo GSetup es un algoritmo aleatorizado que toma como entrada un parámetro de seguridad λ, y emite un parámetro público gparam.

(ASetup)

Un algoritmo ASetup es un algoritmo aleatorizado que toma como entrada el parámetro público gparam y la información de identificación de autoridad t, y emite una clave secreta de autoridad ask_t y un parámetro público de autoridad apk_t.

(AttrGen)

Un algoritmo AttrGen es un algoritmo aleatorizado que toma como entrada el parámetro público gparam, la información de identificación de autoridad t, la clave secreta de autoridad ask_t, la información de identificación de usuario gid, y atributo $\vec{x}_t =: (x_{t,i})\ (i = 1, ..., n_t) \in F_q$, y emite una clave de firma $usk_{gid,(t,xt)}$.

(Sig)

Un algoritmo Sig es un algoritmo aleatorizado que toma como entrada el parámetro público gparam, la clave de firma $usk_{gid,(t,xt)}$, un mensaje m, y una estructura de acceso S := (M, ρ), y emite datos de firma σ que incluyen: una firma $\vec{s}^*$; el mensaje m; y la estructura de acceso S.

(Ver)

Un algoritmo Ver es un algoritmo que toma como entrada los datos de firma σ, el parámetro público gparam, y el parámetro público de autoridad apk_t, y emite un valor booleano 1 (aceptar) o 0 (rechazar).

<2-2 Sistema de procesamiento de firmas 10>

Se describirá un sistema de procesamiento de firmas 10 que ejecuta los algoritmos del esquema de firmas basado en firmas multiautoridad descentralizada descrito anteriormente.

La Fig. 14 es un diagrama de configuración del sistema de procesamiento de firmas 10 que ejecuta los algoritmos del esquema de firmas basado en atributos multiautoridad descentralizado.

El sistema de procesamiento de firmas 10 está dotado con una pluralidad de dispositivos de generación de claves 100, un dispositivo de firmas 200 y un dispositivo de verificación 300.

Un (único) dispositivo de generación de claves 100 ejecuta el algoritmo GSetup tomando como entrada el parámetro de seguridad λ, y genera el parámetro público gparam. Este dispositivo de generación de claves 100 hace público el parámetro público generado gparam.

Cada dispositivo de generación de claves 100 ejecuta el algoritmo ASetup tomando como entrada el parámetro público gparam y la información de identificación de autoridad t asignada a este dispositivo de generación de claves 100, y genera la clave secreta de autoridad ask_t y el parámetro público de autoridad apk_t. Cada dispositivo de generación de claves 100 ejecuta el Algoritmo AttrGen tomando como entrada el parámetro público gparam, la información de identificación de autoridad t asignada a este dispositivo de generación de claves 100, la clave secreta de autoridad ask_t, la información de identificación de usuario gid y el atributo $x_t := (x_{t,i})$ $(i = 1, ..., n_t) \in Fq$, y genera la clave de firma $usk_{gid,(t,xt)}$ y la distribuye al dispositivo de firmas 200 en secreto.

El dispositivo de firmas 200 ejecuta el algoritmo Sig tomando como entrada el parámetro público gparam, la clave de firma $usk_{gid,(t,xt)}$, el mensaje m, y la estructura de acceso S := (M, ρ), y genera los datos de firma σ incluyendo: la firma $s^{\rightarrow *}$; el mensaje m; y la estructura de acceso S. El dispositivo de firmas 200 transmite los datos de firma σ generados al dispositivo de verificación 300.

El dispositivo de verificación 300 ejecuta el algoritmo Ver tomando como entrada los datos de firma σ, el parámetro público gparam y el parámetro público de autoridad apk_t, y emite un valor booleano 1 (aceptar) o 0 (rechazar).

<2-3. Esquema de firmas basado en atributos multiautoridad descentralizada y sistema de procesamiento de firmas 10 en detalle>

El esquema de firmas basado en atributos multiautoridad descentralizada, y la función y la operación del sistema de procesamiento de firmas 10 que ejecuta el esquema de firmas basado en atributos multiautoridad descentralizada se describirán con referencia a las Fig. 15 a 22.

La Fig. 15 es un diagrama de bloques de funciones que muestra la función de cada dispositivo de generación de claves 100. La Fig. 16 es un diagrama de bloques de funciones que muestra la función del dispositivo de firmas 200. La Fig. 17 es un diagrama de bloques de funciones que muestra la función del dispositivo de verificación 300.

Las Fig. 18 a 20 son diagramas de flujo que muestran la operación del dispositivo de generación de claves 100. Obsérvese que la Fig. 18 es un diagrama de flujo que muestra el proceso del algoritmo GSetup, que la Fig. 19 es un diagrama de flujo que muestra el proceso del algoritmo ASetup, y que la Fig. 20 es un diagrama de flujo que muestra el proceso del algoritmo AttrGen. La Fig. 21 es un diagrama de flujo que muestra la operación del dispositivo de firmas 200 y el proceso del algoritmo Sig. La Fig. 22 es un diagrama de flujo que muestra la operación del dispositivo de verificación 300 y el proceso del algoritmo Ver.

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

Como se muestra en la Fig. 15, el dispositivo de generación de claves 100 está dotado con una parte de generación de clave maestra 110, una parte de almacenamiento de clave maestra 120, una parte de entrada de información 130 (primera parte de entrada de información), una parte de generación de clave de firma 140 y una parte de distribución de clave 150 (parte de transmisión de clave de firma).

La parte de generación de clave maestra 110 está dotada con una parte de generación de parámetro global 111 y una parte de generación de clave secreta de autoridad 112. La parte de generación de clave de firma 140 está dotada con una parte de generación de número aleatorio 141 y una parte de generación de elemento de clave 145.

El proceso del algoritmo GSetup ejecutado por el dispositivo de generación de claves 100 se describirá primero con referencia a la Fig. 18. Como se ha descrito anteriormente, el algoritmo GSetup se puede ejecutar por un dispositivo de generación de claves 100 de entre la pluralidad de dispositivos de generación de claves 100.

(S501: Paso de entrada de parámetros de seguridad)

Con el dispositivo de entrada, la parte de generación de parámetros globales 111 toma como entrada un parámetro de seguridad λ (1^{λ}).

(S502: Paso de generación de grupo de emparejamiento bilineal)

Con el dispositivo de procesamiento, la parte de generación de parámetros globales 111 ejecuta el algoritmo G_{bpg} tomando como entrada el parámetro de seguridad λ (1^{λ}) introducido en S501, y genera aleatoriamente los valores de un parámetro $param_G := (q, G, G_T, g, e)$ del grupo de emparejamiento bilineal.

(S503: Paso de generación de parámetros)

Las funciones de comprobación aleatoria H_1 y H_2 se determinan como funciones de comprobación aleatoria indicadas en la Fórmula 166.

[Fórmula 166]

$$H_1 : \{0,1\}^* \rightarrow \mathbb{G},$$
$$H_2 : \{0,1\}^* \rightarrow \mathbb{F}_q$$

Con el dispositivo de procesamiento, la parte de generación de parámetros globales 111 genera los elementos G_0, G_1, G_2, G_3 y G_4 del parámetro global gparam indicados en la Fórmula 167.

[Fórmula 167]

$$G_0 := H_1(0^{\lambda}) \in \mathbb{G},$$
$$G_1 := H_1(1^{\lambda}) \in \mathbb{G},$$
$$G_2 := H_1(1, 0^{\lambda-1}) \in \mathbb{G},$$
$$G_3 := H_1(0, 1, 0^{\lambda-2}) \in \mathbb{G},$$
$$G_4 := H_1(1, 1, 0^{\lambda-2}) \in \mathbb{G}$$

La parte de generación de parámetros globales 111 también establece $g_t := e(G_0, G_1)$ y $g_4 := e(G_0, G_4)$.

(S504: Paso de almacenamiento de parámetros)

La parte de almacenamiento de clave maestra 120 almacena el $param_G$ generado en (S502), las funciones de comprobación aleatoria H_1 y H_2 establecidas en (S503) por la parte de generación de parámetros globales 111, los elementos generados G_0, G_1, G_3 y G_4, y los valores establecidos g_t y g_4, como un parámetro global gparam en el dispositivo de almacenamiento.

En resumen, desde (S501) hasta (S503), el dispositivo de generación de claves 100 genera el parámetro global gparam ejecutando el algoritmo GSetup indicado en la Fórmula 168. Entonces, en (S504), el dispositivo de generación de claves 100 almacena el parámetro global público gparam generado, en el dispositivo de almacenamiento.

Obsérvese que el parámetro global gparam se hace público a través de, por ejemplo, una red, de modo que otros dispositivos de generación de claves 100, el dispositivo de firmas 200 y el dispositivo de verificación 300 puedan adquirirlo.

[Fórmula 168]

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

$$H_1 : \{0,1\}^* \to \mathbb{G};\quad H_2 : \{0,1\}^* \to \mathbb{F}_q;$$

$$G_0 := H_1(0^{\lambda}) \in \mathbb{G},\quad G_1 := H_1(1^{\lambda}) \in \mathbb{G},\quad G_2 := H_1(1,0^{\lambda-1}) \in \mathbb{G},$$

$$G_3 := H_1(0,1,0^{\lambda-2}) \in \mathbb{G},\quad G_4 := H_1(1,1,0^{\lambda-2}) \in \mathbb{G},$$

$$g_T := e(G_0,G_1),\quad g_4 := e(G_0,G_4),$$

$$\text{devolver } \mathsf{gparam} := (\mathsf{param}_{\mathbb{G}},H_1,H_2,G_0,G_1,G_2,G_3,G_4,g_T,g_4).$$

El proceso del algoritmo ASetup ejecutado por el dispositivo de generación de claves 100 se describirá con referencia a la Fig. 19. Como se ha descrito anteriormente, el algoritmo ASetup se puede ejecutar por todos de la pluralidad de dispositivos de generación de claves 100, o solamente algunos de la pluralidad de dispositivos de generación de claves 100.

(S601: Paso de entrada de información)

Con el dispositivo de entrada, la parte de entrada de información 130 toma como entrada la información de identificación t asignada a sí misma (su dispositivo de generación de claves 100). Obsérvese que se asigna diferente información de identificación t a los respectivos dispositivos de generación de claves 100.

Por ejemplo, con el dispositivo de comunicación, la parte de entrada de información 130 adquiere el parámetro global gparam a través de la red. Si esta parte de entrada de información 130 pertenece al dispositivo de generación de claves 100 que ha generado el parámetro global gparam, la parte de entrada de información 130 puede leer el parámetro global gparam de la parte de generación de clave maestra 120.

(S602: paso de generación de espacio)

Con el dispositivo de procesamiento, la parte de generación de clave secreta de autoridad 112 ejecuta el algoritmo G_{dpvs} tomando como entrada el parámetro de seguridad λ (1^{λ}), $N_t = 2n_t + 2 + u_t + w_t + z_t$, y los valores de $pararm_G := (q, G, G_T, g, e)$, para generar los valores de un parámetro $param_{vt} := (q, V_t, G_T, A_t, e)$ de los espacios vectoriales de emparejamiento dual.

Obsérvese que n_t, u_t, w_t y z_t son cada uno un número entero de 1 o más.

(S603: Paso de generación de base U)

Con el dispositivo de procesamiento, la parte de generación de clave secreta de autoridad 112 genera una base U_l para cada número entero l = 1, ..., 4, como se indica en la Fórmula 169.

[Fórmula 169]

$$\mathbb{U}_l := (u_{l,1},\ldots,u_{l,N_t}),$$

$$\text{donde } u_{l,i} := (\overbrace{0,\ldots,0}^{i-1},G_l,\overbrace{0,\ldots,0}^{N_t-i})$$

$$\text{para } l = 0,\ldots,4;\ i = 1,\ldots,N_t$$

(S604: Paso de generación de transformación lineal)

Con el dispositivo de procesamiento, la parte de generación de clave secreta de autoridad 112 toma como entrada $n_t + u_t + w_t + z_t$, y F_q, y genera la transformación lineal $X_t := (\chi_{t,i,j})_{i,j}$ aleatoriamente, como se indica en la Fórmula 170.

[Fórmula 170]

$$X_t \xleftarrow{\cup} GL(N_t,\mathbb{F}_q)$$

(S605: Paso de generación de base B)

Con el dispositivo de procesamiento, la parte de generación de clave secreta de autoridad 112 genera una base B_t y una base B^*_t, como se indica en la Fórmula 171.

[Fórmula 171]

$$(\mathbb{B}_t, \mathbb{B}_t^*) := (X_t(\mathbb{U}_0), (X_t^{\mathrm{T}})^{-1}(\mathbb{U}_1))$$

La parte de generación de clave secreta de autoridad 112 determina π, π' y μ ∈ Fq, como valores que satisfacen $G_2 = \pi G_1$, $G_3 = \pi' G_1$, y $G_3 = \mu G_1$. Entonces, se establece la Fórmula 172.

[Fórmula 172]

$$(\pi \mathbb{B}_t^*, \pi' \mathbb{B}_t^*, \mu \mathbb{B}_t^*) = ((X_t^{\mathrm{T}})^{-1}(\mathbb{U}_2), (X_t^{\mathrm{T}})^{-1}(\mathbb{U}_3), (X_t^{\mathrm{T}})^{-1}(\mathbb{U}_4))$$

(S606: Paso de generación de base B^)

Con el dispositivo de procesamiento, la parte de generación de clave secreta de autoridad 112 genera una subbase $\hat{B}_t$ de la base B_t y una subbase $\hat{B}^*_t$ de la base B^* como se indica en la Fórmula 173.

[Fórmula 173]

$$\hat{\mathbb{B}}_t := (b_{t,1}, \ldots, b_{t,2n_t+2}, b_{t,2n_t+2+u_t+w_t+1}, \ldots, b_{t,2n_t+2+u_t+w_t+z_t}),$$

$$\hat{\mathbb{B}}_t^* := (\pi(b_{t,1}^*, \ldots, b_{t,n_t}^*), \pi'(b_{t,n_t+1}^*, \ldots, b_{t,2n_t}^*), \mu(b_{t,2n_t+1}^*, b_{t,2n_t+2}^*), b_{t,2n_t+2+u_t+1}, \ldots, b_{t,2n_t+2+u_t+w_t})$$

(S607: Paso de almacenamiento de clave maestra)

La parte de almacenamiento de clave maestra 120 almacena el parámetro $param_{vt}$ generado en (S602), y la subbase $\hat{B}_t$ y la subbase $\hat{B}^*_t$ generadas en (S606), en el dispositivo de almacenamiento como un parámetro público de autoridad apk_t. La parte de almacenamiento de clave maestra 120 también almacena la transformación lineal X_t generada en (S604), en el dispositivo de almacenamiento como la clave secreta de autoridad ask_t.

En resumen, desde (S601) hasta (S606), el dispositivo de generación de claves 100 genera el parámetro público de autoridad apk_t y la clave secreta de autoridad ask_t ejecutando el algoritmo ASetup indicado en la Fórmula 174. Entonces, en (S607), el dispositivo de generación de claves 100 almacena el parámetro público de autoridad apk_t y la clave secreta de autoridad ask_t generados, en el dispositivo de almacenamiento.

Obsérvese que el parámetro público de autoridad apk_t se hace público a través de, por ejemplo, una red, de modo que el dispositivo de firmas 200 y el dispositivo de verificación 300 puedan adquirirlo.

[Fórmula 174]

$$\mathrm{ASetup}(\mathrm{gparam}, t):$$

$$N_t := 2n_t + 2 + u_t + w_t + z_t,$$

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

$$\mathbb{U}_l := (u_{l,1}, \ldots, u_{l,N_t}),$$

$$\text{donde } u_{l,i} := (\overbrace{0, \ldots, 0}^{i-1}, G_l, \overbrace{0, \ldots, 0}^{N_t - i})$$

$$\text{para } l = 0, \ldots, 4;\ i = 1, \ldots, N_t,$$

$$X_t \xleftarrow{\cup} GL(N_t, \mathbb{F}_q),\ (\mathbb{B}_t, \mathbb{B}_t^*) := (X_t(\mathbb{U}_0), (X_t^{\mathrm{T}})^{-1}(\mathbb{U}_1)),$$

Permitamos que $\pi, \pi', \mu \in \mathbb{F}_q$ s.t. $G_2 = \pi G_1$, $G_3 = \pi' G_1$, $G_4 = \mu G_1$,

entonces $(\pi\mathbb{B}_t^*, \pi'\mathbb{B}_t^*, \mu\mathbb{B}_t^*) = ((X_t^{\mathrm{T}})^{-1}(\mathbb{U}_2), (X_t^{\mathrm{T}})^{-1}(\mathbb{U}_3), (X_t^{\mathrm{T}})^{-1}(\mathbb{U}_4))$,

$\hat{\mathbb{B}}_t := (b_{t,1}, \ldots, b_{t,2n_t+2}, b_{t,2n_t+2+u_t+w_t+1}, \ldots, b_{t,2n_t+2+u_t+w_t+z_t})$,

$\hat{\mathbb{B}}_t^* := (\pi(b_{t,1}^*, \ldots, b_{t,n_t}^*), \pi'(b_{t,n_t+1}^*, \ldots, b_{t,2n_t}^*), \mu(b_{t,2n_t+1}^*, b_{t,2n_t+2}^*),$

$b_{t,2n_t+2+u_t+1}, \ldots, b_{t,2n_t+2+u_t+w_t})$,

$\mathrm{ask}_t := X_t$, $\mathrm{apk}_t := (\mathrm{param}_{\mathbb{V}_t}, \hat{\mathbb{B}}_t, \hat{\mathbb{B}}_t^*)$,

devolver $(\mathrm{ask}_t, \mathrm{apk}_t)$.

El proceso del algoritmo AttrGen ejecutado por el dispositivo de generación de claves 100 se describirá con referencia a la Fig. 20. Obsérvese que, como se ha descrito anteriormente, el algoritmo AttrGen se ejecuta por el dispositivo de generación de claves 100, entre la pluralidad de dispositivos de generación de claves 100, que ha ejecutado el algoritmo ASetup.

(S701: Paso de entrada de información)

Con el dispositivo de entrada, la parte de entrada de información 130 toma como entrada la información de identificación t asignada a sí misma (su dispositivo de generación de claves 100), la información de identificación gid del usuario al que ha de ser emitida la clave de firma, y la información del atributo $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t).

Por ejemplo, con el dispositivo de comunicación, la parte de entrada de información 130 también adquiere el parámetro global gparam a través de la red. Si esta parte de entrada de información 130 pertenece al dispositivo de generación de claves 100 que ha generado el parámetro global gparam, la parte de entrada de información 130 puede leer el parámetro global gparam de la parte de almacenamiento de clave maestra 120.

La parte de entrada de información 130 también lee la clave secreta de autoridad ask_t desde la parte de almacenamiento de clave maestra 120.

(S702: Paso de generación de número aleatorio)

Con el dispositivo de procesamiento, la parte de generación de número aleatorio 141 genera un número aleatorio $\vec{\Phi}_{t,j}$ para la información de identificación t y cada número entero j = 1, 2, como se indica en la Fórmula 175.

[Fórmula 175]

$$\vec{\varphi}_{t,j} := (\varphi_{t,j,1}, \ldots, \varphi_{t,j,w_t}) \xleftarrow{\cup} \mathbb{F}_q^{w_t}, \text{ para } j = 1, 2,$$

(S703: Paso de generación de elemento de clave)

Supongamos que se establece la Fórmula 176.

[Fórmula 176]

$$G_{\mathrm{gid},j}(= \delta_j G_1) := H_1(j, \mathrm{gid}) \in \mathbb{G}$$

Con el dispositivo de procesamiento, la parte de generación de elemento de clave 145 genera un elemento de clave $k^*_{t,j}$, que es un elemento de la clave de firma $\mathrm{usk}_{\mathrm{gid},(t,\vec{x}t)}$, para la información de identificación t y cada número entero j = 1, 2, como se indica en la Fórmula 177.

[Fórmula 177]

$$k^*_{t,j} := (X_t^{\mathrm{T}})^{-1}((G_{\mathrm{gid},j} + G_1)\vec{x}_t, -\vec{x}_t G_{\mathrm{gid},j}, 0^{2+u_t}, \varphi_{t,j,1}G_1, \ldots, \varphi_{t,j,w_t}G_1, 0^{z_t})$$

$$\text{es decir, } k^*_{t,j} := (\overbrace{(\delta_j+1)(x_{t,1},\ldots,x_{t,n_t})}^{n_t}, \overbrace{-\delta_j(x_{t,1},\ldots,x_{t,n_t})}^{n_t}, \overbrace{0^2}^{2}, \overbrace{0^{u_t}}^{u_t},$$

$$\overbrace{\varphi_{t,j,1},\ldots,\varphi_{t,j,w_t}}^{w_t}, \overbrace{0^{z_t}}^{z_t})_{\mathbb{B}^*_t},$$

$$\text{para } j = 1,2$$

Como se describió anteriormente, para las bases B y B* indicadas en la Fórmula 113, se establece la Fórmula 114. Por lo tanto, la Fórmula 177 significa que el coeficiente para el vector base de una base B^*_t se establece como se describe a continuación. Con el propósito de una representación simple, un vector base $b^*_{t,i}$ se especifica solamente por su parte i. Por ejemplo, un vector base 1 significa un vector base $b^*_{t,1}$. Los vectores base 1, ..., 3 significan vectores base $b^*_{t,1}$, ..., $b^*_{t,3}$, respectivamente.

$(\delta_j+1)x_{t,1}$, ..., $(\delta_j+1)x_{t,nt}$ (donde nt representa n_t) se establecen como el coeficiente para los vectores base 1, ..., n_t. $-\delta_j x_{t,1}$, ..., $-\delta_j x_{t,nt}$ (donde nt representa n_t) se establecen cada uno como el coeficiente para los vectores base $n_t + 1$, ..., $2n_t$. 0 se establece como el coeficiente para los vectores base $2n_t+1$, ..., $2n_t+2+u_t$. Los números aleatorios $\Phi_{t,j,1}$, ..., $\Phi_{t,j,wt}$ (donde wt representa w_t) se establecen cada uno como el coeficiente para los vectores base $2n_t+2+u_t+1$, ..., $2n_t+2+u_t+w_t$. 0 se establece como el coeficiente para los vectores base $2n_t+2+u_t+w_t+1$, ..., $2n_t+2+u_t+w_t+z_t$.

(S704: Paso de distribución de clave)

Por ejemplo, con el dispositivo de comunicación, la parte de distribución de clave 150 distribuye la clave de firma $usk_{gid,(t,xt)}$, constituida como elementos por la información de identificación de usuario gid, la información de identificación t y la información de atributo $\vec{x}_t$, y el elemento de clave $k^*_{t,j}$, al dispositivo de firmas 200 en secreto a través de la red. Como cuestión de rutina, la clave de firma $usk_{gid,(t,xt)}$ se puede distribuir al dispositivo de firmas 200 por otro método.

En resumen, desde (S701) hasta (S703), el dispositivo de generación de claves 100 genera la clave de firma $usk_{gid,(t,xt)}$ ejecutando el algoritmo AttrGen indicado en la Fórmula 178. En (S704), el dispositivo de generación de claves 100 distribuye la clave de firma generada $usk_{gid,(t,xt)}$ al dispositivo de firmas 200.

[Fórmula 178]

$$\mathrm{AttrGen}(\mathrm{gparam}, t, \mathrm{ask}_t, \mathrm{gid}, \vec{x}_t := (x_{t,1},\ldots,x_{t,n_t}) \in \mathbb{F}_q):$$

$$G_{\mathrm{gid},j}(=\delta_j G_1) := H_1(j,\mathrm{gid}) \in \mathbb{G},$$

$$\vec{\varphi}_{t,j} \xleftarrow{\cup} \mathbb{F}_q^{w_t}, \text{ para } j = 1,2,$$

$$k^*_{t,j} := k^*_{t,j} := (X_t^{\mathrm{T}})^{-1}((G_{\mathrm{gid},j} + G_1)\vec{x}_t, -\vec{x}_t G_{\mathrm{gid},j},$$

$$0^{2+u_t}, \varphi_{t,j,1}G_1, \ldots, \varphi_{t,j,w_t}G_1, 0^{z_t})$$

$$\text{es decir, } k^*_{t,j} := (\overbrace{(\delta_j+1)(x_{t,1},\ldots,x_{t,n_t})}^{n_t}, \overbrace{-\delta_j(x_{t,1},\ldots,x_{t,n_t})}^{n_t}, \overbrace{0^2}^{2}, \overbrace{0^{u_t}}^{u_t},$$

$$\overbrace{\varphi_{t,j,1},\ldots,\varphi_{t,j,w_t}}^{w_t}, \overbrace{0^{z_t}}^{z_t})_{\mathbb{B}^*_t},$$

$$\text{para } j = 1,2,$$

$$\text{devolver } (\mathrm{usk}_{\mathrm{gid},(t,x_t)} := (\mathrm{gid}, (t,\vec{x}_t), \{k^*_{t,j}\}_{j=1,2})).$$

Se describirán la función y la operación del dispositivo de firmas 200.

Como se muestra en la Fig. 16, el dispositivo de firmas 200 está dotado con una parte de adquisición de clave de firma 210, una parte de entrada de información 220 (segunda parte de entrada de información), una parte de cálculo de programa de extensión 230, una parte de cálculo de coeficiente complementario 240, una parte de generación de datos de firma 250, y una parte de transmisión de datos de firma 260 (parte de salida de datos de firma).

La parte de entrada de información 220 está dotada con una parte de entrada de información de predicado 221 y una parte de entrada de mensaje 222. La parte de generación de datos de firma 250 está dotada con una parte de generación de número aleatorio 251 y una parte de generación de elemento de firma 255.

El proceso del algoritmo Sig ejecutado por el dispositivo de firmas 200 se describirá con referencia a la Fig. 21.

(S801: Paso de adquisición de clave de firma)

Por ejemplo, con el dispositivo de comunicación, la parte de adquisición de clave de firma 210 adquiere la clave de firma $usk_{gid,(t,xt)}$ generada por cada dispositivo de generación de claves 100, a través de la red. La parte de adquisición de clave de firma 210 también adquiere el parámetro público gparam generado por el dispositivo de generación de claves 100.

(S802: Paso de entrada de información)

Con el dispositivo de entrada, la parte de entrada de información de predicado 221 toma como entrada la estructura de acceso S := (M, ρ). La matriz M es una matriz de L filas x r columnas. L y r son cada uno un número entero de 1 o más.

Con el dispositivo de entrada, la parte de entrada de mensaje 220 toma como entrada el mensaje m a ser firmado.

La matriz M de la estructura de acceso S ha de ser establecida dependiendo de la condición del sistema a ser implementado.

(S803: Paso de cálculo de programa de extensión)

Con el dispositivo de procesamiento, la parte de cálculo de programa de extensión 230 comprueba si la estructura de acceso S introducida en (S802) acepta o no el conjunto Γ de la información de atributo $\vec{x}_t$ incluida en la clave de firma $usk_{gid,(t,xt)}$ adquirida en (S801).

El método de comprobación de si la estructura de acceso acepta o no el conjunto de atributos es el mismo que el descrito en “3. Concepto para implementar cifrado funcional” en la Realización 1.

Si la estructura de acceso S acepta el conjunto de atributos Γ (aceptar en S803), la parte de cálculo de programa de extensión 230 avanza el proceso a (S804). Si la estructura de acceso S rechaza el conjunto Γ de la información de atributo $\vec{x}_t$ (rechazar en S803), la parte de cálculo de programa de extensión 230 finaliza el proceso.

(S804: Paso de cálculo de coeficientes complementarios)

Con el dispositivo de procesamiento, la parte de cálculo de coeficiente complementario 430 calcula I y una constante (coeficiente complementario) α_i para cada número entero i incluido en I, cuyos I y α_i que satisfacen la Fórmula 179.

[Fórmula 179]

$$\vec{1} := \sum_{i \in I} \alpha_i M_i,$$

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

Obsérvese que M_i significa la fila de orden i de la matriz M.

(S805: Paso de generación de número aleatorio)

Con el dispositivo de procesamiento, la parte de generación de número aleatorio 251 genera los números aleatorios ξ_1 y ξ_2, y los números aleatorios β_i y β_i' (i = 1, ..., L), como se indica en la Fórmula 180.

[Fórmula 180]

$$\xi_1, \xi_2 \xleftarrow{\cup} \mathbb{F}_q,$$

$$(\beta_i), (\beta_i{}') \xleftarrow{\cup} \{(\beta_1, \ldots, \beta_L) \Big| \sum_{i=1}^{L} \beta_i M_i = \vec{0}\}$$

(S806: Paso de generación de elemento de firma)

Con el dispositivo de procesamiento, la parte de generación de elemento de firma 255 genera un elemento de firma s^*_i que es un elemento de los datos de firma σ, para cada número entero i = 1, ..., L, como se indica en la Fórmula 181.

[Fórmula 181]

$$\begin{aligned} s_i^* := {} & \gamma_i \cdot (\xi_1 k_{t,1}^* + (1-\xi_1) k_{t,2}^*) + \sum_{\iota=1}^{n_t} y_{i,\iota} (\pi b_{t,\iota}^*) \\ & + \sum_{\iota=1}^{n_t} y'_{i,\iota} (\pi' b_{t,n_t+\iota}^*) + \xi_2 ((\mu b_{t,2n_t+1}^*) + H_2(m, \mathbb{S})(\mu b_{t,2n_t+2}^*)) \\ & + r_i^*, \\ & \text{para } 1 \le i \le L \end{aligned}$$

Obsérvese que r^*_i se define por la Fórmula 182 (véanse las Fórmulas 110 hasta 112 y sus explicaciones).

[Fórmula 182]

$$r_i^* \xleftarrow{\cup} \text{span} \left\langle b_{t,2n_t+2+u_t+1}^*, \ldots, b_{t,2n_t+2+u_t+w_t}^* \right\rangle$$

Obsérvese que γ_i, $\vec{y}_i := (y_{i,i'})$ (i' = 1, ..., n_t), e $\vec{y'}_i := (y'_{i,i'})$ (i' = 1, ..., n_t) se definen por la Fórmula 183.

[Fórmula 183]

$$\begin{aligned} & \text{si } i \in I \wedge \rho(i) = (t, \vec{v}_i), \quad \gamma_i := \alpha_i, \\ & \qquad \vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\}, \\ & \qquad \vec{y}'_i \xleftarrow{\cup} \{\vec{y}'_i \,|\, \vec{y}'_i \cdot \vec{v}_i = 0 \wedge y'_{i,1} = \beta'_i\}, \\ & \text{si } i \in I \wedge \rho(i) = \neg(t, \vec{v}_i), \quad \gamma_i := \frac{\alpha_i}{\vec{v}_i \cdot \vec{x}_t}, \\ & \qquad \vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\}, \\ & \qquad \vec{y}'_i \xleftarrow{\cup} \{\vec{y}'_i \,|\, \vec{y}'_i \cdot \vec{v}_i = \beta'_i\}, \\ & \text{si } i \notin I \wedge \rho(i) = (t, \vec{v}_i), \quad \gamma_i := 0, \\ & \qquad \vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\}, \\ & \qquad \vec{y}'_i \xleftarrow{\cup} \{\vec{y}'_i \,|\, \vec{y}'_i \cdot \vec{v}_i = 0 \wedge y'_{i,1} = \beta'_i\}, \end{aligned}$$

$$\text{si } i \notin I \wedge \rho(i) = \neg(t, \vec{v}_i), \quad \gamma_i := 0,$$

$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

$$\vec{y}'_i \xleftarrow{U} \{\vec{y}'_i \,|\, \vec{y}'_i \cdot \vec{v}_i = \beta'_i\}$$

(S807: Paso de transmisión de datos)

Por ejemplo, con el dispositivo de comunicación, la parte de transmisión de datos de firma 260 transmite los datos de firma σ, incluyendo el elemento de firma s^*_i (i = 1, ..., L), el mensaje m, la estructura de acceso S := (M, ρ) y $g_0 := g_4^{\xi 2}$ (donde ξ2 representa ξ_2), al dispositivo de verificación 300 a través de la red. Como cuestión de rutina, los datos de firma σ se pueden transmitir al dispositivo de verificación 300 por otro método.

En resumen, desde (S801) hasta (S806), el dispositivo de firmas 200 genera los datos de firma σ ejecutando el algoritmo Sig indicado en la Fórmula 184. En (S807), el dispositivo de firmas 200 distribuye los datos de firma σ generados al dispositivo de verificación 300.

[Fórmula 184]

$$\text{Sig}(\text{gparam}, \{\text{apk}_t, \text{usk}_{\text{gid},(t,x_t)} := (\text{gid}, (t, \vec{x}_t), \{k^*_{t,j}\}_{j=1,2}\}, m, \mathbb{S} := (M, \rho))$$

Si $\mathbb{S} := (M, \rho)$ acepta $\Gamma := \{(t, \vec{x}_t) \in \text{usk}_{\text{gid},(t,x_t)}\}$,

entonces calcular I y $\{\alpha_i\}_{i \in I}$ de manera que

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

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

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

$$\xi_1, \xi_2 \xleftarrow{U} \mathbb{F}_q, \quad (\beta_i), (\beta_i') \xleftarrow{U} \{(\beta_1, ..., \beta_L) \,|\, \textstyle\sum_{i=1}^{L} \beta_i M_i = \vec{0}\},$$

$$g_0 := g_4^{\xi_2},$$

$$s^*_i := \gamma_i \cdot (\xi_1 k^*_{t,1} + (1 - \xi_1) k^*_{t,2}) + \textstyle\sum_{t=1}^{n_t} y_{i,t} (\pi b^*_{t,t})$$

$$+ \textstyle\sum_{t=1}^{n_t} y'_{i,t} (\pi' b^*_{t,n_t+t}) + \xi_2 ((\mu b^*_{t,2n_t+1}) + H_2(m, \mathbb{S})(\mu b^*_{t,2n_t+2}))$$

$$+ r^*_i, \quad \text{para } 1 \le i \le L,$$

donde $r^*_i \xleftarrow{U} \text{span}\left\langle b^*_{t,2n_t+2+u_t+1}, ..., b^*_{t,2n_t+2+u_t+w_t} \right\rangle$,

y $\gamma_i, \vec{y}_i := (y_{i,1}, ..., y_{i,n_t})$, $\vec{y}'_i := (y'_{i,1}, ..., y'_{i,n_t})$ se definen como

$$\text{si } i \in I \wedge \rho(i) = (t, \vec{v}_i), \quad \gamma_i := \alpha_i,$$

$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\}, \; \vec{y}'_i \xleftarrow{U} \{\vec{y}'_i \,|\, \vec{y}'_i \cdot \vec{v}_i = 0 \wedge y'_{i,1} = \beta'_i\},$$

$$\text{si } i \in I \wedge \rho(i) = \neg(t, \vec{v}_i), \quad \gamma_i := \frac{\alpha_i}{\vec{v}_i \cdot \vec{x}_t},$$

$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\}, \; \vec{y}'_i \xleftarrow{U} \{\vec{y}'_i \,|\, \vec{y}'_i \cdot \vec{v}_i = \beta'_i\},$$

$$\text{si } i \notin I \wedge \rho(i) = (t, \vec{v}_i), \quad \gamma_i := 0,$$

$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\}, \; \vec{y}'_i \xleftarrow{U} \{\vec{y}'_i \,|\, \vec{y}'_i \cdot \vec{v}_i = 0 \wedge y'_{i,1} = \beta'_i\},$$

$$\text{si } i \notin I \wedge \rho(i) = \neg(t, \vec{v}_i),\ \ \gamma_i := 0,$$
$$\vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \mid \vec{y}_i \cdot \vec{v}_i = \beta_i\},\ \vec{y}'_i \xleftarrow{\cup} \{\vec{y}'_i \mid \vec{y}'_i \cdot \vec{v}_i = \beta'_i\},$$
$$\text{devolver } \vec{s}^* := (s_0^*, ..., s, g_0).$$

Se describirán la función y la operación del dispositivo de verificación 300.

Como se muestra en la Fig. 17, el dispositivo de verificación 300 está dotado con una parte de adquisición de parámetro público 310, una parte de recepción de datos 320 (parte de adquisición de datos), una parte de generación de clave de verificación 330, y una parte de operación de emparejamiento 340.

La parte de generación de clave de verificación 330 está dotada con una parte de generación de número aleatorio 331, una parte de generación de vector f 332, una parte de generación de vector s 333 y una parte de generación de elemento de verificación 337.

El proceso del algoritmo Ver ejecutado por el dispositivo de verificación 300 se describirá con referencia a la Fig. 22.

(S901: Paso de adquisición de parámetro público)

Por ejemplo, con el dispositivo de comunicación, la parte de adquisición de parámetro público 310 adquiere el parámetro global gparam y el parámetro público de autoridad apk_t generado por cada dispositivo de generación de claves 100, a través de la red.

(S902: Paso de recepción de datos de firma)

Por ejemplo, con el dispositivo de comunicación, la parte de recepción de datos 320 recibe los datos de firma σ transmitidos por el dispositivo de firmas 200, a través de la red.

(S903: Paso de generación de vector f)

Con el dispositivo de procesamiento, la parte de generación de vector f 332 genera un vector $\vec{f}$ que tiene r partes de elementos, aleatoriamente como se indica en la Fórmula 185.

[Fórmula 185]

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

(S904: Paso de generación de vector s)

Con el dispositivo de procesamiento, la parte de generación de vector s 333 genera un vector $\vec{s}^{\mathrm{T}}$ como se indica en la Fórmula 186, en base a la matriz M (L filas x r columnas) de la estructura de acceso S incluida en los datos de firma σ recibidos en (S902), y el vector $\vec{f}$ generado en (S403) y que tiene r partes de elementos, x.

[Fórmula 186]

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

Con el dispositivo de procesamiento, la parte de generación de vector s 333 genera un valor s_0, en base al vector $\vec{f}$ generado en (S903), como se indica en la Fórmula 187. Obsérvese que $\vec{1}$ es un vector que tiene un valor 1 en todos sus elementos.

[Fórmula 187]

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

(S905: Paso de generación de vector f)

Con el dispositivo de procesamiento, la parte de generación de vector f 332 genera un vector $\vec{f}'$ que tiene r partes de elementos, aleatoriamente como se indica en la Fórmula 188.

[Fórmula 188]

$$\vec{f}' \xleftarrow{R} \mathbb{F}_q^r, \text{ s.t. } s_0 = \vec{1} \cdot \vec{f}'^{\mathrm{T}}$$

(S906: Paso de generación de vector s')

Con el dispositivo de procesamiento, la parte de generación de vector s 333 genera un vector $(s^{\rightarrow\prime})^{T}$, en base a la matriz M (L filas x r columnas) y el vector $f^{\rightarrow\prime}$ que tiene r partes de elementos, como se indica en la Fórmula 189.

[Fórmula 189]

$$\vec{s}'^{\mathrm{T}} := (s_1', \ldots, s_L')^{\mathrm{T}} := M \cdot \vec{f}'^{\mathrm{T}}$$

(S907: Paso de generación de número aleatorio)

Con el dispositivo de procesamiento, la parte de generación de número aleatorio 331 genera un número aleatorio $\sigma^{\rightarrow}$ y un valor σ_0, como se indica en la Fórmula 190.

[Fórmula 190]

$$\vec{\sigma} := (\sigma_1, \ldots, \sigma_L) \xleftarrow{U} \mathbb{F}_q^L,$$

$$\sigma_0 := \vec{1} \cdot \vec{\sigma}^{\mathrm{T}}$$

(S908: Paso de generación de elemento de verificación)

Con el dispositivo de procesamiento, la parte de generación de elemento de verificación 337 genera un elemento de verificación c_i, que es un elemento de la clave de verificación, para cada número entero i = 1, ..., L, como se indica en la Fórmula 191.

[Fórmula 191]

para $1 \le i \le L$,

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

$$\theta_i, \theta_i', \theta_i'' \xleftarrow{U} \mathbb{F}_q, \ \vec{\eta}_i := (\eta_{i,1}, \ldots, \eta_{i,z_t}) \xleftarrow{U} \mathbb{F}_q^{z_t}$$

$$c_i := (\overbrace{s_i + \theta_i v_{i,1}, \theta_i v_{i,2}, \ldots, \theta_i v_{i,n_t}}^{n_t}, \overbrace{s_i' + \theta_i' v_{i,1}, \theta_i' v_{i,2}, \ldots, \theta_i' v_{i,n_t}}^{n_t},$$

$$\overbrace{\sigma_i}^{2} - \overbrace{\theta_i'' H_2(m, \mathbb{S}), \theta_i''}^{2}, \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1}, \ldots, \eta_{i,z_t}}^{z_t})_{\mathbb{B}_t},$$

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

$$\theta_i'' \xleftarrow{U} \mathbb{F}_q, \ \vec{\eta}_i := (\eta_{i,1}, \ldots, \eta_{i,z_t}) \xleftarrow{U} \mathbb{F}_q^{z_t},$$

$$c_i := (\overbrace{s_i(v_{i,1}, \ldots, v_{i,n_t})}^{n_t}, \overbrace{s_i'(v_{i,1}, \ldots, v_{i,n_t})}^{n_t},$$

$$\overbrace{\sigma_i}^{2} - \overbrace{\theta_i'' H_2(m, \mathbb{S}), \theta_i''}^{2}, \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1}, \ldots, \eta_{i,z_t}}^{z_t})_{\mathbb{B}_t}$$

Como se ha descrito anteriormente, la Fórmula 114 se establece para las bases B y B* indicadas en la Fórmula 113. Por lo tanto, la Fórmula 191 significa que el coeficiente para el vector base de la base B_t se establece como se

describe a continuación. Con el propósito de una representación simple, un vector base $b_{t,i}$ se especifica solamente por su parte i. Por ejemplo, un vector base 1 significa un vector base $b_{t,1}$. Los vectores base 1, ..., 3 significan los vectores base $b_{t,1}$, ..., $b_{t,3}$, respectivamente.

Cuando ρ(i) es una tupla positiva (t, $\vec{v}_i$), $s_i+\theta_i v_{i,1}$ se establece como el coeficiente para el vector base 1. $\theta_i v_{i,2}$, ..., $\theta_i v_{i,nt}$ (donde nt representa n_t) se establecen cada uno como el coeficiente para los vectores base 2, ..., n_t. $s_i'+\theta_i' v_{i,1}$ se establece como el coeficiente para un vector base n_t+1. $\theta_i' v_{i,2}$, ..., $\theta_i' v_{i,nt}$ (donde nt representa n_t) se establecen cada uno como el coeficiente para los vectores bases n_t+2, ..., $2n_t$. $\sigma_i-\theta_i'' H_2(m, S)$ se establece como el coeficiente para un vector base $2n_t+1$. Obsérvese que $H_2(m, S)$ significa que el mensaje m y la estructura de acceso S se dan como entrada a la función de comprobación aleatoria H_2. Por ejemplo, $H_2(m||S)$ puede ser posible. θ_i''' se establece como el coeficiente para un vector base $2n_t+2$. 0 se establece como el coeficiente para los vectores base $2n_t+2+1$, …, $2n_t+2+u_t+w_t$. $\eta_{i,1}$, ..., $\eta_{i,zt}$ (donde zt representa z_t) se establecen cada uno como el coeficiente para los vectores base $2n_t+2+u_t+w_t+1$, …, $2n_t+2+u_t+w_t+z_t$.

Cuando ρ(i) es una tupla negativa ¬(t, $\vec{v}_i$), $s_i v_{i,1}$, …, $s_i v_{i,nt}$ (donde nt representa n_t) se establecen cada uno como el coeficiente para los vectores base 1, ..., n_t. $s_i' v_{i,1}$, …, $s_i' v_{i,nt}$ (donde nt representa n_t) se establecen cada uno como el coeficiente para los vectores base n_t+1, ..., $2n_t$. $\sigma_i-\theta_i'' H_2(m, S)$ se establece como el coeficiente para el vector base $2n_t+1$. θ_i'' se establece como el coeficiente para el vector base $2n_t+2$. 0 se establece como el coeficiente para los vectores base $2n_t+2+1$, ..., $2n_t+2+u_t+w_t$. $\eta_{i,1}$, …, $\eta_{i,zt}$ (donde zt representa z_t) se establecen cada uno como el coeficiente para los vectores base $2n_t+2+u_t+w_t+1$, ..., $2n_t+2+u_t+w_t+z_t$.

(S909: Paso de operación de emparejamiento)

Con el dispositivo de procesamiento, la parte de operación de emparejamiento 340 dirige una operación de emparejamiento indicada en la Fórmula 192.

[Fórmula 192]

$$\prod_{i=1}^{L} e(c_i, s_i^*)$$

Si el resultado del cálculo de la operación de emparejamiento indicada en la Fórmula 192 es un valor $g_T s^0 g_0^{\sigma 0}$ (donde s0 representa s_0 y σ0 representa σ_0), la parte de operación de emparejamiento 340 emite el valor 1 que indica el éxito de la verificación de firma; de otro modo, el valor 0 que indica el fallo de la verificación de firma.

Si los datos de firma σ son auténticos, como consecuencia del cálculo de la Fórmula 192, se obtiene el valor 1, como se indica en la Fórmula 193.

[Fórmula 193]

$$\begin{aligned}
&\prod_{i=1}^{L} e(c_i, s_i^*) \\
&= \prod_{i\in I} e(c_i, k_{t,1}^*)^{\gamma_i \xi_1} \cdot \prod_{i\in I} e(c_i, k_{t,2}^*)^{\gamma_i (1-\xi_1)} \cdot \\
&\quad \prod_{i=1}^{L} \prod_{\iota=1}^{n_t} e(c_i, b_{t,\iota}^*)^{\pi y_{i,\iota}} \cdot \\
&\quad \prod_{i=1}^{L} \prod_{\iota=1}^{n_t} e(c_i, b_{t,n_t+\iota}^*)^{\pi' y'_{i,\iota}} \cdot \\
&\quad \prod_{i=1}^{L} e(c_i, b_{t,2n_t+1}^*)^{\xi_2 \mu} \cdot \prod_{i=1}^{L} e(c_i, b_{t,2n_t+2}^*)^{\xi_2 \mu H_2(m,\mathbb{S})} \\
&= \prod_{i\in I} g_T^{\alpha_i s_i} \cdot \prod_{i=1}^{L} g_T^{\pi \beta_i s_i} \cdot \prod_{i=1}^{L} g_T^{\pi' \beta_i' s_i} \cdot \prod_{i=1}^{L} g_T^{\xi_2 \mu \sigma_i} \\
&= g_T^{s_0} \cdot 1 \cdot 1 \cdot g_4^{\xi_2 \sigma_0} \\
&= g_T^{s_0} \cdot g_0^{\sigma_0}
\end{aligned}$$

En resumen, desde (S901) hasta (S909), el dispositivo de verificación 300 verifica los datos de firma σ ejecutando el algoritmo Ver indicado en la Fórmula 194.

[Fórmula 194]

$$\mathrm{Ver}(g\mathrm{param}, \mathrm{apk}_t, m, \mathbb{S} := (M, \rho), \vec{s}^*)$$

$$\vec{f} \xleftarrow{\mathrm{U}} \mathbb{F}_q^r, \quad \vec{s}^{\mathrm{T}} := (s_1, \ldots, s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, \quad s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}},$$

$$\vec{f}' \xleftarrow{\mathrm{R}} \mathbb{F}_q^r, \quad \text{s.t. } s_0 = \vec{1} \cdot \vec{f}'^{\mathrm{T}}, \quad \vec{s}'^{\mathrm{T}} := (s_1', \ldots, s_L')^{\mathrm{T}} := M \cdot \vec{f}'^{\mathrm{T}},$$

$$\vec{\sigma} := (\sigma_1, \ldots, \sigma_L) \xleftarrow{\mathrm{U}} \mathbb{F}_q^L, \quad \sigma_0 := \vec{1} \cdot \vec{\sigma}^{\mathrm{T}},$$

para $1 \le i \le L$,

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

si $s_i^* \notin \mathbb{V}_t$ devolver 0,

de otro modo $\theta_i, \theta_i', \theta_i'' \xleftarrow{\mathrm{U}} \mathbb{F}_q, \quad \vec{\eta}_i \xleftarrow{\mathrm{U}} \mathbb{F}_q^{z_t}$

$$c_i := (\overbrace{s_i + \theta_i v_{i,1}, \theta_i v_{i,2}, \ldots, \theta_i v_{i,n_t}}^{n_t}, \overbrace{s_i' + \theta_i' v_{i,1}, \theta_i' v_{i,2}, \ldots, \theta_i' v_{i,n_t}}^{n_t},$$

$$\overbrace{\sigma_i - \theta_i'' H_2(m, \mathbb{S}), \theta_i''}^{2}, \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1}, \ldots, \eta_{i,z_t}}^{z_t})_{\mathbb{B}_t},$$

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

si $s_i^* \notin \mathbb{V}_t$ devolver 0,

de otro modo $\theta_i'' \xleftarrow{\mathrm{U}} \mathbb{F}_q, \quad \vec{\eta}_i \xleftarrow{\mathrm{U}} \mathbb{F}_q^{z_t}$

$$c_i := (\overbrace{s_i(v_{i,1}, \ldots, v_{i,n_t})}^{n_t}, \overbrace{s_i'(v_{i,1}, \ldots, v_{i,n_t})}^{n_t},$$

$$\overbrace{\sigma_i - \theta_i'' H_2(m, \mathbb{S}), \theta_i''}^{2}, \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1}, \ldots, \eta_{i,z_t}}^{z_t})_{\mathbb{B}_t}$$

devolver 1 si $\prod_{i=1}^{L} e(c_i, s_i^*) = g_T^{s_0} g_0^{\sigma_0}$, devolver 0 de otro modo.

Como se ha descrito anteriormente, el sistema de procesamiento de firmas 10 según la Realización 2 implementa el esquema de firmas basado en atributos multiautoridad en el que la pluralidad de dispositivos de generación de claves 100 genera claves de firma. En particular, el esquema de firmas implementado por el sistema de procesamiento de firmas 10 es un esquema de firmas basado en atributos multiautoridad descentralizada sin autoridad central.

Obsérvese que el sistema de procesamiento de firmas 10 según la Realización 2 implementa un esquema de firmas basado en atributos con un predicado no monótono, como lo hace el sistema de procesamiento de firmas 10 según lo hace la Realización 1.

El esquema de firmas basado en atributos implementado por el sistema de procesamiento de firmas 10 según la Realización 2 es altamente seguro y satisface los requisitos de privacidad.

En la descripción anterior, las dimensiones u_t, w_t y z_t (t = 0, ..., d) se proporcionan para mejorar la seguridad. Por lo tanto, si u_t, w_t y z_t (t = 1, ..., d) se establecen cada una en 0, las dimensiones u_t, w_t y z_t (t = 1, ..., d) no necesitan ser proporcionadas, aunque la seguridad se puede degradar.

En la descripción anterior, el número de dimensiones de cada una de la base B_t y la base B^*_t se establece en $2n_t+2+u_t+w_t+z_t$. Alternativamente, $2n_t+2+u_t+w_t+z_t$ se puede sustituir por 2+2+2+6+4+1, y el número de dimensiones de cada una de las bases B_t y la base B^*_t se puede establecer en 17.

En este caso, el algoritmo GSetup indicado en Fórmula 168 se reescribe como la Fórmula 195.

[Fórmula 195]

$$\begin{aligned}
&\mathsf{GSetup}(1^\lambda):\ \mathsf{param}_{\mathbb{G}} := (q,\mathbb{G},\mathbb{G}_T,g,e) \xleftarrow{R} \mathcal{G}_{\mathsf{bpg}}(1^\lambda),\\
&H_1 : \{0,1\}^* \to \mathbb{G};\quad H_2 : \{0,1\}^* \to \mathbb{F}_q;\\
&G_0 := H_1(0^\lambda) \in \mathbb{G},\quad G_1 := H_1(1^\lambda) \in \mathbb{G},\quad G_2 := H_1(1,0^{\lambda-1}) \in \mathbb{G},\\
&G_3 := H_1(0,1,0^{\lambda-2}) \in \mathbb{G},\quad G_4 := H_1(1,1,0^{\lambda-2}) \in \mathbb{G},\\
&g_T := e(G_0,G_1),\quad g_4 := e(G_0,G_4),\\
&\text{devolver } \mathsf{gparam} := (\mathsf{param}_{\mathbb{G}},H_1,H_2,G_0,G_1,G_2,G_3,G_4,g_T,g_4).
\end{aligned}$$

El algoritmo ASetup indicado en la Fórmula 174 se reescribe como Fórmula 196.

[Fórmula 196]

$$\begin{aligned}
&\mathsf{ASetup}(\mathsf{gparam},t):\\
&\mathsf{param}_{\mathbb{V}_t} := (q,\mathbb{V}_t,\mathbb{G}_T,\mathbb{A}_t,e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda,17,\mathsf{param}_{\mathbb{G}}),\\
&\mathbb{U}_l := (u_{l,1},...,u_{l,17}),\\
&\text{donde } u_{l,i} := (\overbrace{0,...,0}^{i-1},G_l,\overbrace{0,...,0}^{17-i}) \text{ para } l=0,...,4;\ i=1,...,17,\\
&X_t \xleftarrow{\mathsf{U}} GL(17,\mathbb{F}_q),\ (\mathbb{B}_t,\mathbb{B}^*_t) := (X_t(\mathbb{U}_0),(X_t^{\mathrm{T}})^{-1}(\mathbb{U}_1)),\\
&\text{Permitamos que } \pi,\pi',\mu \in \mathbb{F}_q \text{ s.t. } G_2=\pi G_1,\ G_3=\pi' G_1,\ G_4=\mu G_1,\\
&\text{entonces } (\pi\mathbb{B}^*_t,\pi'\mathbb{B}^*_t,\mu\mathbb{B}^*_t) = ((X_t^{\mathrm{T}})^{-1}(\mathbb{U}_2),(X_t^{\mathrm{T}})^{-1}(\mathbb{U}_3),(X_t^{\mathrm{T}})^{-1}(\mathbb{U}_4)),\\
&\hat{\mathbb{B}}_t := (b_{t,1},...,b_{t,6},b_{t,17}),\\
&\hat{\mathbb{B}}^*_t := (\pi b^*_{t,1},\pi b^*_{t,2},\pi' b^*_{t,3},\pi' b^*_{t,4},\mu b^*_{t,5},\mu b^*_{t,6},b^*_{t,13},...,b^*_{t,16}),\\
&\mathrm{ask}_t := X_t,\ \ \mathrm{apk}_t := (\mathsf{param}_{\mathbb{V}_t},\hat{\mathbb{B}}_t,\hat{\mathbb{B}}^*_t),\\
&\text{devolver } (\mathrm{ask}_t,\mathrm{apk}_t).
\end{aligned}$$

El algoritmo AttrGen indicado en la Fórmula 178 se reescribe como la Fórmula 197.

[Fórmula 197]

$$\mathsf{AttrGen}(\mathsf{gparam}, t, \mathrm{ask}_t, \mathrm{gid}, x_t \in \mathbb{F}_q):$$

$$G_{\mathrm{gid},j}\,(=\delta_j G_1) := H_1(j, \mathrm{gid}) \in \mathbb{G},$$

$$\vec{\varphi}_{t,j} := (\varphi_{t,j,1}, \ldots, \varphi_{t,j,4}) \xleftarrow{\cup} \mathbb{F}_q^4, \text{ para } j = 1,2,$$

$$k^*_{t,j} := (X_t^{\mathrm{T}})^{-1}((G_{\mathrm{gid},j} + G_1), x_t(G_{\mathrm{gid},j} + G_1), -G_{\mathrm{gid},j}, -x_t G_{\mathrm{gid},j},$$
$$0^8, \varphi_{t,j,1} G_1, \ldots, \varphi_{t,j,4} G_1, 0)$$

$$\text{es decir, } k^*_{t,j} := (\overbrace{(\delta_j + 1)(1, x_t)}^{2}, \overbrace{-\delta_j(1, x_t)}^{2}, \overbrace{0^2}^{2}, \overbrace{0^6}^{6}, \overbrace{\vec{\varphi}_{t,j}}^{4}, \overbrace{0}^{1})_{\mathbb{B}^*_t},$$

$$\text{para } j = 1,2,$$

$$\text{devolver } (\mathrm{usk}_{\mathrm{gid},(t,x_t)} := (\mathrm{gid}, (t, x_t), \{k^*_{t,j}\}_{j=1,2})).$$

El algoritmo Sig indicado en la Fórmula 184 se reescribe como la Fórmula 198.

[Fórmula 198]

$$\mathsf{Sig}(\mathsf{gparam}, \{\mathrm{apk}_t, \mathrm{usk}_{\mathrm{gid},(t,x_t)} := (\mathrm{gid}, (t, x_t), \{k^*_{t,j}\}_{j=1,2}\}, m, \mathbb{S} := (M, \rho))$$

$$\text{Si } \mathbb{S} := (M, \rho) \text{ acepta } \Gamma := \{(t, x_t) \in \mathrm{usk}_{\mathrm{gid},(t,x_t)}\},$$

$$\text{entonces calcular } I \text{ y } \{\alpha_i\}_{i \in I} \text{ de manera que}$$

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

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

$$\xi_1, \xi_2 \xleftarrow{\cup} \mathbb{F}_q, \quad (\beta_i), (\beta_i') \xleftarrow{\cup} \{(\beta_1, \ldots, \beta_L) \Big| \textstyle\sum_{i=1}^{L} \beta_i M_i = \vec{0}\},$$

$$g_0 := g_4^{\xi_2},$$

$$s_i^* := \gamma_i \cdot (\xi_1 k^*_{t,1} + (1 - \xi_1) k^*_{t,2}) + \textstyle\sum_{t=1}^{2} y_{i,t}(\pi b^*_{t,t})$$
$$+ \textstyle\sum_{t=3}^{4} y_{i,t}(\pi' b^*_{t,t}) + \xi_2((\mu b^*_{t,5}) + H_2(m, \mathbb{S})(\mu b^*_{t,6}))$$
$$+ r_i^*, \text{ para } 1 \le i \le L,$$

$$\text{donde } r_i^* \xleftarrow{\cup} \mathrm{span}\langle b^*_{t,13}, \ldots, b^*_{t,16} \rangle,$$

$$\text{y } \gamma_i, \vec{y}_i := (y_{i,1}, \ldots, y_{i,4}) \text{ se definen como}$$

$$\text{si } i \in I \wedge \rho(i) = (t, v_i), \quad \gamma_i := \alpha_i, \quad \vec{y}_i := (\beta_i(1, v_i), \beta_i'(1, v_i)),$$

$$\text{si } i \in I \wedge \rho(i) = \neg(t, v_i), \quad \gamma_i := \frac{\alpha_i}{v_i - x_t},$$

$$\vec{y}_i := \left(\frac{\beta_i}{v_i - y_i}(1, y_i), \frac{\beta_i'}{v_i - y_i'}(1, y_i')\right) \ (y_i, y_i' \xleftarrow{\cup} \mathbb{F}_q \setminus \{v_i\}),$$

$$\text{si } i \notin I \wedge \rho(i) = (t, v_i), \quad \gamma_i := 0, \quad \vec{y}_i := (\beta_i(1, v_i), \beta_i'(1, v_i)),$$

$$\text{si } i \notin I \wedge \rho(i) = \neg(t, v_i), \quad \gamma_i := 0,$$

$$\vec{y}_i := \left(\frac{\beta_i}{v_i - y_i}(1, y_i), \frac{\beta_i'}{v_i - y_i'}(1, y_i')\right) \ (y_i, y_i' \xleftarrow{U} \mathbb{F}_q \setminus \{v_i\}),$$

devolver $\vec{s}^* := (s_0^*, \ldots, s_L^*, g_0)$.

El algoritmo Ver indicado en la Fórmula 194 se reescribe como la Fórmula 199.

[Fórmula 199]

$$\mathrm{Ver}(gparam, apk_t, m, \mathbb{S} := (M, \rho), \vec{s}^*)$$

$$\vec{f} \xleftarrow{U} \mathbb{F}_q^r, \ \vec{s}^{\mathrm{T}} := (s_1, \ldots, s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, \ s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}},$$

$$\vec{f}' \xleftarrow{R} \mathbb{F}_q^r, \ \text{s.t. } s_0 = \vec{1} \cdot \vec{f}'^{\mathrm{T}}, \ \vec{s}'^{\mathrm{T}} := (s_1', \ldots, s_L')^{\mathrm{T}} := M \cdot \vec{f}'^{\mathrm{T}},$$

$$\vec{\sigma} := (\sigma_1, \ldots, \sigma_L) \xleftarrow{U} \mathbb{F}_q^L, \ \sigma_0 := \vec{1} \cdot \vec{\sigma}^{\mathrm{T}},$$

para $1 \le i \le L$,

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

devolver 0 si $s_i^* \notin \mathbb{V}_t$, de otro modo $\theta_i, \theta_i', \theta_i'', \eta_i \xleftarrow{U} \mathbb{F}_q$,

$$c_i := (\overbrace{s_i + \theta_i v_i}^{2}, \overbrace{-\theta_i}^{2}, \overbrace{s_i' + \theta_i' v_i}^{2}, \overbrace{-\theta_i'}^{2}, \overbrace{\sigma_i - \theta_i'' H_2(m, \mathbb{S})}^{2}, \theta_i'', \underbrace{0^6}_{6}, \underbrace{0^4}_{4}, \underbrace{\eta_i}_{1})_{\mathbb{B}_t},$$

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

devolver 0 si $s_i^* \notin \mathbb{V}_t$, de otro modo $\theta_i'' \xleftarrow{U} \mathbb{F}_q, \ \eta_i \xleftarrow{U} \mathbb{F}_q$,

$$c_i := (\overbrace{s_i(v_i, -1)}^{2}, \overbrace{s_i'(v_i, -1)}^{2}, \overbrace{\sigma_i - \theta_i'' H_2(m, \mathbb{S})}^{2}, \theta_i'', \underbrace{0^6}_{6}, \underbrace{0^4}_{4}, \underbrace{\eta_i}_{1})_{\mathbb{B}_t},$$

devolver 1 si $\prod_{i=1}^{L} e(c_i, s_i^*) = g_T^{s_0} g_0^{\sigma_0}$, devolver 0 de otro modo.

El algoritmo GSetup se puede ejecutar solamente una vez por un dispositivo de generación 100 en la configuración del sistema de procesamiento de firmas 10, y no necesita ser ejecutado todas las veces que ha de ser generada una clave de firma. Del mismo modo, el algoritmo ASetup se puede ejecutar solamente una vez por cada dispositivo de generación de claves 100 en la configuración del sistema de procesamiento de firmas 10, y no necesita ser ejecutado todas las veces que ha de ser generada una clave de firma.

En la explicación anterior, el algoritmo GSetup, el algoritmo ASetup y el algoritmo KeyGen se ejecutan por el dispositivo de generación de claves 100. Alternativamente, el algoritmo GSetup, el algoritmo ASetup y el algoritmo KeyGen se pueden ejecutar por diferentes dispositivos.

Realización 3.

En las realizaciones anteriores, se ha descrito el método de implementación del proceso de firma en los espacios vectoriales duales. En la Realización 3, se describirá un método de implementación de un proceso de firma en grupos aditivos duales.

Más específicamente, en las realizaciones anteriores, el proceso de firma se implementa en el grupo cíclico del orden primo q. Cuando un anillo R se expresa como se indica en la Fórmula 200 usando un número compuesto M, el proceso de firma descrito en las realizaciones anteriores también se puede aplicar a un módulo que tiene el anillo R como coeficiente.

[Fórmula 200]

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

donde

$\mathbb{Z}$: un número entero; y

M: un número compuesto

Cuando el esquema de firmas basado en atributos descrito en la Realización 1 se implementa en el grupo aditivo que tiene el anillo R como coeficiente, entonces resultan las Fórmulas 201 a 205.

[Fórmula 201]

$$\mathsf{Setup}(1^\lambda, \vec{n} := (d; n_t, u_t, w_t, z_t)\ (t = 0,...,d+1))$$

$$\mathsf{hk} \xleftarrow{R} \mathsf{KH}_\lambda,\ n_0 := 1,\ n_{d+1} := 2,$$

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

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

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

$$\mathsf{sk} := b_{0,1}^*,$$

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

$$b_{0,1+u_0+1}^*,...,b_{0,1+u_0+w_0}^*).$$

devolver sk, pk.

[Fórmula 202]

$$\mathcal{G}_{\mathsf{ob}}(1^{\lambda}, \vec{n} := (d; n_t, u_t, w_t, z_t)\ (t = 0,\ldots,d+1)):$$

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

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

$$N_t := n_t + u_t + w_t + z_t \text{ para } t = 0,\ldots,d+1,$$

Para $t = 0,\ldots,d+1$,

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

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

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

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

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

devolver $(\mathsf{param}^-_n, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d+1})$.

[Fórmula 203]

$$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \Gamma := \{(t, \vec{x}_t := (x_{t,1},\ldots,x_{t,n_t}) \in \mathbb{R}^{n_t}) \,|\, 1 \le t \le d\})$$

$$\delta \xleftarrow{\mathsf{U}} \mathbb{R}^{\times},$$

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

$$\vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{R}^{w_t} \text{ para } t = 1,\ldots,d,$$

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

$$k^*_0 := (\delta, \overbrace{0^{u_0}}^{u_0}, \overbrace{\varphi_{0,1},\ldots,\varphi_{0,w_0}}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbb{B}^*_0},$$

$$k^*_t := (\overbrace{\delta(x_{t,1},\ldots,x_{t,n_t})}^{n_t}, \overbrace{0^{u_t}}^{u_t}, \overbrace{\varphi_{t,1},\ldots,\varphi_{t,w_t}}^{w_t}, \overbrace{0^{z_t}}^{z_t})_{\mathbb{B}^*_t}$$

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

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

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

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

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

[Fórmula 204]

$\mathsf{Sig}(\mathsf{pk}, \mathsf{sk}_\Gamma, m, \mathbb{S} := (M,\rho))$

Si $\mathbb{S} := (M,\rho)$ acepta $\Gamma := \{(t,\vec{x}_t)\}$,

entonces calcular I y $\{\alpha_i\}_{i\in I}$ de manera que

$$\sum_{i\in I} \alpha_i M_i := \vec{1}$$

e $I \subseteq \{i \in \{1,\ldots,L\} \,|\, [\rho(i) = (t,\vec{v}_i) \wedge (t,\vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t = 0]$

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

$$\xi \xleftarrow{U} \mathbb{R}^\times,\quad (\beta_i) \xleftarrow{U} \{(\beta_1,\ldots,\beta_L) \,|\, \textstyle\sum_{i=1}^{L} \beta_i M_i = \vec{0}\},$$

$$s^*_0 := \xi k^*_0 + r^*_0,\quad \text{donde } r^*_0 \xleftarrow{U} \mathsf{span}\langle b^*_{0,1+u_0+1},\ldots,b^*_{0,1+u_0+w_0}\rangle,$$

$$s^*_i := \gamma_i \cdot \xi k^*_t + \textstyle\sum_{t=1}^{n_t} y_{i,t} \cdot b^*_{t,t} + r^*_i,\ \text{para } 1 \le i \le L,$$

donde $r^*_i \xleftarrow{U} \mathsf{span}\langle b^*_{t,n_t+u_t+1},\ldots,b^*_{t,n_t+u_t+w_t}\rangle$,

y $\gamma_i, \vec{y}_i := (y_{i,1},\ldots,y_{i,n_t})$ se definen como

si $i \in I \wedge \rho(i) = (t,v_i)$, $\gamma_i := \alpha_i$, $\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\}$,

si $i \in I \wedge \rho(i) = \neg(t,v_i)$, $\gamma_i := \dfrac{\alpha_i}{\vec{v}_i \cdot \vec{x}_t}$,

$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

si $i \notin I \wedge \rho(i) = (t,v_i)$, $\gamma_i := 0$, $\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\}$,

si $i \notin I \wedge \rho(i) = \neg(t,v_i)$, $\gamma_i := 0$,

$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

$$s^*_{L+1} := \xi(k^*_{d+1,1} + \mathsf{H}^{\lambda,D}_{\mathsf{hk}}(m \| \mathbb{S}) \cdot k^*_{d+1,2}) + r^*_{L+1},$$

donde $r^*_{L+1} \xleftarrow{U} \mathsf{span}\langle b^*_{d+1,2+u_{d+1}+1},\ldots,b^*_{d+1,2+u_{d+1}+w_{d+1}}\rangle$,

devolver $\vec{s}^* := (s^*_0,\ldots,s^*_{L+1})$.

[Fórmula 205]

$$\mathsf{Ver}(\mathsf{pk}, m, \mathbb{S} := (M, \rho), \vec{s}^{*})$$

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

$$\vec{\eta}_0 \xleftarrow{\cup} \mathbb{R}^{z_0},\ \eta_{L+1} \xleftarrow{\cup} \mathbb{R}^{z_{d+1}},\ \theta_{L+1}, s_{L+1} \xleftarrow{\cup} \mathbb{R},$$

$$c_0 := (-s_0 - s_{L+1}, \overbrace{0^{u_0}}^{u_0}, \overbrace{0^{w_0}}^{w_0}, \overbrace{\eta_{0,1}, \ldots, \eta_{0,z_0}}^{z_0})_{\mathbb{B}_0},$$

para $1 \le i \le L$,

si $\rho(i) = (t, \vec{v}_i := (v_{i,1}, \ldots, v_{i,n_t}) \in \mathbb{R}^{n_t})$,

si $s_i^{*} \notin \mathbb{V}_t$ devolver 0,

de otro modo $\theta_i \xleftarrow{\cup} \mathbb{R}, \vec{\eta}_i \xleftarrow{\cup} \mathbb{R}^{z_t}$,

$$c_i := (\overbrace{s_i + \theta_i v_{i,1}, \theta_i v_{i,2}, \ldots, \theta_i v_{i,n_t}}^{n_t}, \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1}, \ldots, \eta_{i,z_t}}^{z_t})_{\mathbb{B}_t},$$

si $\rho(i) = \neg(t, \vec{v}_i := (v_{i,1}, \ldots, v_{i,n_t}) \in \mathbb{R}^{n_t})$,

si $s_i^{*} \notin \mathbb{V}_t$ devolver 0,

de otro modo $\vec{\eta}_i \xleftarrow{\cup} \mathbb{R}^{z_t}$,

$$c_i := (\overbrace{s_i\ (v_{i,1}, \ldots, v_{i,n_t})}^{n_t}, \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1}, \ldots, \eta_{i,z_t}}^{z_t})_{\mathbb{B}_t}$$

$$c_{L+1} := (\overbrace{s_{L+1} - \theta_{L+1} \mathsf{H}_{\mathsf{hk}}^{\lambda,\mathsf{D}}(m \| \mathbb{S}), \theta_{L+1}}^{2}, \overbrace{0^{u_{d+1}}}^{u_{d+1}}, \overbrace{0^{w_{d+1}}}^{w_{d+1}}, \overbrace{\eta_{L+1,1}, \ldots, \eta_{L+1,z_{d+1}}}^{z_{d+1}})_{\mathbb{B}_{d+1}}$$

devolver 0 si $e(b_{0,1}, s_0^{*}) = 1$,

devolver 1 si $\prod_{i=0}^{L+1} e(c_i, s_i^{*}) = 1$, devolver 0 de otro modo.

Cuando el esquema de firmas basado en atributos multiautoridad descentralizada descrito en la Realización 2 se implementa en el grupo de aditivos que tiene el anillo R como coeficiente, entonces resultan las Fórmulas 206 a 210.

[Fórmula 206]

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

$$H_1 : \{0,1\}^{*} \to \mathbb{G};\quad H_2 : \{0,1\}^{*} \to \mathbb{R};$$

$$G_0 := H_1(0^{\lambda}) \in \mathbb{G},\quad G_1 := H_1(1^{\lambda}) \in \mathbb{G},\quad G_2 := H_1(1, 0^{\lambda-1}) \in \mathbb{G},$$

$G_3 := H_1(0,1,0^{\lambda-2}) \in \mathbb{G}, \quad G_4 := H_1(1,1,0^{\lambda-2}) \in \mathbb{G},$

$g_T := e(G_0, G_1), \quad g_4 := e(G_0, G_4),$

devolver $\mathsf{gparam} := (\mathsf{param}_{\mathbb{G}}, H_1, H_2, G_0, G_1, G_2, G_3, G_4, g_T, g_4).$

[Fórmula 207]

$\mathsf{ASetup}(\mathsf{gparam}, t):$

$N_t := 2n_t + 2 + u_t + w_t + z_t,$

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

$\mathbb{U}_l := (u_{l,1}, \ldots, u_{l,N_t}),$

donde $u_{l,i} := (\overbrace{0,\ldots,0}^{i-1}, G_l, \overbrace{0,\ldots,0}^{N_t-i})$

para $l = 0,\ldots,4;\ i = 1,\ldots,N_t,$

$X_t \xleftarrow{\cup} GL(N_t, \mathbb{R}), \quad (\mathbb{B}_t, \mathbb{B}_t^*) := (X_t(\mathbb{U}_0), (X_t^{\mathrm{T}})^{-1}(\mathbb{U}_1)),$

Permitamos que $\pi, \pi', \mu \in \mathbb{R}$ s.t. $G_2 = \pi G_1,\ G_3 = \pi' G_1,\ G_4 = \mu G_1,$

entonces $(\pi\mathbb{B}_t^*, \pi'\mathbb{B}_t^*, \mu\mathbb{B}_t^*) = ((X_t^{\mathrm{T}})^{-1}(\mathbb{U}_2), (X_t^{\mathrm{T}})^{-1}(\mathbb{U}_3), (X_t^{\mathrm{T}})^{-1}(\mathbb{U}_4)),$

$\hat{\mathbb{B}}_t := (b_{t,1}, \ldots, b_{t,2n_t+2}, b_{t,2n_t+2+u_t+w_t+1}, \ldots, b_{t,2n_t+2+u_t+w_t+z_t}),$

$\hat{\mathbb{B}}_t^* := (\pi(b_{t,1}^*, \ldots, b_{t,n_t}^*), \pi'(b_{t,n_t+1}^*, \ldots, b_{t,2n_t}^*), \mu(b_{t,2n_t+1}^*, b_{t,2n_t+2}^*),$

$b_{t,2n_t+2+u_t+1}, \ldots, b_{t,2n_t+2+u_t+w_t}),$

$\mathsf{ask}_t := X_t, \quad \mathsf{apk}_t := (\mathsf{param}_{\mathbb{V}_t}, \hat{\mathbb{B}}_t, \hat{\mathbb{B}}_t^*),$

devolver $(\mathsf{ask}_t, \mathsf{apk}_t).$

[Fórmula 208]

$\mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}, \vec{x}_t := (x_{t,1}, \ldots, x_{t,n_t}) \in \mathbb{R}):$

$G_{\mathsf{gid},j} (= \delta_j G_1) := H_1(j, \mathsf{gid}) \in \mathbb{G},$

$\vec{\varphi}_{t,j} \xleftarrow{\cup} \mathbb{R}^{w_t}, \ \text{para } j = 1,2,$

$k_{t,j}^* := k_{t,j}^* := (X_t^{\mathrm{T}})^{-1}((G_{\mathsf{gid},j} + G_1)\vec{x}_t, -\vec{x}_t G_{\mathsf{gid},j},$

$0^{2+u_t}, \varphi_{t,j,1} G_1, \ldots, \varphi_{t,j,w_t} G_1, 0^{z_t})$

es decir, $k_{t,j}^* := (\overbrace{(\delta_j + 1)(x_{t,1}, \ldots, x_{t,n_t})}^{n_t}, \overbrace{-\delta_j (x_{t,1}, \ldots, x_{t,n_t})}^{n_t}, \overbrace{0^2}^{2}, \overbrace{0^{u_t}}^{u_t},$

$$\underbrace{\varphi_{t,j,1},\ldots,\varphi_{t,j,w_t}}_{w_t},\underbrace{0^{z_t}}_{z_t})_{\mathbb{B}_t^*},$$

para $j=1,2,$

devolver $(\mathrm{usk}_{\mathrm{gid},(t,x_t)}:=(\mathrm{gid},(t,\vec{x}_t),\{k_{t,j}^*\}_{j=1,2})).$

[Fórmula 209]

$$\mathrm{Sig}(\mathrm{gparam},\{\mathrm{apk}_t,\mathrm{usk}_{\mathrm{gid},(t,x_t)}:=(\mathrm{gid},(t,\vec{x}_t),\{k_{t,j}^*\}_{j=1,2}\},m,\mathbb{S}:=(M,\rho))$$

Si $\mathbb{S}:=(M,\rho)$ acepta $\Gamma:=\{(t,\vec{x}_t)\in \mathrm{usk}_{\mathrm{gid},(t,x_t)}\},$

entonces calcular I y $\{\alpha_i\}_{i\in I}$ de manera que

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

e $I\subseteq\{i\in\{1,\ldots,L\}|\ [\rho(i)=(t,\vec{v}_i)\wedge(t,\vec{x}_t)\in\Gamma\wedge\vec{v}_i\cdot\vec{x}_t=0]$

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

$\xi_1,\xi_2\xleftarrow{\cup}\mathbb{R},\ \ (\beta_i),(\beta_i')\xleftarrow{\cup}\{(\beta_1,\ldots,\beta_L)\Big|\sum_{i=1}^{L}\beta_i M_i=\vec{0}\},$

$g_0:=g_4^{\xi_2},$

$s_i^*:=\gamma_i\cdot(\xi_1 k_{t,1}^*+(1-\xi_1)k_{t,2}^*)+\sum_{t=1}^{n_t}y_{i,t}(\pi b_{t,t}^*)$

$+\sum_{t=1}^{n_t}y'_{i,t}(\pi' b_{t,n_t+t}^*)+\xi_2((\mu b_{t,2n_t+1}^*)+H_2(m,\mathbb{S})(\mu b_{t,2n_t+2}^*))$

$+r_i^*,$ para $1\le i\le L,$

donde $r_i^*\xleftarrow{\cup}\mathrm{span}\left\langle b_{t,2n_t+2+u_t+1}^*,\ldots,b_{t,2n_t+2+u_t+w_t}^*\right\rangle,$

y $\gamma_i,\vec{y}_i:=(y_{i,1},\ldots,y_{i,n_t}),\ \vec{y}'_i:=(y'_{i,1},\ldots,y'_{i,n_t})$ se definen como

si $i\in I\wedge\rho(i)=(t,\vec{v}_i),\ \ \gamma_i:=\alpha_i,$

$\vec{y}_i\xleftarrow{\cup}\{\vec{y}_i\big|\vec{y}_i\cdot\vec{v}_i=0\wedge y_{i,1}=\beta_i\},\ \vec{y}'_i\xleftarrow{\cup}\{\vec{y}'_i\big|\vec{y}'_i\cdot\vec{v}_i=0\wedge y'_{i,1}=\beta'_i\},$

si $i\in I\wedge\rho(i)=\neg(t,\vec{v}_i),\ \ \gamma_i:=\dfrac{\alpha_i}{\vec{v}_i\cdot\vec{x}_t},$

$\vec{y}_i\xleftarrow{\cup}\{\vec{y}_i\big|\vec{y}_i\cdot\vec{v}_i=\beta_i\},\ \vec{y}'_i\xleftarrow{\cup}\{\vec{y}'_i\big|\vec{y}'_i\cdot\vec{v}_i=\beta'_i\},$

si $i\notin I\wedge\rho(i)=(t,\vec{v}_i),\ \ \gamma_i:=0,$

$\vec{y}_i\xleftarrow{\cup}\{\vec{y}_i\big|\vec{y}_i\cdot\vec{v}_i=0\wedge y_{i,1}=\beta_i\},\ \vec{y}'_i\xleftarrow{\cup}\{\vec{y}'_i\big|\vec{y}'_i\cdot\vec{v}_i=0\wedge y'_{i,1}=\beta'_i\},$

si $i\notin I\wedge\rho(i)=\neg(t,\vec{v}_i),\ \ \gamma_i:=0,$

$\vec{y}_i\xleftarrow{\cup}\{\vec{y}_i\big|\vec{y}_i\cdot\vec{v}_i=\beta_i\},\ \vec{y}'_i\xleftarrow{\cup}\{\vec{y}'_i\big|\vec{y}'_i\cdot\vec{v}_i=\beta'_i\},$

devolver $\vec{s}^*:=(s_0^*,\ldots,s,g_0).$

[Fórmula 210]

$$\mathrm{Ver}(gparam, \mathrm{apk}_t, m, \mathbb{S} := (M, \rho), \vec{s}^*)$$

$$\vec{f} \xleftarrow{U} \mathbb{R}^r, \quad \vec{s}^{\mathrm{T}} := (s_1, ..., s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, \quad s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}},$$

$$\vec{f}' \xleftarrow{R} \mathbb{R}^r, \text{ s.t. } s_0 = \vec{1} \cdot \vec{f}'^{\mathrm{T}}, \quad \vec{s}'^{\mathrm{T}} := (s_1', ..., s_L')^{\mathrm{T}} := M \cdot \vec{f}'^{\mathrm{T}},$$

$$\vec{\sigma} := (\sigma_1, ..., \sigma_L) \xleftarrow{U} \mathbb{R}^L, \quad \sigma_0 := \vec{1} \cdot \vec{\sigma}^{\mathrm{T}},$$

para $1 \le i \le L$,

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

si $s_i^* \notin \mathbb{V}_t$ devolver 0,

de otro modo $\theta_i, \theta_i', \theta_i'' \xleftarrow{U} \mathbb{R}, \ \vec{\eta}_i \xleftarrow{U} \mathbb{R}^{z_t}$

$$c_i := (\overbrace{s_i + \theta_i v_{i,1}, \theta_i v_{i,2}, ..., \theta_i v_{i,n_t}}^{n_t}, \overbrace{s_i' + \theta_i' v_{i,1}, \theta_i' v_{i,2}, ..., \theta_i' v_{i,n_t}}^{n_t},$$

$$\overbrace{\sigma_i - \theta_i'' H_2(m, \mathbb{S}), \theta_i''}^{2}, \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1}, ..., \eta_{i,z_t}}^{z_t})_{\mathbb{B}_t},$$

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

si $s_i^* \notin \mathbb{V}_t$ devolver 0,

de otro modo $\theta_i'' \xleftarrow{U} \mathbb{R}, \ \vec{\eta}_i \xleftarrow{U} \mathbb{R}^{z_t}$

$$c_i := (\overbrace{s_i(v_{i,1}, ..., v_{i,n_t})}^{n_t}, \overbrace{s_i'(v_{i,1}, ..., v_{i,n_t})}^{n_t},$$

$$\overbrace{\sigma_i - \theta_i'' H_2(m, \mathbb{S}), \theta_i''}^{2}, \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1}, ..., \eta_{i,z_t}}^{z_t})_{\mathbb{B}_t}$$

devolver 1 si $\prod_{i=1}^{L} e(c_i, s_i^*) = g_T^{s_0} g_0^{\sigma_0}$, devolver 0 de otro modo.

Desde el punto de vista de la prueba de seguridad, en las realizaciones anteriores, ρ(i) para cada número entero i = 1, ..., L puede estar limitado a una tupla positiva (t, $v^{\rightarrow}_i$) o una tupla negativa ¬(t, $v^{\rightarrow}_i$) para información de identificación t diferente.

En otras palabras, cuando ρ(i) = (t, $v^{\rightarrow}_i$) o ρ(i) = ¬(t, $v^{\rightarrow}_i$), permitamos que una función $\rho^{\sim}$ sea un mapa de {1, ..., L} → {1, ..., d} con el cual se establece $\rho^{\sim}(i) = t$. En este caso, $\rho^{\sim}$ puede estar limitado a inyección. Obsérvese que ρ(i) es ρ(i) en la estructura de acceso S := (M, ρ(i)) descrita anteriormente.

En la descripción anterior, el programa de extensión M^ acepta la secuencia de entrada δ si y sólo si la combinación lineal de las filas de la matriz M_δ obtenida a partir de la matriz ^ por la secuencia de entrada δ da $1^{\rightarrow}$. Alternativamente, el programa de extensión M^ puede aceptar la secuencia de entrada δ si y sólo si se obtiene otro vector $h^{\rightarrow}$ en lugar de $1^{\rightarrow}$.

En este caso, en el algoritmo KeyGen, $s_0 := h^{\rightarrow} \cdot f^{\rightarrow T}$ se puede establecer en lugar de $s_0 := 1^{\rightarrow} \cdot f^{\rightarrow T}$.

Se describirá la configuración de hardware del sistema de procesamiento de firmas 10 (el dispositivo de generación de claves 100, el dispositivo de firmas 200 y el dispositivo de verificación 300) en las realizaciones anteriores.

La Fig. 23 es un diagrama que muestra un ejemplo de la configuración de hardware de cada uno del dispositivo de generación de claves 100, el dispositivo de firmas 200 y el dispositivo 300 de verificación.

Como se muestra en la Fig. 23, cada uno del dispositivo de generación de claves 100, dispositivo de firmas 200 y dispositivo de verificación 300 incluye la CPU 911 (también conocida como Unidad Central de Procesamiento, dispositivo de procesamiento central, dispositivo de procesamiento, dispositivo de cálculo, microprocesador, microordenador o procesador) que ejecuta programas. La CPU 911 está conectada a la ROM 913, la RAM 914, un LCD 901 (Visualizador de Cristal Líquido), un teclado 902 (K/B), la placa de comunicación 915 y el 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 dispositivo de lectura/escritura de tarjeta de memoria. El dispositivo de disco magnético 920 está conectado a través de una interfaz predefinida de disco fijo.

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

El dispositivo de disco magnético 920, la ROM 913 o similar almacena un sistema operativo 921 (OS), un sistema de ventanas 922, programas 923 y archivos 924. La CPU 911, el sistema operativo 921 y el sistema de ventanas 922 ejecutan cada programa de los programas 923.

Los programas 923 almacenan software y programas que ejecutan las funciones descritas como la “parte de generación de clave maestra 110”, la “parte de almacenamiento de clave maestra 120”, la “parte de entrada de información 130”, la “parte de generación de clave de firma 140”, la “parte de distribución de clave 150”, la “parte de adquisición de clave de firma 210”, la “parte de entrada de información 220”, la “parte de cálculo de programa de extensión 230”, la “parte de cálculo de coeficiente complementario 240”, la “parte de generación de datos de firma 250”, la “parte de transmisión de datos de firma 260”, la “parte de adquisición de parámetros públicos 310”, la “parte de recepción de datos 320”, la “parte de generación de clave de verificación 330”, la “parte de operación de emparejamiento 340”, y similares en la descripción anterior. Los programas 923 almacenan otros programas también. Los programas se leen y se ejecutan por la CPU 911.

Los archivos 924 almacenan información, datos, valores de señal, valores de variables y parámetros tales como el “parámetro público”, la “clave maestra”, los “datos de firma σ”, la “clave de firma”, la “estructura de acceso S”, la “información de atributos”, el “conjunto de atributos Γ”, el “mensaje m” y similares de la explicación anterior, como los elementos de un “archivo” y una “base de datos”. El “archivo” y la “base de datos” se almacenan en un medio de grabación tal como un disco o memoria. La información, los datos, los valores de señal, los valores de variables y los parámetros almacenados en el medio de grabación tal como el disco o la memoria se leen de la memoria principal o la memoria caché por la CPU 911 a través de un circuito de lectura/escritura, y se usan para las operaciones de la CPU 911 tales como extracción, examen, búsqueda, comparación, computación, cálculo, proceso, salida, impresión y visualización. La información, los datos, los valores de señal, los valores de variables y los parámetros se almacenan temporalmente en la memoria principal, la memoria caché o el almacenador temporal durante las operaciones de la CPU 1911, que incluyen extracción, examen, búsqueda, comparación, computación, cálculo, proceso , salida, impresión y visualización.

Las flechas de los diagramas de flujo en la explicación anterior indican principalmente la entrada/salida de datos y señales. Los datos y los valores de señal se almacenan en la memoria de la RAM 914, el medio de grabación, tal como un disco óptico, o en un chip de IC. Los datos y las 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 un “paso”, “procedimiento” o “proceso”. El “dispositivo” puede ser un “circuito”, “equipo”, “medio” o “función”; o un “paso”, “procedimiento” o “proceso”. El “proceso” puede ser un “paso”. Esto es, la “parte” se puede implementar como microprograma almacenado en la ROM 913. Alternativamente, la “parte” se puede poner en práctica solamente como software, solamente como hardware tal como un elemento, un dispositivo, un sustrato, o una línea de cableado; como una combinación de software y hardware; o además como una combinación de software, hardware y microprograma. El microprograma y el software se almacenan, como programas, en el medio de grabación tal como la ROM 913. El programa se lee por la CPU 911 y se ejecuta por la CPU 911. Esto es, el programa hace que el ordenador funcione como una “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 signos de referencia

10: sistema de procesamiento de firmas; 100: dispositivo de generación de claves; 110: parte de generación de clave maestra; 111: parte de generación de parámetro global; 112: parte de generación de clave secreta de autoridad; 120: parte de almacenamiento de clave maestra; 130: parte de entrada de información; 140: parte de

generación de clave de firma; 141: parte de generación de número aleatorio; 142: parte de generación del elemento de clave 0; 143: parte de generación del elemento de clave t; 144: parte de generación del elemento de clave d+1; 145: parte de generación de elemento de clave; 150: parte de distribución de clave; 200: dispositivo de firmas; 210: parte de adquisición de clave de firma; 220: parte de entrada de información; 221: parte de entrada de información de predicado; 222: parte de entrada de mensaje; 230: parte de cálculo del programa de extensión; 240: parte de cálculo de coeficiente complementario; 250: parte de generación de datos de firma; 251: parte de generación de número aleatorio; 252: parte de generación del elemento de firma 0; 253: parte de generación del elemento de firma i; 254: parte de generación del elemento de firma L+1; 255: parte de generación de elemento de firma; 260: parte de transmisión de datos de firma; 300: dispositivo de verificación; 310: parte de adquisición de parámetro público; 320: parte de recepción de datos; 330: parte de generación de clave de verificación; 331: parte de generación de número aleatorio; 332: parte de generación de vector f; 333: parte de generación de vector s; 334: parte de generación del elemento de verificación 0; 335: parte de generación del elemento de verificación i; 336: parte de generación del elemento de verificación L+1; 337: parte de generación de elemento de verificación; 340: parte de operación de emparejamiento.

REIVINDICACIONES

1. Un sistema de procesamiento de firmas (10) que comprende un dispositivo de generación de claves (100), un dispositivo de firmas (200) y un dispositivo de verificación (300), y que sirve para ejecutar un proceso de firma usando una base B_t y una base B^*_t para cada número entero t = 0, ..., d+1 (d es un número entero de 1 o más),

en donde el dispositivo de generación de claves incluye

una primera parte de entrada de información (130) que toma como entrada un conjunto de atributos Γ que incluye información de identificación t e información de atributo $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t donde n_t es un número entero de 1 o más) para al menos un número entero t = 1, ..., d,

una parte de generación del elemento de clave 0 (142) que genera un elemento de clave k^*_0 donde un valor δ predeterminado se establece como coeficiente para un vector base $b^*_{0,1}$ de una base B^*_0,

una parte de generación del elemento de clave t (143) que genera un elemento de clave k^*_t donde $\delta x_{t,i}$ (i = 1, ..., n_t) obtenido multiplicando la información de atributo $\vec{x}_t$ por el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{t,i}$ (i = 1, ..., n_t) de la base B^*_t, que concierne a cada información de identificación t incluida en el conjunto de atributos Γ introducido por la primera parte de entrada de información,

una parte de generación del elemento de clave d+1 (144) que genera un elemento de clave $k^*_{d+1,1}$ donde el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{d+1,1}$ de una base B^*_{d+1}, y un elemento de clave $k^*_{d+1,2}$ donde el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{d+1,2}$ de la base B^*_{d+1}, y

una parte de transmisión de clave de firma (150) que transmite, al dispositivo de firma, una clave de firma sk_Γ que incluye: el elemento de clave k^*_0 generado por la parte de generación del elemento de clave 0; el elemento de clave k^*_t generado por la parte de generación del elemento de clave t que concierne a cada información de identificación t incluida en el conjunto de atributos Γ; el elemento de clave $k^*_{d+1,1}$ y el elemento de clave $k^*_{d+1,2}$ que se generan por la parte de generación del elemento de clave d+1; y el conjunto de atributos Γ,

en donde el dispositivo de firmas incluye

una segunda parte de entrada de información (220) que toma como entrada una variable ρ(i) para cada número entero i = 1, …, L (L es un número entero de 1 o más), cuya variable ρ(i) es cualquiera de una tupla positiva $(t, \vec{v}_i)$ y una tupla negativa $\neg(t, \vec{v}_i)$ de la información de identificación t (t es cualquier número entero de t = 1, ..., d) y la información de atributo $\vec{v}_i := (v_{i,i'})$ (i' = 1, ..., n_t); una matriz M predeterminada que tiene L filas y r columnas (r es un número entero de 1 o más); y un mensaje m,

una parte de adquisición de clave de firma (210) que adquiere la clave de firma sk_Γ transmitida por la parte de transmisión de clave de firma,

una parte de cálculo de coeficiente complementario (240) que, en base a la variable ρ(i) introducida por la segunda parte de entrada de información y el conjunto de atributos Γ incluido en la clave de firma sk_Γ adquirida por la parte de adquisición de clave de firma, especifica, entre los números enteros i = 1, ..., L, un conjunto I de un número entero i para el cual la variable ρ(i) es una tupla positiva $(t, \vec{v}_i)$ y con el cual un producto interno de $\vec{v}_i$ de la tupla positiva y $\vec{x}_t$ incluido en el conjunto de atributos Γ indicado por la información de identificación t de la tupla positiva llega a ser 0, y un número entero i para el cual la variable ρ(i) es una tupla negativa $\neg(t, \vec{v}_i)$ y con el cual un producto interno de $\vec{v}_i$ de la tupla negativa y $\vec{x}_t$ incluido en el conjunto de atributos Γ indicado por la información de identificación t de la tupla negativa no llega a ser 0; y calcula, concerniente a i incluido en el conjunto I especificado, un coeficiente complementario α_i con el cual un total de $\alpha_i M_i$ en base a M_i que es un elemento en una fila de orden i de la matriz M introducida por la segunda parte de entrada de información llega a ser un vector $\vec{h}$ predeterminado,

una parte de generación del elemento de firma 0 (252) que genera un elemento de firma s^*_0 que incluye el elemento de clave k^*_0 incluido en la clave de firma sk_Γ,

una parte de generación del elemento de firma i (253) que genera, para cada número entero i = 1 ..., L, un elemento de firma s^*_i que incluye $\gamma_i k^*_t$ obtenido multiplicando el elemento de clave k^*_t incluido en la clave de firma sk_Γ por un valor γ_i, estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i$ cuando el número entero i se incluye en el conjunto I especificado por la parte de cálculo de coeficiente complementario y la variable ρ(i) es una tupla positiva $(t, \vec{v}_i)$; estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i/(\vec{v}_i \cdot \vec{x}_t)$ cuando el número entero i está incluido en el conjunto I y la variable ρ(i) es una tupla negativa $\neg(t, \vec{v}_i)$; y estableciendo el valor γ_i para satisfacer $\gamma_i := 0$ cuando el número entero i no está incluido en el conjunto I,

una parte de generación del elemento de firma L+1 (254) que genera un elemento de firma s^*_{L+1} que incluye una suma del elemento de clave $k^*_{d+1,1}$ incluido en la clave de firma sk_Γ y $m' \cdot k^*_{d+1,2}$ obtenido multiplicando el elemento de clave $k^*_{d+1,2}$ por un valor m' generado usando el mensaje m, y

una parte de transmisión de datos de firma (260) que transmite, al dispositivo de verificación, datos de firma σ que incluyen: el elemento de firma s^*_0 generado por la parte de generación del elemento de firma 0; el elemento de firma s^*_i generado para cada número entero i = 1, ..., L por la parte de generación del elemento de firma i; el elemento de firma s^*_{L+1} generado por la parte de generación del elemento de firma L+1; el mensaje m; la variable ρ(i); y la matriz M, y

en donde el dispositivo de verificación incluye

una parte de adquisición de datos (320) que adquiere los datos de firma σ transmitidos por la parte de transmisión de datos de firma,

una parte de generación del elemento de verificación 0 (334) que genera un elemento de verificación c_0 estableciendo, como coeficiente para un vector base $b_{0,1}$ de una base B_0, $-s_0 - s_{L+1}$ calculado a partir de un valor $s_0 := h^{\rightarrow \cdot} \cdot f^{\rightarrow}$ y un valor predeterminado s_{L+1}, el valor $s_0 := h^{\rightarrow \cdot} \cdot f^{\rightarrow}$ que se genera usando un vector $f^{\rightarrow}$ que tiene r partes de elementos, y el vector $h^{\rightarrow}$,

una parte de generación del elemento de verificación i (335) que, para cada número entero i = 1, ..., L y usando un vector de columna $s^{\rightarrow T} := (s_1, ..., s_L)^T := M \cdot f^{\rightarrow T}$ generado en base al vector $f^{\rightarrow}$ y la matriz M que se incluye en los datos de firma σ adquiridos por la parte de adquisición de datos, y un número predeterminado θ_i para cada número entero i = 1, ..., L, genera un elemento de verificación c_i, cuando la variable ρ(i) es una tupla positiva (t, $v^{\rightarrow}_i$), estableciendo $s_i + \theta_i v_{i,1}$ como coeficiente para un vector base $b_{t,1}$ de la base B_t indicado por la información de identificación t de la tupla positiva y estableciendo $\theta_i v_{i,i'}$ (i' = 2, ..., n_t) como coeficiente para un vector base $b_{t,i'}$ (i' = 2, ..., n_t), y genera un elemento de verificación c_i, cuando la variable ρ(i) es una tupla negativa ¬(t, $v^{\rightarrow}_i$) estableciendo $s_i v_{i,i'}$ (i' = 1, ..., n_t) como coeficiente para el vector base $b_{t,i'}$ (i' = 1, ..., n_t) indicado por la información de identificación t de la tupla negativa,

una parte de generación del elemento de verificación L+1 (336) que genera un elemento de verificación c_{L+1} estableciendo $s_{L+1} - \theta_{L+1} m'$ calculado a partir del valor predeterminado s_{L+1}, el valor m', y un valor predeterminado θ_{L+1} como coeficiente para un vector base $b_{d+1,1}$ de una base B_{d+1}, y estableciendo el valor predeterminado θ_{L+1} como coeficiente para un vector base $b_{d+1,2}$, y

una parte de operación de emparejamiento (340) que verifica la autenticidad de los datos de firma σ dirigiendo una operación de emparejamiento $\Pi_{i=0}^{L+1} e(c_i, s^*_i)$ para el elemento de verificación c_0 generado por la parte de generación del elemento de verificación 0, el elemento de verificación c_i generado por la parte de generación del elemento de verificación i, el elemento de verificación c_{L+1} generado por la parte de generación del elemento de verificación L+1, y los elementos de firma s^*_0, s^*_i y s^*_{L+1} incluidos en los datos de firma σ.

2. El sistema de procesamiento de firmas según la reivindicación 1, que ejecuta el proceso de firma usando

una base B_0 que tiene al menos el vector base $b_{t,i}$ (i = 1, ..., $1+u_0$, …, $1+u_0+w_0$, …, $1+u_0+w_0+z_0$),

la base B_t (t = 1, …, d) que tiene al menos el vector base $b_{t,i}$ (i = 1, ..., n_t, …, n_t+u_t, …, $n_t+u_t+w_t$, …, $n_t+u_t+w_t+z_t$) (u_t, w_t y z_t son cada uno un número entero de 1 o más),

la base B_{d+1} que tiene al menos el vector base $b_{t,i}$ (i = 1, 2, ..., $2+u_{d+1}$, …, $2+u_{d+1}+w_{d+1}$, …, $2+u_{d+1}+w_{d+1}+z_{d+1}$),

la base B^*_0 que tiene al menos el vector base $b^*_{t,i}$ (i = 1, ..., $1+u_0$, …, $1+u_0+w_0$, …, $1+u_0+w_0+z_0$),

la base B^*_t (t = 1, …, d) que tiene al menos el vector base $b^*_{t,i}$ (i = 1, ..., n_t, …, n_t+u_t, …, $n_t+u_t+w_t$, …, $n_t+u_t+w_t+z_t$) (u_t, w_t y z_t son cada uno un número entero de 1 o más), y

la base B^*_{d+1} que tiene al menos el vector base $b^*_{t,i}$ (i = 1, 2, ..., $2+u_{d+1}$, …, $2+u_{d+1}+w_{d+1}$, …, $2+u_{d+1}+w_{d+1}+z_{d+1}$),

en donde, en el dispositivo de generación de claves,

la parte de generación del elemento de clave 0 genera el elemento de clave k^*_0 indicado en la Fórmula 1 en base a un número aleatorio δ y un número aleatorio $\Phi_{0,i}$ (i = 1, ..., w_0),

la parte de generación del elemento de clave t genera el elemento de clave k^*_i indicado en la Fórmula 2 para cada información de identificación t incluida en el conjunto de atributos Γ en base al número aleatorio δ y un número aleatorio $\Phi_{i,i}$ (i = 1, ..., w_t), y

la parte de generación del elemento de clave d+1 genera el elemento de clave $k^*_{d+1,1}$ y el elemento de clave $k^*_{d+1,2}$ que se indican en la Fórmula 3 en base al número aleatorio δ, un número aleatorio $\Phi_{d+1,1,,i}$ (i = 1, ..., w_{d+1}), y un número aleatorio $\Phi_{d+1,2,,i}$ (i = 1, ..., w_{d+1}),

en donde, en el dispositivo de firma,

la parte de generación del elemento de firma 0 genera el elemento de firma s^*_0 indicado en la Fórmula 4 en base a un número aleatorio ξ,

la parte de generación del elemento de firma i genera el elemento de firma s^*_i indicado en la Fórmula 5 para cada número entero i = 1, ..., L en base a un número aleatorio ξ, y

la parte de generación del elemento de firma L+1 genera el elemento de firma s^*_{L+1} indicado en la Fórmula 6 en base al número aleatorio ξ y el valor m', y

en donde, en el dispositivo de verificación,

la parte de generación del elemento de verificación 0 genera el elemento de verificación c_0 indicado en la Fórmula 7 en base al valor s_0, el número aleatorio s_{L+1}, y un número aleatorio $\eta_{0,i}$ (i = 1, ..., z_0),

la parte de generación del elemento de verificación i genera el elemento de verificación c_i indicado en la Fórmula 8 para cada número entero i = 1, ..., L en base al vector de columna $s^{\rightarrow T}$, el número aleatorio θ_i, y un número aleatorio $\eta_{i,i'}$ (i = 1, ..., L; i' = 1, ..., z_t), y

la parte de generación del elemento de verificación L+1 genera el elemento c_{L+1} indicado en la Fórmula 9 en base al número aleatorio s_{L+1}, el número aleatorio θ_{L+1}, un número aleatorio $\eta_{L+1,i'}$ (i' = 1, ..., z_{d+1}), y el valor m'.

[Fórmula 1]

$$k_0^* := (\delta, \overbrace{0^{u_0}}^{u_0}, \overbrace{\varphi_{0,1},\ldots,\varphi_{0,w_0}}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbf{B}_0^*}$$

[Fórmula 2]

$$k_t^* := (\overbrace{\delta(x_{t,1},\ldots,x_{t,n_t})}^{n_t}, \overbrace{0^{u_t}}^{u_t}, \overbrace{\varphi_{t,1},\ldots,\varphi_{t,w_t}}^{w_t}, \overbrace{0^{z_t}}^{z_t})_{\mathbf{B}_t^*}$$

[Fórmula 3]

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

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

[Fórmula 4]

$$s_0^* := \xi k_0^* + r_0^*,$$

$$\text{donde } r_0^* \xleftarrow{U} \text{span}\left\langle b_{0,1+u_t+1}^*,\ldots,b_{0,1+u_t+w_t}^* \right\rangle$$

[Fórmula 5]

$$s_i^* := \gamma_i \cdot \xi k_t^* + \sum_{t=1}^{n_t} y_{i,t} \cdot b_{t,t}^* + r_i^* \text{ para } 1 \le i \le L,$$

donde

$$r_i^* \xleftarrow{U} \text{span}\left\langle b_{t,n_t+u_t+1}^*,\ldots,b_{t,n_t+u_t+w_t}^* \right\rangle,$$

$\gamma_i, \vec{y}_i := (y_{i,1},...,y_{i,n_t})$ se define como

$$\text{si } i \in I \wedge \rho(i) = (t, v_i),\quad \gamma_i := \alpha_i,\quad \vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},$$

$$\text{si } i \in I \wedge \rho(i) = \neg(t, v_i),\quad \gamma_i := \frac{\alpha_i}{\vec{v}_i \cdot \vec{x}_t},$$

$$\vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

$$\text{si } i \notin I \wedge \rho(i) = (t, v_i),\quad \gamma_i := 0,\quad \vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},$$

$$\text{si } i \notin I \wedge \rho(i) = \neg(t, v_i),\quad \gamma_i := 0,$$

$$\vec{y}_i \xleftarrow{\cup} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

$$(\beta_i) \xleftarrow{\cup} \left\{(\beta_1,...,\beta_L) \,\middle|\, \sum_{i=1}^{L} \beta_i M_i = \vec{0}\right\}$$

[Fórmula 6]

$$s^*_{L+1} := \xi(k^*_{d+1,1} + m' \cdot k^*_{d+1,2}) + r^*_{L+1},$$

$$\text{donde } r^*_{L+1} \xleftarrow{\cup} \text{span}\left\langle b^*_{d+1,2+u_{d+1}+1},...,b^*_{d+1,2+u_{d+1}+w_{d+1}} \right\rangle$$

[Fórmula 7]

$$c_0 := (-s_0 - s_{L+1}, \overbrace{0^{u_0}}^{u_0}, \overbrace{0^{w_0}}^{w_0}, \overbrace{\eta_{0,1},...,\eta_{0,z_0}}^{z_0})_{\mathbf{B}_0}$$

[Fórmula 8]

$$\text{si } \rho(i) = (t, v_i),$$

$$c_i := (\overbrace{s_i + \theta_i v_{i,1}, \theta_i v_{i,2},..., \theta_i v_{i,n_t}}^{n_t}, \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1},...,\eta_{i,z_t}}^{z_t})_{\mathbf{B}_t},$$

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

$$c_i := (\overbrace{s_i\ (v_{i,1},...,v_{i,n_t})}^{n_t}, \overbrace{0^{u_t}}^{u_t}, \overbrace{0^{w_t}}^{w_t}, \overbrace{\eta_{i,1},...,\eta_{i,z_t}}^{z_t})_{\mathbf{B}_t}$$

[Fórmula 9]

$$c_{L+1} := (\overbrace{s_{L+1} - \theta_{L+1} m', \theta_{L+1}}^{2}, \overbrace{0^{u_{d+1}}}^{u_{d+1}},$$

$$\overbrace{0^{w_{d+1}}}^{w_{d+1}}, \overbrace{\eta_{L+1,1},\ldots,\eta_{L+1,z_{d+1}}}^{z_{d+1}})\mathbf{B}_{d+1}$$

3. El sistema de procesamiento de firmas según la reivindicación 1 o 2,

en donde, en el dispositivo de firma,

la parte de generación del elemento de firma L+1 genera el elemento de firma s^*_{L+1} usando un valor de comprobación aleatoria obtenido a la introducción del mensaje m, la matriz M y la variable ρ(i) para cada número entero i = 1, ..., L, como el valor m', y

en donde, en el dispositivo de verificación,

la parte de generación del elemento de verificación L+1 genera el elemento de verificación c_{L+1} usando el valor de comprobación aleatoria como el valor m'.

4. Un dispositivo de generación de claves (100) que genera una clave de firma sk_Γ, en un sistema de procesamiento de firmas (10) que ejecuta un proceso de firma usando una base B_t y una base B^*_t para cada número entero t = 0, ..., d+1 (d es un número entero de 1 o más), el dispositivo de generación de claves que comprende:

una primera parte de entrada de información (130) que toma como entrada un conjunto de atributos Γ que incluye información de identificación t e información de atributo $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t donde n_t es un número entero de 1 o más) para al menos un número entero t = 1, ..., d;

una parte de generación del elemento de clave 0 (142) que genera un elemento de clave k^*_0 donde un valor δ predeterminado se establece como coeficiente para un vector base $b^*_{0,1}$ de una base B^*_0;

una parte de generación del elemento de clave t (143) que genera un elemento de clave k^*_t donde $\delta x_{t,i}$ (i = 1, ..., n_t) obtenido multiplicando la información de atributo $\vec{x}_t$ por el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{t,i}$ (i = 1, ..., n_t) de la base B^*_t, que concierne a cada información de identificación t incluida en el conjunto de atributos Γ introducido por la primera parte de entrada de información;

una parte de generación del elemento de clave d+1 (144) que genera un elemento de clave $k^*_{d+1,1}$ donde el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{d+1,1}$ de una base B^*_{d+1}, y un elemento de clave $k^*_{d+1,2}$ donde el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{d+1,2}$ de la base B^*_{d+1}, y

una parte de transmisión de clave de firma (150) que transmite, a un dispositivo de firma (200), la clave de firma sk_Γ que incluye: el elemento de clave k^*_0 generado por la parte de generación del elemento de clave 0; el elemento de clave k^*_t generado por la parte de generación del elemento de clave t que concierne a cada información de identificación t incluida en el conjunto de atributos Γ; el elemento de clave $k^*_{d+1,1}$ y el elemento de clave $k^*_{d+1,2}$ que se generan por la parte de generación de elemento de clave d+1; y el conjunto de atributos Γ,

5. Un dispositivo de firmas (100) que genera datos de firma σ, en un sistema de procesamiento de firmas que ejecuta un proceso de firma usando una base B_t y una base B^*_t para cada número entero t = 0, ..., d+1 (d es un número entero de 1 o más), el dispositivo de firmas que comprende:

una parte de adquisición de clave de firma (210) que adquiere la clave de firma sk_Γ,

un conjunto de atributos Γ que incluye información de identificación t e información de atributos $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t donde n_t es un número entero de 1 o más) para al menos un número entero t = 1, …, d,

un elemento de clave k^*_0 donde un valor δ predeterminado se establece como coeficiente para un vector base $b^*_{0,1}$ de base B^*_0,

un elemento de clave k^*_t donde $\delta x_{t,i}$ (i = 1, ..., n_t) obtenido multiplicando la información de atributo $\vec{x}_t$ por el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{t,i}$ (i = 1, ..., n_t) de la base B^*_t, que concierne a cada información de identificación t incluida en el conjunto de atributos Γ,

un elemento de clave $k^*_{d+1,1}$ donde el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{d+1,1}$ de una base B^*_{d+1}, y

un elemento de clave $k^*_{d+1,2}$ donde el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{d+1,2}$ de la base B^*_{d+1};

una segunda parte de entrada de información (220) que toma como entrada una variable ρ(i) para cada número entero i = 1, ..., L (L es un número entero de 1 o más), cuya variable ρ(i) es cualquiera de una tupla positiva (t, $v^{\rightarrow}_i$) y una tupla negativa ¬(t, $v^{\rightarrow}_i$) de la información de identificación t (t es cualquier número entero de t = 1, ..., d) y la información de atributo $v^{\rightarrow}_i := (v_{i,i'})$ (i' = 1, ..., n_t); una matriz M predeterminada que tiene L filas y r columnas (r es un número entero de 1 o más); y un mensaje m;

una parte de cálculo de coeficiente complementario (240) que, en base a la variable ρ(i) introducida por la segunda parte de entrada de información y el conjunto de atributos Γ incluido en la clave de firma sk_Γ adquirida por la parte de adquisición de clave de firma, especifica, entre los números enteros i = 1, ..., L, un conjunto I de un número entero i para el cual la variable ρ(i) es una tupla positiva (t, $v^{\rightarrow}_i$) y con el cual un producto interno de $v^{\rightarrow}_i$ de la tupla positiva y $x^{\rightarrow}_t$ incluido en el conjunto de atributos Γ indicado por la información de identificación t de la tupla positiva llega a ser 0, y un número entero i para el cual la variable ρ(i) es una tupla negativa ¬(t, $v^{\rightarrow}_i$) y con el cual un producto interno de $v^{\rightarrow}_i$ de la tupla negativa y $x^{\rightarrow}_t$ incluido en el conjunto de atributos Γ indicado por la información de identificación t de la tupla negativa no llega a ser 0; y calcula, concerniente a i incluido en el conjunto I especificado, un coeficiente complementario α_i con el cual un total de $\alpha_i M_i$ en base a M_i que es un elemento en una fila de orden i de la matriz M introducida por la segunda parte de entrada de información llega a ser un vector $h^{\rightarrow}$ predeterminado,

una parte de generación del elemento de firma 0 (252) que genera un elemento de firma s^*_0 que incluye el elemento de clave k^*_0 incluido en la clave de firma sk_Γ;

una parte de generación del elemento de firma i (253) que genera, para cada número entero i = 1 ..., L, un elemento de firma s^*_i que incluye $\gamma_i k^*_t$ obtenido multiplicando el elemento de clave k^*_t incluido en la clave de firma sk_Γ por un valor γ_i, estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i$ cuando el número entero i se incluye en el conjunto I especificado por la parte de cálculo de coeficiente complementario y la variable ρ(i) es una tupla positiva (t, $v^{\rightarrow}_i$); estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i/(v^{\rightarrow}_i \cdot x^{\rightarrow}_t)$ cuando el número entero i está incluido en el conjunto I y la variable ρ(i) es una tupla negativa ¬(t, $v^{\rightarrow}_i$); y estableciendo el valor γ_i para satisfacer $\gamma_i := 0$ cuando el número entero i no está incluido en el conjunto I;

una parte de generación del elemento de firma L+1 (254) que genera un elemento de firma s^*_{L+1} que incluye una suma del elemento de clave $k^*_{d+1,1}$ incluido en la clave de firma sk_Γ y $m' \cdot k^*_{d+1,2}$ obtenido multiplicando el elemento de clave $k^*_{d+1,2}$ por un valor m' generado usando el mensaje m, y

una parte de transmisión de datos de firma (260) que transmite, a un dispositivo de verificación, los datos de firma σ que incluyen: el elemento de firma s^*_0 generado por la parte de generación del elemento de firma 0; el elemento de firma s^*_i generado para cada número entero i = 1, ..., L por la parte de generación del elemento de firma i; el elemento de firma s^*_{L+1} generado por la parte de generación del elemento de firma L+1; el mensaje m; la variable ρ(i); y la matriz M.

6. Un dispositivo de verificación (300) que verifica los datos de firma σ, en un sistema de procesamiento de firmas (10) que ejecuta un proceso de firma usando una base B_t y una base B^*_t para cada número entero t = 0, ..., d+1 (d es un número entero de 1 o más), el dispositivo de verificación que comprende:

una parte de adquisición de datos (320) que adquiere los datos de firma σ que incluyen: un elemento de firma s^*_0; un elemento de firma s^*_i para cada número entero i = 1, …, L; un elemento de firma s^*_{L+1}; un mensaje m; una variable ρ(i) para cada número entero i = 1, …, L (L es un número entero de 1 o más), cuya variable ρ(i) es cualquiera de una tupla positiva (t, $v^{\rightarrow}_i$) y una tupla negativa ¬(t, $v^{\rightarrow}_i$) de la información de identificación t (t es cualquier número entero de t = 1, …, d) y la información de atributo $v^{\rightarrow}_i := (v_{i,i'})$ (i' = 1, ..., n_t) y una matriz M predeterminada que tiene L filas y r columnas (r es un número entero de 1 o más);

una parte de generación del elemento de verificación 0 (334) que genera un elemento de verificación c_0 estableciendo, como coeficiente para un vector base $b_{0,1}$ de una base B_0, $-s_0 - s_{L+1}$ calculado a partir de un valor $s_0 := h^{\rightarrow'} \cdot f^{\rightarrow}$ y un valor predeterminado s_{L+1}, el valor $s_0 := h^{\rightarrow'} \cdot f^{\rightarrow}$ que se genera usando un vector $f^{\rightarrow}$ que tiene r partes de elementos, y un vector $h^{\rightarrow}$ que tiene r partes de elementos;

una parte de generación del elemento de verificación i (335) que, para cada número entero i = 1, ..., L y usando un vector de columna $s^{\rightarrow T} := (s_1, ..., s_L)^T := M \cdot f^{\rightarrow T}$ generado en base al vector $f^{\rightarrow}$ y la matriz M que se incluye en los datos de firma σ adquiridos por la parte de adquisición de datos, y un número predeterminado θ_i para cada número entero i = 1, ..., L, genera un elemento de verificación c_i, cuando la variable ρ(i) es una tupla positiva (t, $v^{\rightarrow}_i$), estableciendo $s_i + \theta_i v_{i,1}$ como coeficiente para un vector base $b_{t,1}$ de la base B_t indicado por la información de identificación t de la tupla positiva y estableciendo $\theta_i v_{i,i'}$ (i' = 2, ..., n_t) como coeficiente para un vector base $b_{t,i'}$ (i' = 2, ..., n_t), y genera un elemento de verificación c_i, cuando la variable ρ(i) es una tupla negativa ¬(t, $v^{\rightarrow}_i$) estableciendo $s_i v_{i,i'}$ (i' = 1, ..., n_t) como coeficiente para el vector base $b_{t,i'}$ (i' = 1, ..., n_t) indicado por la información de identificación t de la tupla negativa,

una parte de generación del elemento de verificación L+1 (336) que genera un elemento de verificación c_{L+1} estableciendo $s_{L+1} - \theta_{L+1} m'$ calculado a partir del valor predeterminado s_{L+1}, un valor m' calculado a partir del

mensaje m, y un valor predeterminado θ_{L+1} como coeficiente para un vector base $b_{d+1,1}$ de una base B_{d+1}, y estableciendo el valor predeterminado θ_{L+1} como coeficiente para un vector base $b_{d+1,2}$, y

una parte de operación de emparejamiento (340) que verifica la autenticidad de los datos de firma σ dirigiendo una operación de emparejamiento $\Pi_{i=0}^{L+1} e(c_i, s^*_i)$ para el elemento de verificación c_0 generado por la parte de generación del elemento de verificación 0, el elemento de verificación c_i generado por la parte de generación del elemento de verificación i, el elemento de verificación c_{L+1} generado por la parte de generación del elemento de verificación L+1, y los elementos de firma s^*_0, s^*_i y s^*_{L+1} incluidos en los datos de firma σ.

7. Un sistema de procesamiento de firmas (10) que comprende d (d es un número entero de 1 o más) unidades de dispositivos de generación de claves (100), un dispositivo de firmas (200) y un dispositivo de verificación (300), y que sirve para ejecutar un proceso de firma usando una base B_t y una base B^*_t para al menos número entero t = 0, ..., d,

en donde cada una de las d unidades de dispositivos de generación de claves incluye

una primera parte de entrada de información (130) que toma como entrada información de atributo $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t donde n_t es un número entero de 1 o más) para un número entero t entre los números enteros t = 1, ..., d, que se predetermina para cada uno de los dispositivos de generación de claves,

una parte de generación de elemento de clave (145) que, para el número entero t y cada número entero j = 1, 2 genera un elemento de clave $k^*_{t,j}$ incluyendo un vector indicado por la Fórmula 10 en base a una información de atributo $\vec{x}_t$ introducida por la primera parte de entrada de información, un valor δ predeterminado$_j$, y un vector base $b^*_{t,i}$ (i = 1, ..., $2n_t$) de la base B^*_t, y

una parte de transmisión de clave de firma (150) que transmite, al dispositivo de firma, una clave de firma usk que incluye: el elemento de clave $k^*_{t,j}$ generado por la parte de generación de elemento de clave; y la información de atributo $\vec{x}_t$.

en donde el dispositivo de firmas incluye

una segunda parte de entrada de información (220) que toma como entrada una variable ρ(i) para cada número entero i = 1, ..., L (L es un número entero de 1 o más), cuya variable ρ(i) es cualquiera de una tupla positiva (t, $\vec{v}_i$) y una tupla negativa ¬(t, $\vec{v}_i$) de la información de identificación t (t es cualquier número entero de t = 1, ..., d) y la información de atributo $\vec{v}_i := (v_{i,i'})$ (i' = 1, ..., n_t); una matriz M predeterminada que tiene L filas y r columnas (r es un número entero de 1 o más); y un mensaje m,

una parte de adquisición de clave de firma (210) que adquiere la clave de firma usk transmitida por la parte de transmisión de clave de firma de al menos un dispositivo de generación de claves entre las d unidades de dispositivos de generación de claves,

una parte de cálculo de coeficiente complementario (240) que, en base a la variable ρ(i) introducida por la segunda parte de entrada de información y la información de atributo $\vec{x}_i$ incluida en la clave de firma usk adquirida por la parte de adquisición de clave de firma, especifica, entre los números enteros i = 1, ..., L, un conjunto I de un número entero i para el cual la variable ρ(i) es una tupla positiva (t, $\vec{v}_i$), la clave de firma usk que incluye $\vec{x}_t$ indicado por la información de identificación t de la tupla positiva siendo adquirida por la parte de adquisición de clave de firma, y con el cual un producto interno de $\vec{v}_i$ de la tupla positiva y la información de atributo $\vec{x}_t$ indicado por la información de identificación t de la tupla positiva llega a ser 0, y un número entero i para el cual la variable ρ(i) es una tupla negativa ¬(t, $\vec{v}_i$), la clave de firma usk que incluye $\vec{x}_t$ indicada por la información de identificación t de la tupla negativa siendo adquirida por la parte de adquisición de clave de firma, y con el cual un producto interno de $\vec{v}_i$ de la tupla negativa y la información de atributo $\vec{x}_t$ indicada por la información de identificación t de la tupla negativa no llega a ser 0; y calcula, concerniente a i incluido en el conjunto I especificado, un coeficiente complementario α_i con el cual un total de $\alpha_i M_i$ en base a M_i que es un elemento en una fila de orden i de la matriz M introducida por la segunda parte de entrada de información llega a ser un vector $\vec{h}$ predeterminado,

una parte de generación de elemento de firma (255) que genera, para cada número entero i = 1, …, L, un elemento de firma s^*_i que incluye un vector indicado en la Fórmula 11 usando el vector base $b^*_{t,i}$ (i = $2n_t$+1, $2n_t$+2) de la base B^*_t, en base a un elemento de clave $k^*_{t,1}$ y un elemento de clave $k^*_{t,2}$ incluidos en la clave de firma usk, los valores predeterminados ξ_1, E y μ, y un valor m' calculado a partir del mensaje m, estableciendo un valor γ_i para satisfacer $\gamma_i := \alpha_i$ cuando el número entero i está incluido en el conjunto I especificado por la parte de cálculo de coeficiente complementario y la variable ρ(i) es una tupla positiva (t, $\vec{v}_i$); estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i/(v_i \cdot x_t)$ cuando el número entero i está incluido en el conjunto I y la variable ρ(i) es una tupla negativa ¬(t, $\vec{v}_i$); y estableciendo el valor γ_i para satisfacer $\gamma_i := 0$ cuando el número entero i no está incluido en el conjunto I, y

una parte de transmisión de datos de firma (260) que transmite, al dispositivo de verificación, los datos de firma σ que incluyen: el elemento de firma s^*_i generado para cada número entero i = 1, ..., L por la parte de generación de elemento de firma; el mensaje m; la variable ρ(i); y la matriz M, y

en donde el dispositivo de verificación incluye

una parte de adquisición de datos (320) que adquiere los datos de firma σ transmitidos por la parte de transmisión de datos de firma,

una parte de generación de vector (332, 333) que genera un vector de columna $s^{\rightarrow T} := (s_1, ..., s_L)^T := M \cdot f^{\rightarrow T}$ en base a un vector $f^{\rightarrow}$ que tiene r partes de elementos y la matriz M incluida en los datos de firma σ adquiridos por la parte de adquisición de datos, y genera un vector de columna $(s^{\rightarrow\prime})^T := (s_1', ..., s_L')^T := M \cdot (f^{\rightarrow\prime})^T$ en base a la matriz M y a un vector $f^{\rightarrow\prime}$ que tiene r partes de elementos y que satisface $s_0 = h^{\rightarrow} \cdot (f^{\rightarrow\prime})^T$ donde $s_0 = h^{\rightarrow} \cdot f^{\rightarrow T}$,

una parte de generación de elemento de verificación (337) que, para cada número entero i = 1, ..., L y en base al vector de columna $s^{\rightarrow T}$ y al vector de columna $(s^{\rightarrow\prime})^T$ que se generan por la parte de generación de vector, y los valores predeterminados θ_i, θ_i', θ_i'', y σ_i para cada número entero i = 1, ..., L, genera un elemento de verificación c_i que incluye un vector indicado en la Fórmula 12, cuando la variable ρ(i) es una tupla positiva $(t, v^{\rightarrow}_i)$, usando un vector base $b_{t,i'}$ (i' = 1, …, $2n_t+2$) de la base B_t indicada por la información de identificación t de la tupla positiva, y genera un elemento de verificación c_i que incluye un vector indicado en la Fórmula 13, cuando la variable ρ(i) es una tupla negativa $\neg(t, v^{\rightarrow}_i)$, usando un vector base $b_{t,i}$ (i = 1, …, $2n_t+2$) indicado por la información de identificación t de la tupla negativa, y

una parte de operación de emparejamiento (340) que verifica una autenticidad de los datos de firma σ dirigiendo una operación de emparejamiento $\Pi_{i=1}{}^{L} e(c_i, s^*_i)$ para el elemento de verificación c_i generado por la parte de generación de elemento de verificación, y el elemento de firma s^*_i incluido en los datos de firma σ.

[Fórmula 10]

$$(\overbrace{(\delta_j+1)(x_{t,1},...,x_{t,n_t})}^{n_t},\overbrace{-\delta_j(x_{t,1},...,x_{t,n_t})}^{n_t},0,...,0)_{\mathbf{B}_t^*}$$

[Fórmula 11]

$$\gamma_i \cdot (\xi_1 k^*_{t,1} + (E-\xi_1)k^*_{t,2}) + (\mu b^*_{t,2n_t+1}) + m'(\mu b^*_{t,2n_t+2})$$

[Fórmula 12]

$$(\overbrace{s_i+\theta_i v_{i,1},\theta_i v_{i,2},...,\theta_i v_{i,n_t}}^{n_t},\overbrace{s_i'+\theta_i' v_{i,1},\theta_i' v_{i,2},...,\theta_i' v_{i,n_t}}^{n_t},$$
$$\overbrace{\sigma_i-\theta_i"m',\theta_i"}^{2},0,...,0)_{\mathbf{B}_t}$$

[Fórmula 13]

$$(\overbrace{s_i(v_{i,1},...,v_{i,n_t})}^{n_t},\overbrace{s_i'(v_{i,1},...,v_{i,n_t})}^{n_t},\overbrace{\sigma_i-\theta_i"m',\theta_i"}^{2},0,...,0)_{\mathbf{B}_t}$$

8. El sistema de procesamiento de firmas según la reivindicación 7, que ejecuta el proceso de firma usando, para al menos un número entero t = 1, ..., d, la base B_t que tiene al menos el vector base $b_{t,i}$ (i = 1, …, $2n_t+2$ …, $2n_t+2+u_t$, …, $2n_t+2+u_t+w_t$, …, $2n_t+2+u_t+w_t+z_t$) (donde u_t, w_t y z_t son cada uno un número entero de 1 o más), y la base B^*_t que tiene al menos el vector base $b^*_{t,i}$ (i = 1, …, $2n_t+2$ …, $2n_t+2+u_t$, …, $2n_t+2+u_t+w_t$, …, $2n_t+2+u_t+w_t+z_t$),

en donde, en el dispositivo de generación de claves,

el elemento de clave $k^*_{t,j}$ indicado en la Fórmula 14 se genera para el número entero t y cada número entero j = 1, 2 en base a la información de atributo $x^{\rightarrow}_t$, los valores predeterminados δ y Δ, y un número aleatorio $\Phi_{t,j,i}$ (j = 1, 2; i = 1, ..., w_t),

en donde, en el dispositivo de firma,

la parte de generación de elemento de firma genera, para cada número entero i = 1 ..., L, el elemento de firma s^*_i indicado en la Fórmula 16 usando r^*_i, γ_i, $y^{\rightarrow}_i := (y_{i,i})$ (i = 1, ..., n_t), e $y'^{\rightarrow}_i := (y'_{i,i})$ (i = 1, ..., n_t) indicado en la Fórmula 15, en base al elemento de clave $k^*_{t,1}$ y al elemento de clave $k^*_{t,2}$, los números aleatorios ξ_1 y ξ_2, los valores predeterminados E, π, π', y μ, y el valor m', y

en donde, en el dispositivo de verificación,

la parte de generación de elemento de verificación, para cada número entero i = 1, ..., L y en base al vector de columna $s^{\rightarrow T}$ y el vector de columna $(s^{\rightarrow})^T$, los números aleatorios θ_i, θ_i' y θ_i'', el valor predeterminado σ_i, y un número aleatorio $\eta_{i,i'}$ (i = 1, ..., L; i' = 1, ..., z_t), genera el elemento de verificación c_i indicado en la Fórmula 17 cuando la variable ρ(i) es una tupla positiva (t, $v^{\rightarrow}_i$), y genera el elemento de verificación c_i indicado en la Fórmula 18 cuando la variable ρ(i) es una tupla negativa ¬(t, $v^{\rightarrow}_i$).

[Fórmula 14]

$$k^*_{t,j} := (\overbrace{(\delta_j + \Delta)(x_{t,1},...,x_{t,n_t})}^{n_t}, \overbrace{-\delta_j(x_{t,1},...,x_{t,n_t})}^{n_t}, \overbrace{0^2}^{2}, \overbrace{0^{u_t}}^{u_t}, \overbrace{\varphi_{t,j,1},...,\varphi_{t,j,w_t}}^{w_t}, \overbrace{0^{z_t}}^{z_t})_{\mathbf{B}^*_t}$$

[Fórmula 15]

$$r^*_i \xleftarrow{U} \mathrm{span}\left\langle b^*_{t,2n_t+2+u_t+1},...,b^*_{t,2n_t+2+u_t+w_t} \right\rangle$$

$$\text{si } i \in I \wedge \rho(i) = (t,\vec{v}_i),\ \ \gamma_i := \alpha_i,$$

$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},$$

$$\vec{y}'_i \xleftarrow{U} \{\vec{y}'_i \,|\, \vec{y}'_i \cdot \vec{v}_i = 0 \wedge y'_{i,1} = \beta'_i\},$$

$$\text{si } i \in I \wedge \rho(i) = \neg(t,\vec{v}_i),\ \ \gamma_i := \frac{\alpha_i}{\vec{v}_i \cdot \vec{x}_t},$$

$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

$$\vec{y}'_i \xleftarrow{U} \{\vec{y}'_i \,|\, \vec{y}'_i \cdot \vec{v}_i = \beta'_i\},$$

$$\text{si } i \notin I \wedge \rho(i) = (t,\vec{v}_i),\ \ \gamma_i := 0,$$

$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = 0 \wedge y_{i,1} = \beta_i\},$$

$$\vec{y}'_i \xleftarrow{U} \{\vec{y}'_i \,|\, \vec{y}'_i \cdot \vec{v}_i = 0 \wedge y'_{i,1} = \beta'_i\},$$

$$\text{si } i \notin I \wedge \rho(i) = \neg(t,\vec{v}_i),\ \ \gamma_i := 0,$$

$$\vec{y}_i \xleftarrow{U} \{\vec{y}_i \,|\, \vec{y}_i \cdot \vec{v}_i = \beta_i\},$$

$$\vec{y}'_i \xleftarrow{U} \{\vec{y}'_i \,|\, \vec{y}'_i \cdot \vec{v}_i = \beta'_i\},$$

$$(\beta_i),(\beta_i') \xleftarrow{U} \{(\beta_1,...,\beta_L) \,|\, \textstyle\sum_{i=1}^{L} \beta_i M_i = \vec{0}\}$$

[Fórmula 16]

$$s_i^* := \gamma_i \cdot (\xi_1 k_{t,1}^* + (1-\xi_1) k_{t,2}^*) + \sum_{\iota=1}^{n_t} y_{i,\iota} (\pi b_{t,\iota}^*) + \sum_{\iota=1}^{n_t} y'_{i,\iota} (\pi' b_{t,n_t+\iota}^*) + \xi_2 ((\mu b_{t,2n_t+1}^*) + m'(\mu b_{t,2n_t+2}^*)) + r_i^*$$

[Fórmula 17]

$$c_i := (\overbrace{s_i + \theta_i v_{i,1}, \theta_i v_{i,2}, ..., \theta_i v_{i,n_t}}^{n_t}, \overbrace{s_i' + \theta_i' v_{i,1}, \theta_i' v_{i,2}, ..., \theta_i' v_{i,n_t}}^{n_t}, \overbrace{\sigma_i - \theta_i "m', \theta_i ", 0^{u_t}, 0^{w_t}, \eta_{i,1}, ..., \eta_{i,z_t}}^{2\ u_t\ w_t\ z_t})_{\mathbf{B}_t}$$

[Fórmula 18]

$$c_i := (\overbrace{s_i(v_{i,1}, ..., v_{i,n_t})}^{n_t}, \overbrace{s_i'(v_{i,1}, ..., v_{i,n_t})}^{n_t}, \overbrace{\sigma_i - \theta_i "m', \theta_i ", 0^{u_t}, 0^{w_t}, \eta_{i,1}, ..., \eta_{i,z_t}}^{2\ u_t\ w_t\ z_t})_{\mathbf{B}_t}$$

9. El sistema de procesamiento de firmas según la reivindicación 7 u 8,

en donde, en el dispositivo de firma,

la parte de generación de elemento de firma genera el elemento de firma s^*_i usando un valor de comprobación aleatoria obtenido tras la introducción del mensaje m, la matriz M y la variable ρ(i) para cada número entero i = 1, ..., L, como el valor m', y

en donde, en el dispositivo de verificación,

la parte de generación de elemento de verificación genera el elemento de verificación c_i usando el valor de comprobación aleatoria como el valor m'.

10. Un dispositivo de generación de claves (100) que genera una clave de firma usk, en un sistema de procesamiento de firmas (10) que ejecuta un proceso de firma usando una base B_t y una base B^*_t para al menos número entero t = 1, ..., d, el dispositivo de generación de claves que comprende:

una primera parte de entrada de información (130) que toma como entrada la información de atributo $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t) para un número entero t predeterminado entre los números enteros t = 1, ..., d;

una parte de generación de elemento de clave (145) que, para el número entero t y cada número entero j = 1, 2, genera un elemento de clave $k^*_{t,j}$ que incluye un vector indicado en la Fórmula 19, en base a la información de atributo $\vec{x}_t$ introducida por la primera parte de entrada de información, un valor δ_j predeterminado, y un vector base $b^*_{t,i}$ (i = 1, …, $2n_t$) de la base atributo B^*_t; y

una parte de transmisión de clave de firma (150) que transmite la clave de firma usk que incluye: el elemento de clave $k^*_{t,j}$ generado por la parte de generación de elemento de clave; y la información de atributo $\vec{x}_t$, a un dispositivo de firma (200).

[Fórmula 19]

$$(\overbrace{(\delta_j+1)(x_{t,1},...,x_{t,n_t})}^{n_t},\overbrace{-\delta_j(x_{t,1},...,x_{t,n_t})}^{n_t},0,...,0)_{\mathbf{B}_t^*}$$

11. Un dispositivo de firmas (200) que genera datos de firma σ, en un sistema de procesamiento de firmas (10) que ejecuta un proceso de firma usando una base B_t y una base B^*_t para al menos número entero t = 1, ..., d, el dispositivo de firmas que comprende:

una parte de adquisición de clave de firma (210) que, para al menos uno de los números enteros t de t = 1, ..., d, y cada número entero j = 1, 2 y en base a la información de atributo $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t) un valor δ_j predeterminado, y un vector base $b^*_{t,i}$ (i = 1, ..., $2n_t$) de la base B^*_t, adquiere una clave de firma usk que incluye: un elemento de clave $k^*_{t,j}$ generado para incluir un vector indicado en la Fórmula 20; y la información de atributo $\vec{x}_t$;

una segunda parte de entrada de información (220) que toma como entrada una variable ρ(i) para cada número entero i = 1, ..., L (L es un número entero de 1 o más), cuya variable ρ(i) es cualquiera de una tupla positiva (t, $\vec{v}_i$) y una tupla negativa ¬(t, $\vec{v}_i$) de la información de identificación t (t es cualquier número entero de t = 1, ..., d) y la información de atributo $\vec{v}_i := (v_{i,i'})$ (i' = 1, ..., n_t); una matriz M predeterminada que tiene L filas y r columnas (r es un número entero de 1 o más); y un mensaje m;

una parte de cálculo de coeficiente complementario (240) que, en base a la variable ρ(i) introducida por la segunda parte de entrada de información y la información de atributo $\vec{x}_t$ incluida en la clave de firma usk adquirida por la parte de adquisición de clave de firma, especifica, entre los números enteros i = 1, ..., L, un conjunto I de un número entero i para el cual la variable ρ(i) es una tupla positiva (t, $\vec{v}_i$), la clave de firma usk que incluye $\vec{x}_t$ indicado por la información de identificación t de la tupla positiva que se adquiere por la parte de adquisición de clave de firma, y con el cual un producto interno de $\vec{v}_i$ de la tupla positiva y la información de atributo $\vec{x}_t$ indicado por la información de identificación t de la tupla positiva llega a ser 0, y un número entero i para el cual la variable ρ(i) es una tupla negativa ¬(t, $\vec{v}_i$), la clave de firma usk que incluye $\vec{x}_t$ indicada por la información de identificación t de la tupla negativa que se adquiere por la parte de adquisición de clave de firma, y con el cual un producto interno de $\vec{v}_i$ de la tupla negativa y la información de atributo $\vec{x}_t$ indicada por la información de identificación t de la tupla negativa no llega a ser 0; y $\vec{v}_i$ y $\vec{x}_t$ no son iguales; y calcula, concerniente a i incluido en el conjunto I especificado, un coeficiente complementario α_i con el cual un total de $\alpha_i M_i$ en base a M_i que es un elemento en una fila de orden i de la matriz M introducida por la segunda parte de entrada de información llega a ser un vector $\vec{h}$ predeterminado;

una parte de generación de elemento de firma (255) que genera, para cada número entero i = 1, …, L, un elemento de firma s^*_i que incluye un vector indicado en la Fórmula 21 usando el vector base $b^*_{t,i}$ (i = $2n_t$+1, $2n_t$+2) de la base B^*_t, en base a un elemento de clave $k^*_{t,1}$ y un elemento de clave $k^*_{t,2}$ incluidos en la clave de firma usk, los valores predeterminados ξ_1, E y μ, y un valor m' calculado a partir del mensaje m, estableciendo un valor γ_i para satisfacer $\gamma_i := \alpha_i$ cuando el número entero i está incluido en el conjunto I especificado por la parte de cálculo de coeficiente complementario y la variable ρ(i) es una tupla positiva (t, $\vec{v}_i$), estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i/(\vec{v}_i \cdot \vec{x}_t)$ cuando el número entero i está incluido en el conjunto I y la variable ρ(i) es una tupla negativa ¬(t, $\vec{v}_i$); y estableciendo el valor γ_i para satisfacer $\gamma_i := 0$ cuando el número entero i no está incluido en el conjunto I; y

una parte de transmisión de datos de firma (260) que transmite, a un dispositivo de verificación (300), los datos de firma σ que incluyen: el elemento de firma s^*_i generado para cada número entero i = 1, ..., L por la parte de generación de elemento de firma; el mensaje m; la variable ρ(i); y la matriz M.

[Fórmula 20]

$$(\overbrace{(\delta_j+1)(x_{t,1},...,x_{t,n_t})}^{n_t},\overbrace{-\delta_j(x_{t,1},...,x_{t,n_t})}^{n_t},0,...,0)_{\mathbf{B}_t^*}$$

[Fórmula 21]

$$\gamma_i \cdot (\xi_1 k^*_{t,1} + (E-\xi_1)k^*_{t,2}) + (\mu b^*_{t,2n_t+1}) + m'(\mu b^*_{t,2n_t+2})$$

12. Un dispositivo de verificación (300) que verifica los datos de firma σ, en un sistema de procesamiento de firmas (10) que ejecuta un proceso de firma usando una base B_t y una base B^*_t para al menos número entero t = 1, ..., d, el dispositivo de verificación que comprende:

una parte de adquisición de datos (320) que adquiere los datos de firma σ que incluyen: un elemento de firma s^*_i para cada número entero i = 1, …, L; un mensaje m; una variable ρ(i) para cada número entero i = 1, …, L (L es un número entero de 1 o más), cuya variable ρ(i) es cualquiera de una tupla positiva $(t, v^{\rightarrow}_i)$ y una tupla negativa $\neg(t, v^{\rightarrow}_i)$ de la información de identificación t (t es cualquier número entero de t = 1, …, d) y la información de atributo $v^{\rightarrow}_i := (v_{i,i'})$ (i' = 1, ..., n_t); y una matriz M predeterminada que tiene L filas y r columnas (r es un número entero de 1 o más);

una parte de generación de vector (332, 333) que genera un vector de columna $s^{\rightarrow T} := (s_1, ..., s_L)^T := M \cdot f^{\rightarrow T}$ en base a un vector $f^{\rightarrow}$ que tiene r partes de elementos y la matriz M incluida en los datos de firma σ adquiridos por la parte de adquisición de datos, y genera un vector de columna $(s^{\rightarrow'})^T := (s_1', ..., s_L')^T := M \cdot (f^{\rightarrow'})^T$ en base a la matriz M y a un vector $f^{\rightarrow'}$ que tiene r partes de elementos y que satisface $s_0 = h^{\rightarrow} \cdot (f^{\rightarrow'})^T$ donde $s_0 = h^{\rightarrow} \cdot f^{\rightarrow T}$;

una parte de generación de elemento de verificación (337) que, para cada número entero i = 1, ..., L y en base al vector de columna $s^{\rightarrow T}$ y al vector de columna $(s^{\rightarrow'})^T$ que se generan por la parte de generación de vector, y los valores predeterminados θ_i, θ_i', θ_i'', y σ_i para cada número entero i = 1, ..., L, genera un elemento de verificación c_i que incluye un vector indicado en la Fórmula 22, cuando la variable ρ(i) es una tupla positiva $(t, v^{\rightarrow}_i)$, usando un vector base $b_{t,i'}$ (i' = 1, …, $2n_t+2$) de la base B_t indicada por la información de identificación t de la tupla positiva, y genera un elemento de verificación c_i que incluye un vector indicado en la Fórmula 23, cuando la variable ρ(i) es una tupla negativa $\neg(t, v^{\rightarrow}_i)$, usando un vector base $b_{t,i}$ (i = 1, …, $2n_t+2$) indicado por la información de identificación t de la tupla negativa; y

una parte de operación de emparejamiento (340) que verifica una autenticidad de los datos de firma σ dirigiendo una operación de emparejamiento $\Pi_{i=1}^{L} e(c_i, s^*_i)$ para el elemento de verificación c_i generado por la parte de generación de elemento de verificación, y el elemento de firma s^*_i incluido en los datos de firma σ.

[Fórmula 22]

$$(\overbrace{s_i + \theta_i v_{i,1}, \theta_i v_{i,2}, ..., \theta_i v_{i,n_t}}^{n_t}, \overbrace{s_i' + \theta_i' v_{i,1}, \theta_i' v_{i,2}, ..., \theta_i' v_{i,n_t}}^{n_t}, \overbrace{\sigma_i - \theta_i "m', \theta_i "}^{2}, 0, ..., 0)_{\mathbf{B}_t}$$

[Fórmula 23]

$$(\overbrace{s_i(v_{i,1}, ..., v_{i,n_t})}^{n_t}, \overbrace{s_i'(v_{i,1}, ..., v_{i,n_t})}^{n_t}, \overbrace{\sigma_i - \theta_i "m', \theta_i "}^{2}, 0, ..., 0)_{\mathbf{B}_t}$$

13. Un método de procesamiento de firmas de ejecución de un proceso de firma que usa una base B_t y una base B^*_t para cada número entero t = 0, ..., d+1, (d es un número entero de 1 o más), que comprende:

un primer paso de entrada de información de, con un dispositivo de generación de claves (100), toma como entrada de un conjunto de atributos Γ que incluye la información de identificación t y la información de atributo $x^{\rightarrow}_t := (x_{t,i})$ (i = 1, ..., n_t donde n_t es un número entero de 1 o más) para al menos un número entero t = 1, ..., d;

un paso de generación del elemento de clave 0 de, con el dispositivo de generación de claves, generación de un elemento de clave k^*_0 donde un valor δ predeterminado se establece como coeficiente para un vector base $b^*_{0,1}$ de una base B^*_0;

un paso de generación del elemento de clave t de, con el dispositivo de generación de claves, generación de un elemento de clave k^*_t donde $\delta x_{t,i}$ (i = 1, ..., n_t) obtenido multiplicando la información de atributo $x^{\rightarrow}_t$ por el valor δ predeterminado se establece como coeficiente para un vector base $b_{t,i}$ (i = 1, …, n_t) de la base B^*_t, que concierne a cada información de identificación t incluida en el conjunto de atributos Γ introducido en el primer paso de entrada de información;

un paso de generación del elemento de clave d+1 de, con el dispositivo de generación de claves, generación de un elemento de clave $k^*_{d+1,1}$ donde el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{d+1,1}$ de una base B^*_{d+1}, y un elemento de clave $k^*_{d+1,2}$ donde el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{d+1,2}$ de la base B^*_{d+1};

un paso de transmisión de clave de firma de, con el dispositivo de generación de clave, transmisión, a un dispositivo de firmas (200), de una clave de firma sk_Γ que incluye: el elemento de clave k^*_0 generado en el paso

de generación del elemento de clave 0; el elemento de clave k^*_t generado en el paso de generación del elemento de clave t que concierne a cada información de identificación t incluida en el conjunto de atributos Γ; el elemento de clave $k^*_{d+1,1}$ y el elemento de clave $k^*_{d+1,2}$ que se generan en el paso de generación del elemento de clave d+1; y el conjunto de atributos Γ;

un segundo paso de entrada de información de, con el dispositivo de firma, toma como entrada de una variable ρ(i) para cada número entero i = 1, ..., L (L es un número entero de 1 o más), cuya variable ρ(i) es cualquiera de una tupla positiva $(t, \vec{v}_i)$ y una tupla negativa $\neg(t, \vec{v}_i)$ de la información de identificación t (t es cualquier número entero de t = 1,. .., d) y la información de atributo $\vec{v}_i := (v_{i,i'})$ (i' = 1, ..., n_t); una matriz M predeterminada que tiene L filas y r columnas (r es un número entero de 1 o más); y un mensaje m;

un paso de adquisición de clave de firma de, con el dispositivo de firma, adquisición de la clave de firma sk_Γ transmitida en el paso de transmisión de clave de firma;

un paso de cálculo de coeficiente complementario de, con el dispositivo de firma, en base a la variable ρ(i) introducida en el segundo paso de entrada de información y el conjunto de atributos Γ incluido en la clave de firma sk_Γ adquirida en el paso de adquisición de clave de firma, que especifica, entre los números enteros i = 1, ..., L, un conjunto I de un número entero i para el cual la variable ρ(i) es una tupla positiva $(t, \vec{v}_i)$ y con el cual un producto interno de $\vec{v}_i$ de la tupla positiva y $\vec{x}_t$ incluida en el conjunto de atributos Γ indicado por la información de identificación t de la tupla positiva llega a ser 0, y un número entero i para el cual la variable ρ(i) es una tupla negativa $\neg(t, \vec{v}_i)$ y con el cual un producto interno de $\vec{v}_i$ de la tupla negativa y $\vec{x}_t$ incluida en el conjunto de atributos Γ indicado por la información de identificación t de la tupla negativa no llega a ser 0; y de cálculo, concerniente a i incluido en el conjunto I especificado, de un coeficiente complementario α_i con el cual un total de $\alpha_i M_i$ en base a M_i que es un elemento en una fila de orden i de la matriz M introducida en el segundo paso de entrada de información llega a ser un vector $\vec{h}$ predeterminado;

un paso de generación del elemento de firma 0 de, con el dispositivo de firma, generación de un elemento de firma s^*_0 que incluye el elemento de clave k^*_0 incluido en la clave de firma sk_Γ;

un paso de generación del elemento de firma i de, con el dispositivo de firma, generación, para cada número entero i = 1 ..., L, de un elemento de firma s^*_i que incluye $\gamma_i k^*_t$ obtenido multiplicando el elemento de clave k^*_t incluido en la clave de firma sk_Γ por un valor γ_i, estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i$ cuando el número entero i se incluye en el conjunto I especificado en el paso de cálculo de coeficiente complementario y la variable ρ(i) es una tupla positiva $(t, \vec{v}_i)$; estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i/(\vec{v}_i \cdot \vec{x}_t)$ cuando el número entero i está incluido en el conjunto I y la variable ρ(i) es una tupla negativa $\neg(t, \vec{v}_i)$; y estableciendo el valor γ_i para satisfacer $\gamma_i := 0$ cuando el número entero i no está incluido en el conjunto I;

un paso de generación del elemento de firma L+1 de, con el dispositivo de firma, generación de un elemento de firma s^*_{L+1} que incluye una suma del elemento de clave $k^*_{d+1,1}$ incluido en la clave de firma sk_Γ y $m' \cdot k^*_{d+1,2}$ obtenido multiplicando el elemento de clave $k^*_{d+1,2}$ por un valor m' generado usando el mensaje m;

un paso de transmisión de datos de firma de, con el dispositivo de firma, transmisión, al dispositivo de verificación (300), de datos de firma σ que incluyen: el elemento de firma s^*_0 generado en el paso de generación del elemento de firma 0; el elemento de firma s^*_i generado para cada número entero i = 1, ..., L en el paso de generación del elemento de firma i; el elemento de firma s^*_{L+1} generado en el paso de generación del elemento de firma L+1; el mensaje m; la variable ρ(i); y la matriz M;

un paso de adquisición de datos de, con el dispositivo de verificación, adquisición de los datos de firma σ transmitidos por el paso de transmisión de datos de firma;

un paso de generación del elemento de verificación 0 de, con el dispositivo de verificación, generación de un elemento de verificación c_0 estableciendo, como coeficiente para un vector base $b_{0,1}$ de una base B_0, $-s_0 - s_{L+1}$ calculado a partir de un valor $s_0 := \vec{h}' \cdot \vec{f}$ y un valor predeterminado s_{L+1}, el valor $s_0 := \vec{h}' \cdot \vec{f}$ que se genera usando un vector $\vec{f}$ que tiene r partes de elementos, y el vector $\vec{h}$;

un paso de generación del elemento de verificación i de, con el dispositivo de verificación, para cada número entero i = 1, ..., L y usando un vector de columna $\vec{s}^T := (s_1, ..., s_L)^T := M \cdot \vec{f}^T$ generado en base al vector $\vec{f}$ y la matriz M que se incluye en los datos de firma σ adquiridos en el paso de adquisición de datos, y un número predeterminado θ_i para cada número entero i = 1, ..., L, generación de un elemento de verificación c_i, cuando la variable ρ(i) es una tupla positiva $(t, \vec{v}_i)$, estableciendo $s_i + \theta_i v_{i,1}$ como coeficiente para un vector base $b_{t,1}$ de la base B_t indicado por la información de identificación t de la tupla positiva y estableciendo $\theta_i v_{i,i'}$ (i' = 2, ..., n_t) como coeficiente para un vector base $b_{t,i'}$ (i' = 2, ..., n_t), y generación de un elemento de verificación c_i, cuando la variable ρ(i) es una tupla negativa $\neg(t, \vec{v}_i)$, estableciendo $s_i v_{i,i'}$ (i' = 1, ..., n_t) como coeficiente para el vector base $b_{t,i'}$ (i' = 1, ..., n_t) indicado por la información de identificación t de la tupla negativa;

un paso de generación del elemento de verificación L+1 de, con el dispositivo de verificación, generación de un elemento de verificación c_{L+1} estableciendo $s_{L+1} - \theta_{L+1} m'$ calculado a partir del valor predeterminado s_{L+1}, el valor

m', y un valor predeterminado θ_{L+1} como coeficiente para un vector base $b_{d+1,1}$ de una base B_{d+1}, y estableciendo el valor predeterminado θ_{L+1} como coeficiente para un vector base $b_{d+1,2}$; y

un paso de operación de emparejamiento de, con el dispositivo de verificación, verificación de la autenticidad de los datos de firma σ dirigiendo una operación de emparejamiento $\Pi_{i=0}^{L+1}e(c_i, s^*_i)$ para el elemento de verificación c_0 generado en el paso de generación del elemento de verificación 0, el elemento de verificación c_i generado en el paso de generación del elemento de verificación i, el elemento de verificación c_{L+1} generado en el paso de generación del elemento de verificación L+1, y los elementos de firma s^*_0, s^*_i y s^*_{L+1} incluidos en los datos de firma σ.

14. Un programa de procesamiento de firmas que comprende un programa de generación de claves para ejecutar en un dispositivo de generación de claves (100), un programa de firma para ejecutarse en un dispositivo de firmas (200), y un programa de verificación para ejecutarse en un dispositivo de verificación (300), y que sirve para ejecutar un proceso de firma usando una base B_t y una base B^*_t para cada número entero t = 0, ..., d+1 (d es un número entero de 1 o más),

en donde el programa de generación de claves hace que un ordenador (911) ejecute

un primer proceso de entrada de información de toma como entrada de un conjunto de atributos Γ que incluye la información de identificación t y la información de atributo $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t donde n_t es un número entero de 1 o más) para al menos un número entero t = 1, ..., d,

un proceso de generación del elemento de clave 0 de generación de un elemento de clave k^*_0 donde un valor δ predeterminado se establece como coeficiente para un vector base $b^*_{0,1}$ de una base B^*_0,

un proceso de generación del elemento de clave t de generación de un elemento de clave k^*_t donde $\delta x_{t,i}$ (i = 1, ..., n_t) obtenido multiplicando la información de atributo $\vec{x}_t$ por el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{t,i}$ (i = 1, ..., n_t) de la base B^*_t, que concierne a cada información de identificación t incluida en el conjunto de atributos Γ introducido por el primer proceso de entrada de información,

un proceso de generación del elemento de clave d+1 de generación de un elemento de clave $k^*_{d+1,1}$ donde el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{d+1,1}$ de una base B^*_{d+1}, y un elemento de clave $k^*_{d+1,2}$ donde el valor δ predeterminado se establece como coeficiente para un vector base $b^*_{d+1,2}$ de la base B^*_{d+1}, y

un proceso de transmisión de clave de firma de transmisión, a un dispositivo de firma, de una clave de firma sk_Γ que incluye: el elemento de clave k^*_0 generado en el proceso de generación del elemento de clave 0; el elemento de clave k^*_t generado en el proceso de generación del elemento de clave t que concierne a cada información de identificación t incluida en el conjunto de atributos Γ; el elemento de clave $k^*_{d+1,1}$ y el elemento de clave $k^*_{d+1,2}$ que se generan en el proceso de generación del elemento de clave d+1; y el conjunto de atributos Γ,

en donde el programa de firma hace que el ordenador ejecute

un segundo proceso de entrada de información de toma como entrada de una variable ρ(i) para cada número entero i = 1, ..., L (L es un número entero de 1 o más), cuya variable ρ(i) es cualquiera de una tupla positiva (t, $\vec{v}_i$) y una tupla negativa ¬(t, $\vec{v}_i$) de la información de identificación t (t es cualquier número entero de t = 1, ..., d) y la información de atributo $\vec{v}_i := (v_{i,i'})$ (i' = 1, ..., n_t); una matriz M predeterminada que tiene L filas y r columnas (r es un número entero de 1 o más); y un mensaje m,

un proceso de adquisición de clave de firma de adquisición de la clave de firma sk_Γ transmitida en el proceso de transmisión de clave de firma,

un proceso de cálculo de coeficiente complementario de, en base a la variable ρ(i) introducida en el segundo proceso de entrada de información y el conjunto de atributos Γ incluido en la clave de firma sk_Γ adquirida en el proceso de adquisición de clave de firma, especificación, entre los números enteros i = 1, ..., L, de un conjunto I de un número entero i para el cual la variable ρ(i) es una tupla positiva (t, $\vec{v}_i$) y con el cual un producto interno de $\vec{v}_i$ de la tupla positiva y $\vec{x}_t$ incluido en el conjunto de atributos Γ indicado por la información de identificación t de la tupla positiva llega a ser 0, y un número entero i para el cual la variable ρ(i) es una tupla negativa ¬(t, $\vec{v}_i$) y con el cual un producto interno de $\vec{v}_i$ de la tupla negativa y $\vec{x}_t$ incluida en el conjunto de atributos Γ indicada por la información de identificación t de la tupla negativa no llega a ser 0; y de cálculo, concerniente a i incluido en el conjunto I especificado, de un coeficiente complementario α_i con el cual un total de $\alpha_i M_i$ en base a M_i que es un elemento en una fila de orden i de la matriz M introducida en el segundo proceso de entrada de información llega a ser un vector $\vec{h}$ predeterminado,

un proceso de generación del elemento de firma 0 de generación de un elemento de firma s^*_0 que incluye el elemento de clave k^*_0 incluido en la clave de firma sk_Γ,

un proceso de generación del elemento de firma i de generación, para cada número entero i = 1, ..., L, de un elemento de firma s^*_i que incluye $\gamma_i k^*_t$ obtenido multiplicando el elemento de clave k^*_t incluido en la clave de firma sk_Γ por un valor γ_i, estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i$ cuando el número entero i se incluye en el conjunto I especificado en el proceso de cálculo de coeficiente complementario y la variable $\rho(i)$ es una tupla positiva $(t, \vec{v}_i)$; estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i/(\vec{v}_i \cdot \vec{x}_t)$ cuando el número entero i está incluido en el conjunto I y la variable $\rho(i)$ es una tupla negativa $\neg(t, \vec{v}_i)$; y estableciendo el valor γ_i para satisfacer $\gamma_i := 0$ cuando el número entero i no está incluido en el conjunto I,

un proceso de generación del elemento de firma L+1 de generación de un elemento de firma s^*_{L+1} que incluye una suma del elemento de clave $k^*_{d+1,1}$ incluido en la clave de firma sk_Γ y $m' \cdot k^*_{d+1,2}$ obtenido multiplicando el elemento de clave $k^*_{d+1,2}$ por un valor m' generado usando el mensaje m, y

un proceso de transmisión de datos de firma de transmisión, a un dispositivo de verificación, de datos de firma σ que incluyen: el elemento de firma s^*_0 generado en el proceso de generación del elemento de firma 0; el elemento de firma s^*_i generado para cada número entero i = 1, ..., L en el proceso de generación del elemento de firma i; el elemento de firma s^*_{L+1} generado en el proceso de generación del elemento de firma L+1; el mensaje m; la variable $\rho(i)$; y la matriz M, y

en donde el programa de verificación hace al ordenador ejecutar

un proceso de adquisición de datos de adquisición de los datos de firma σ transmitidos en el proceso de transmisión de datos de firma,

un proceso de generación del elemento de verificación 0 de generación de un elemento de verificación c_0 estableciendo, como coeficiente para un vector base $b_{0,1}$ de una base B_0, $-s_0 - s_{L+1}$ calculado a partir de un valor $s_0 := \vec{h} \cdot \vec{f}$ y un valor predeterminado s_{L+1}, el valor $s_0 := \vec{h} \cdot \vec{f}$ que se genera usando un vector $\vec{f}$ que tiene r partes de elementos, y el vector $\vec{h}$,

un proceso de generación del elemento de verificación i de, para cada número entero i = 1, ..., L y usando un vector de columna $\vec{s}^T := (s_1, ..., s_L)^T := M \cdot \vec{f}^T$ generado en base al vector $\vec{f}$ y la matriz M que se incluye en los datos de firma σ adquiridos en el proceso de adquisición de datos, y un número predeterminado θ_i para cada número entero i = 1, ..., L, generación de un elemento de verificación c_i, cuando la variable $\rho(i)$ es una tupla positiva $(t, \vec{v}_i)$, estableciendo $s_i + \theta_i v_{i,1}$ como coeficiente para un vector base $b_{t,1}$ de la base B_t indicado por la información de identificación t de la tupla positiva y estableciendo $\theta_i v_{i,i'}$ (i' = 2, ..., n_t) como coeficiente para un vector base $b_{t,i'}$ (i' = 2, ..., n_t), y generación de un elemento de verificación c_i, cuando la variable $\rho(i)$ es una tupla negativa $\neg(t, \vec{v}_i)$ estableciendo $s_i v_{i,i'}$ (i' = 1, ..., n_t) como coeficiente para el vector base $b_{i,i'}$ (i' = 1, ..., n_t) indicado por la información de identificación t de la tupla negativa,

un proceso de generación del elemento de verificación L+1 de generación de un elemento de verificación c_{L+1} estableciendo $s_{L+1} - \theta_{L+1} m'$ calculado a partir del valor predeterminado s_{L+1}, el valor m', y un valor predeterminado θ_{L+1} como coeficiente para un vector base $b_{d+1,1}$ de una base B_{d+1}, y estableciendo el valor predeterminado θ_{L+1} como coeficiente para un vector base $b_{d+1,2}$, y

un proceso de operación de emparejamiento de verificación de la autenticidad de los datos de firma σ dirigiendo una operación de emparejamiento $\Pi_{i=0}^{L+1} e(c_i, s^*_i)$ para el elemento de verificación c_0 generado en el proceso de generación del elemento de verificación 0, el elemento de verificación c_i generado en el proceso de generación del elemento de verificación i, el elemento de verificación c_{L+1} generado en el proceso de generación del elemento de verificación L+1, y los elementos de firma s^*_0, s^*_i, y s^*_{L+1} incluidos en los datos de firma σ.

15. Un método de procesamiento de firmas de ejecución de un proceso de firma que usa una base B_t y una base B^*_t para al menos un número entero t = 0, ..., d (d es un número entero de 1 o más), el método de procesamiento de firmas que incluye:

un primer paso de entrada de información de, con al menos un dispositivo de generación de claves entre d unidades de dispositivos de generación de claves (100), toma como entrada de la información de atributo $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t) para un número entero t entre t = 1, ..., d que se predetermina para cada uno de los dispositivos de generación de claves;

un paso de generación del elemento de clave de, con el al menos un dispositivo de generación de claves, para el número entero t y cada número entero j = 1, 2, generación de un elemento de clave $k^*_{t,j}$ que incluye un vector indicado en la Fórmula 24 en base a la información de atributo $\vec{x}_t$ introducida en el primer paso de entrada de información, un valor δ_j predeterminado, y un vector base $b^*_{t,j}$ (i = 1, …, $2n_t$) de una base B^*_t;

un paso de transmisión de clave de firma de, con el al menos un dispositivo de generación de claves, transmisión, a un dispositivo de firmas (200), de una clave de firma usk que incluye: el elemento de clave $k^*_{t,j}$ generado en el paso de generación del elemento de clave; y la información de atributo $\vec{x}_t$;

un segundo paso de entrada de información de, con el dispositivo de firma, toma como entrada de una variable ρ(i) para cada número entero i = 1, ..., L (L es un número entero de 1 o más), cuya variable ρ(i) es cualquiera de una tupla positiva $(t, v^{\rightarrow}_i)$ y una tupla negativa $\neg(t, v^{\rightarrow}_i)$ de la información de identificación t (t es cualquier número entero de t = 1, …, d) y la información de atributo $v^{\rightarrow}_i := (v_{i,i'})$ (i' = 1, ..., n_t); una matriz M predeterminada que tiene L filas y r columnas (r es un número entero de 1 o más); y un mensaje m;

un paso de adquisición de clave de firma de, con el dispositivo de firma, adquisición de la clave de firma usk transmitida en el paso de transmisión de clave de firma del al menos un dispositivo de generación de claves entre las d unidades de dispositivos de generación de claves;

un paso de cálculo de coeficiente complementario de, con el dispositivo de firma y en base a la variable ρ(i) introducida en el segundo paso de entrada de información y la información de atributo $x^{\rightarrow}_t$ incluida en la clave de firma usk adquirida en el paso de adquisición de clave de firma, especificación, entre los números enteros i = 1, ..., L, de un conjunto I de un número entero i para el cual la variable ρ(i) es una tupla positiva $(t, v^{\rightarrow}_i)$, la clave de firma usk que incluye $x^{\rightarrow}_t$ indicado por la información de identificación t de la tupla positiva que se adquiere en el paso de adquisición de clave de firma, y con el cual un producto interno de $v^{\rightarrow}_i$ de la tupla positiva y la información de atributo $x^{\rightarrow}_t$ indicada por la información de identificación t de la tupla positiva llega a ser 0, y un número entero i para el cual la variable ρ(i) es una tupla negativa $\neg(t, v^{\rightarrow}_i)$, la clave de firma usk que incluye $x^{\rightarrow}_t$ indicado por la información de identificación t de la tupla negativa que se adquiere en el paso de adquisición de clave de firma, y con el cual un producto interno de $v^{\rightarrow}_i$ de la tupla negativa y la información de atributo $x^{\rightarrow}_t$ indicada por la información de identificación t de la tupla negativa no llega a ser 0, y cálculo, concerniente a i incluido en el conjunto I especificado, de un coeficiente complementario α_i con el cual un total de $\alpha_i M_i$ en base a M_i que es un elemento en una fila de orden i de la matriz M introducida en el segundo paso de entrada de información llega a ser un vector $h^{\rightarrow}$ predeterminado;

un paso de generación del elemento de firma de, con el dispositivo de firma, generación, para cada número entero i = 1 ..., L, de un elemento de firma s^*_i que incluye un vector indicado en la Fórmula 25 usando el vector base $b^*_{t,i}$ (i = $2n_t$+1, $2n_t$+2) de la base B^*_t, en base a un elemento de clave $k^*_{t,1}$ y un elemento de clave $k^*_{t,2}$ incluidos en la clave de firma usk, los valores predeterminados ξ_1, E y μ, y un valor m' calculado a partir del mensaje m, estableciendo un valor γ_i para satisfacer $\gamma_i := \alpha_i$ cuando el número entero i está incluido en el conjunto I especificado en el paso de cálculo de coeficiente complementario y la variable ρ(i) es una tupla positiva $(t, v^{\rightarrow}_i)$, estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i/(v_i \cdot x_t)$ cuando el número entero i está incluido en el conjunto I y la variable ρ(i) es una tupla negativa $\neg(t, v^{\rightarrow}_i)$; y estableciendo el valor γ_i para satisfacer $\gamma_i := 0$ cuando el número entero i no está incluido en el conjunto I;

un paso de transmisión de datos de firma de, con el dispositivo de firma, transmisión, al dispositivo de verificación (300), de datos de firma σ que incluyen: el elemento de firma s^*_i generado para cada número entero i = 1, ..., L por en el paso de generación de elemento de firma; el mensaje m; la variable ρ(i); y la matriz M;

un paso de adquisición de datos de, con el dispositivo verificación, adquisición de los datos de firma σ transmitidos en el paso de transmisión de datos de firma;

un paso de generación de vector de, con el dispositivo verificación, generación de un vector de columna $s^{\rightarrow T} := (s_1, ..., s_L)^T := M \cdot f^{\rightarrow T}$ en base a un vector $f^{\rightarrow T}$ que tiene r partes de elementos y la matriz M incluida en los datos de firma σ adquiridos en el paso de adquisición de datos, y generación de un vector de columna $(s^{\rightarrow'})^T := (s_1', ..., s_L')^T := M \cdot (f^{\rightarrow''})^T$ en base a la matriz M y a un vector $f^{\rightarrow''}$ que tiene r partes de elementos y que satisface $s_0 = h^{\rightarrow} \cdot (f^{\rightarrow''})^T$ donde $s_0 = h^{\rightarrow} \cdot f^{\rightarrow T}$;

un paso de generación de elemento de verificación de, con el dispositivo verificación, para cada número entero i = 1, ..., L y en base al vector de columna $s^{\rightarrow T}$ y al vector de columna $(s^{\rightarrow'})^T$ que se generan en el paso de generación de vector, y los valores predeterminados θ_i, θ_i', θ_i'', y σ_i para cada número entero i = 1, ..., L, generación de un elemento de verificación c_i que incluye un vector indicado en la Fórmula 26, cuando la variable ρ(i) es una tupla positiva $(t, v^{\rightarrow}_i)$, usando un vector base $b_{t,i'}$ (i' = 1, …, $2n_t$+2) de la base B_t indicada por la información de identificación t de la tupla positiva, y generación de un elemento de verificación c_i que incluye un vector indicado en la Fórmula 27, cuando la variable ρ(i) es una tupla negativa $\neg(t, v^{\rightarrow}_i)$, usando un vector base $b_{t,i}$ (i' = 1, …, $2n_t$+2) indicado por la información de identificación t de la tupla negativa; y

un paso de operación de emparejamiento de, con el dispositivo verificación, verificación de la autenticidad de los datos de firma σ dirigiendo una operación de emparejamiento $\Pi_{i=1}{}^{L} e(c_i, s^*_i)$ para el elemento de verificación c_i generado en el paso de generación de elemento de verificación y el elemento de firma s^*_i incluido en los datos de firma σ.

[Fórmula 24]

$$(\overbrace{(\delta_j + 1)(x_{t,1}, ..., x_{t,n_t})}^{n_t}, \overbrace{-\delta_j (x_{t,1}, ..., x_{t,n_t})}^{n_t}, 0, ..., 0)_{\mathbf{B}^*_t}$$

[Fórmula 25]

$$\gamma_i \cdot (\xi_1 k^*_{t,1} + (E - \xi_1) k^*_{t,2}) + (\mu b^*_{t,2n_t+1}) + m'(\mu b^*_{t,2n_t+2})$$

[Fórmula 26]

$$(\overbrace{s_i + \theta_i v_{i,1}, \theta_i v_{i,2}, ..., \theta_i v_{i,n_t}}^{n_t}, \overbrace{s_i' + \theta_i' v_{i,1}, \theta_i' v_{i,2}, ..., \theta_i' v_{i,n_t}}^{n_t}, \overbrace{\sigma_i - \theta_i "m', \theta_i "}^{2}, 0, ..., 0)_{\mathbf{B}_t}$$

[Fórmula 27]

$$(\overbrace{s_i(v_{i,1}, ..., v_{i,n_t})}^{n_t}, \overbrace{s_i'(v_{i,1}, ..., v_{i,n_t})}^{n_t}, \overbrace{\sigma_i - \theta_i "m', \theta_i "}^{2}, 0, ..., 0)_{\mathbf{B}_t}$$

16. Un programa de procesamiento de firmas que comprende un programa de generación de claves para ejecutarse en d (d es un número entero de 1 o más) unidades de dispositivos de generación de claves (100), un programa de firma para ejecutarse en un dispositivo de firmas (200), y un programa de verificación para ejecutarse en un dispositivo de verificación (300), y que sirven para ejecutar un proceso de firma usando una base B_t y base B^*_t para al menos un número entero t = 0, ..., d,

en donde el programa de generación de claves hace que un ordenador (911) ejecute

un primer proceso de entrada de información de toma como entrada la información de atributo $\vec{x}_t := (x_{t,i})$ (i = 1, ..., n_t) para un número entero t entre los números enteros t = 1, ..., d que se predetermina para cada uno de los dispositivos de generación de claves,

un proceso de generación de elemento de clave de, para el número entero t y cada número entero j = 1, 2, generación de un elemento de clave $k^*_{t,j}$ que incluye un vector indicado en la Fórmula 28 en base a la información de atributo $\vec{x}_t$ introducida en el primer proceso de entrada de información, un valor δ_j predeterminado, y un vector base $b^*_{t,i}$ (i = 1, …, $2n_t$) de una base B^*_t, y

un proceso de transmisión de clave de firma de transmisión, a un dispositivo de firmas, de una clave de firma usk que incluye: el elemento de clave $k^*_{t,j}$ generado en el proceso de generación de elemento de clave; y la información de atributo $\vec{x}_t$,

en donde el programa de firma hace que el ordenador ejecute

un segundo proceso de entrada de información de toma como entrada de una variable ρ(i) para cada número entero i = 1, ..., L (L es un número entero de 1 o más), cuya variable ρ(i) es cualquiera de una tupla positiva (t, $\vec{v}_i$) y una tupla negativa ¬(t, $\vec{v}_i$) de la información de identificación t (t es cualquier número entero de t = 1, …, d) y la información de atributo $\vec{v}_i := (v_{i,i'})$ (i' = 1, ..., n_t); una matriz M predeterminada que tiene L filas y r columnas (r es un número entero de 1 o más); y un mensaje m,

un proceso de adquisición de clave de firma de adquisición de la clave de firma usk transmitida en el proceso de transmisión de clave de firma del al menos un dispositivo de generación de claves entre las d unidades de dispositivos de generación de claves,

un proceso de cálculo de coeficiente complementario de, en base a la variable ρ(i) introducida en el segundo proceso de entrada de información y la información de atributo x_t incluida en la clave de firma usk adquirida en el proceso de adquisición de clave de firma, especificación, entre los números enteros i = 1, ..., L, de un conjunto I de un número entero i para el cual la variable ρ(i) es una tupla positiva (t, $\vec{v}_i$), la clave de firma usk que incluye $\vec{x}_t$ indicado por la información de identificación t de la tupla positiva que se adquiere en el proceso de adquisición de clave de firma, y con el cual un producto interno de $\vec{v}_i$ de la tupla positiva y la información de atributo $\vec{x}_t$ indicada por la información de identificación t de la tupla positiva llega a ser 0, y un número entero i para el cual la variable ρ(i) es una tupla negativa ¬(t, $\vec{v}_i$), la clave de firma usk que incluye $\vec{x}_t$ indicada por la información de identificación t de la tupla negativa que se adquiere en el proceso de adquisición de clave de firma, y con el cual un producto interno de $\vec{v}_i$ de la tupla negativa y la información de atributo $\vec{x}_t$ indicada por la información de identificación t de la tupla negativa no llega a ser 0; y cálculo, concerniente a i incluido en el

conjunto I especificado, de un coeficiente complementario α_i con el cual un total de $\alpha_i M_i$ en base a M_i que es un elemento en una fila de orden i de la matriz M introducida en el segundo proceso de entrada de información llega a ser un vector $h^{\rightarrow}$ predeterminado,

un proceso de generación de elemento de firma de generación, para cada número entero i = 1, ..., L, de un elemento de firma s^*_i incluyendo un vector indicado en la Fórmula 29 usando el vector base $b^*_{t,i}$ ($i = 2n_t+1, 2n_t+2$) de la base B^*_t, en base a un elemento de clave $k^*_{t,1}$ y un elemento de clave $k^*_{t,2}$ incluidos en la clave de firma usk, los valores predeterminados ξ_1, E y μ, y un valor m' calculado a partir del mensaje m, estableciendo un valor γ_i para satisfacer $\gamma_i := \alpha_i$ cuando el número entero i está incluido en el conjunto I especificado en el proceso de cálculo de coeficiente complementario y la variable $\rho(i)$ es una tupla positiva $(t, v^{\rightarrow}_i)$; estableciendo el valor γ_i para satisfacer $\gamma_i := \alpha_i/(v^{\rightarrow}_i \cdot x^{\rightarrow}_t)$ cuando el número entero i está incluido en el conjunto I y la variable $\rho(i)$ es una tupla negativa $\neg(t, v^{\rightarrow}_i)$; y estableciendo el valor γ_i para satisfacer $\gamma_i := 0$ cuando el número entero i no está incluido en el conjunto I, y

un proceso de transmisión de datos de firma de transmisión, al dispositivo de verificación, de datos de firma σ que incluyen: el elemento de firma s^*_i generado para cada número entero i = 1, ..., L en el proceso de generación de elemento de firma; el mensaje m; la variable $\rho(i)$; y la matriz M, y

en donde el programa de verificación hace que el ordenador ejecute

un proceso de adquisición de datos de adquisición de los datos de firma σ transmitidos en el proceso de transmisión de datos de firma,

un proceso de generación de vector de generación de un vector de columna $s^{\rightarrow T} := (s_1, ..., s_L)^T := M \cdot f^{\rightarrow T}$ en base a un vector $f^{\rightarrow}$ que tiene r partes de elementos y la matriz M incluida en los datos de firma σ adquiridos en el proceso de adquisición de datos, y generación de un vector de columna $(s^{\rightarrow'})^T := (s_1', ..., s_L')^T := M \cdot (f^{\rightarrow'})^T$ en base a la matriz M y a un vector $f^{\rightarrow'}$ que tiene r partes de elementos y que satisface $s_0 = h^{\rightarrow} \cdot (f^{\rightarrow'})^T$ donde $s_0 = h^{\rightarrow} \cdot f^{\rightarrow T}$,

un proceso de generación de elemento de verificación de, para cada número entero i = 1, ..., L y en base al vector de columna $s^{\rightarrow T}$ y al vector de columna $(s^{\rightarrow'})^T$ que se generan en el proceso de generación de vector, y los valores predeterminados θ_i, θ_i', θ_i'', y σ_i para cada número entero i = 1, ..., L, generación de un elemento de verificación c_i que incluye un vector indicado en la Fórmula 30, cuando la variable $\rho(i)$ es una tupla positiva $(t, v^{\rightarrow}_i)$, usando un vector base $b_{t,i'}$ ($i' = 1, \ldots, 2n_t+2$) de la base B_t indicada por la información de identificación t de la tupla positiva, y generación de un elemento de verificación c_i que incluye un vector indicado en la Fórmula 31, cuando la variable $\rho(i)$ es una tupla negativa $\neg(t, v^{\rightarrow}_i)$, usando un vector base $b_{t,i}$ ($i = 1, \ldots, 2n_t+2$) indicado por la información de identificación t de la tupla negativa, y

un proceso de operación de emparejamiento de verificación de la autenticidad de los datos de firma σ dirigiendo una operación de emparejamiento $\Pi_{i=1}{}^{L} e(c_i, s^*_i)$ para el elemento de verificación c_i generado en el proceso de generación de elemento de verificación, y el elemento de firma s^*_i incluido en los datos de firma σ.

[Fórmula 28]

$$(\overbrace{(\delta_j+1)(x_{t,1},...,x_{t,n_t})}^{n_t},\overbrace{-\delta_j(x_{t,1},...,x_{t,n_t})}^{n_t},0,...,0)_{\mathbf{B}^*_t}$$

[Fórmula 29]

$$\gamma_i \cdot (\xi_1 k^*_{t,1} + (E-\xi_1)k^*_{t,2}) + (\mu b^*_{t,2n_t+1}) + m'(\mu b^*_{t,2n_t+2})$$

[Fórmula 30]

$$(\overbrace{s_i+\theta_i v_{i,1}, \theta_i v_{i,2}, ..., \theta_i v_{i,n_t}}^{n_t}, \overbrace{s_i'+\theta_i' v_{i,1}, \theta_i' v_{i,2}, ..., \theta_i' v_{i,n_t}}^{n_t},$$
$$\overbrace{\sigma_i - \theta_i'' m', \theta_i''}^{2}, 0, ..., 0)_{\mathbf{B}_t}$$

[Fórmula 31]

$$(\overbrace{s_i(v_{i,1},\ldots,v_{i,n_t})}^{n_t},\overbrace{s_i'(v_{i,1},\ldots,v_{i,n_t})}^{n_t},\overbrace{\sigma_i-\theta_i''m',\theta_i''}^{2},0,\ldots,0)_{\mathbf{B}_t}$$

Fig. 1

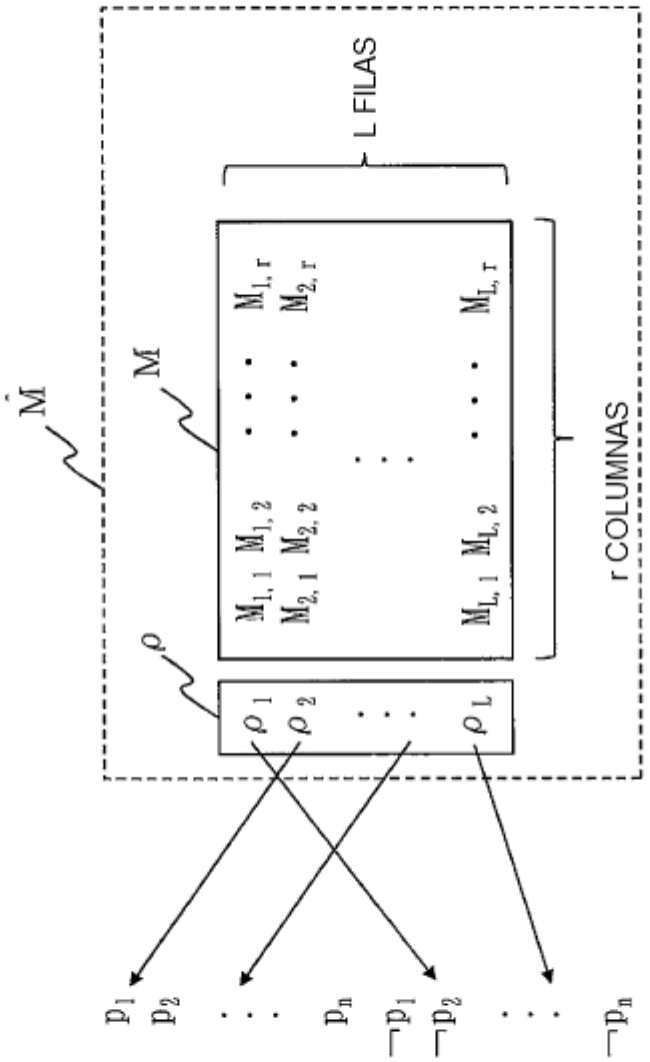

M̂
M
L FILAS
r COLUMNAS
ρ
ρ 1
ρ 2
ρ L
M1, 1 M1, 2 M1, r
M2, 1 M2, 2 M2, r
ML, 1 ML, 2 ML, r
p1
p2
pn
¬p1
¬p2
¬pn

Fig. 2

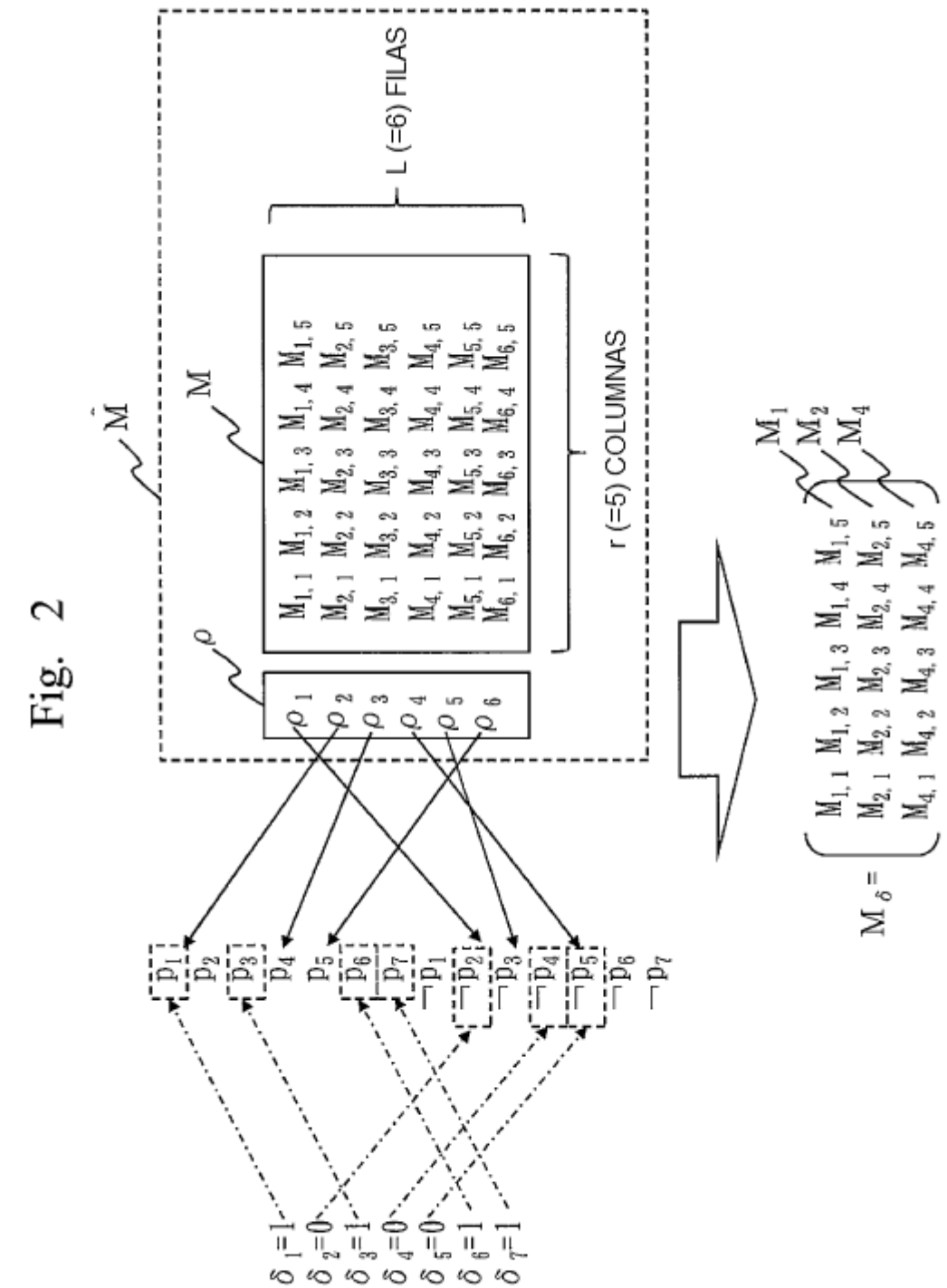

M̂
M
L (=6) FILAS
r (=5) COLUMNAS
ρ
ρ 1 ρ 2 ρ 3 ρ 4 ρ 5 ρ 6
p1 p2 p3 p4 p5 p6 p7
¬p1 ¬p2 ¬p3 ¬p4 ¬p5 ¬p6 ¬p7
δ1=1 δ2=0 δ3=1 δ4=0 δ5=0 δ6=1 δ7=1
M1 M2 M4
Mδ=

Fig. 3

$$s_0 = \begin{pmatrix} f_1 \\ \cdot \\ \cdot \\ \cdot \\ f_r \end{pmatrix} \begin{bmatrix} 1, \ldots, 1 \end{bmatrix} \quad \text{(r COLUMNAS)} = \sum_{k=1}^{r} f_k$$

Fig. 4

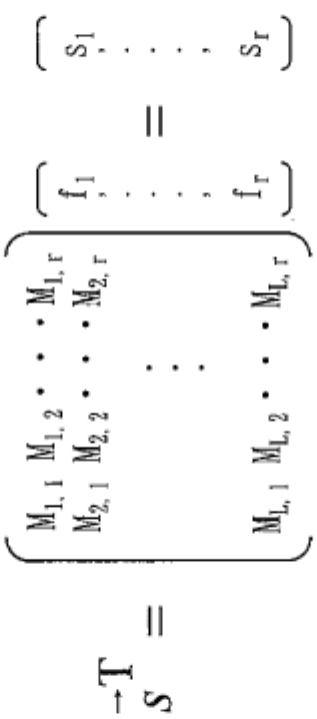

$\vec{S} = \vec{T}$
$\begin{pmatrix} M_{1,1} & M_{1,2} & \cdots & M_{1,r} \\ M_{2,1} & M_{2,2} & \cdots & M_{2,r} \\ & & \ddots & \\ M_{L,1} & M_{L,2} & \cdots & M_{L,r} \end{pmatrix}$
$\begin{pmatrix} f_1 \\ \cdot \\ \cdot \\ \cdot \\ f_r \end{pmatrix}$
$=$
$\begin{pmatrix} S_1 \\ \cdot \\ \cdot \\ \cdot \\ S_r \end{pmatrix}$

Fig. 5

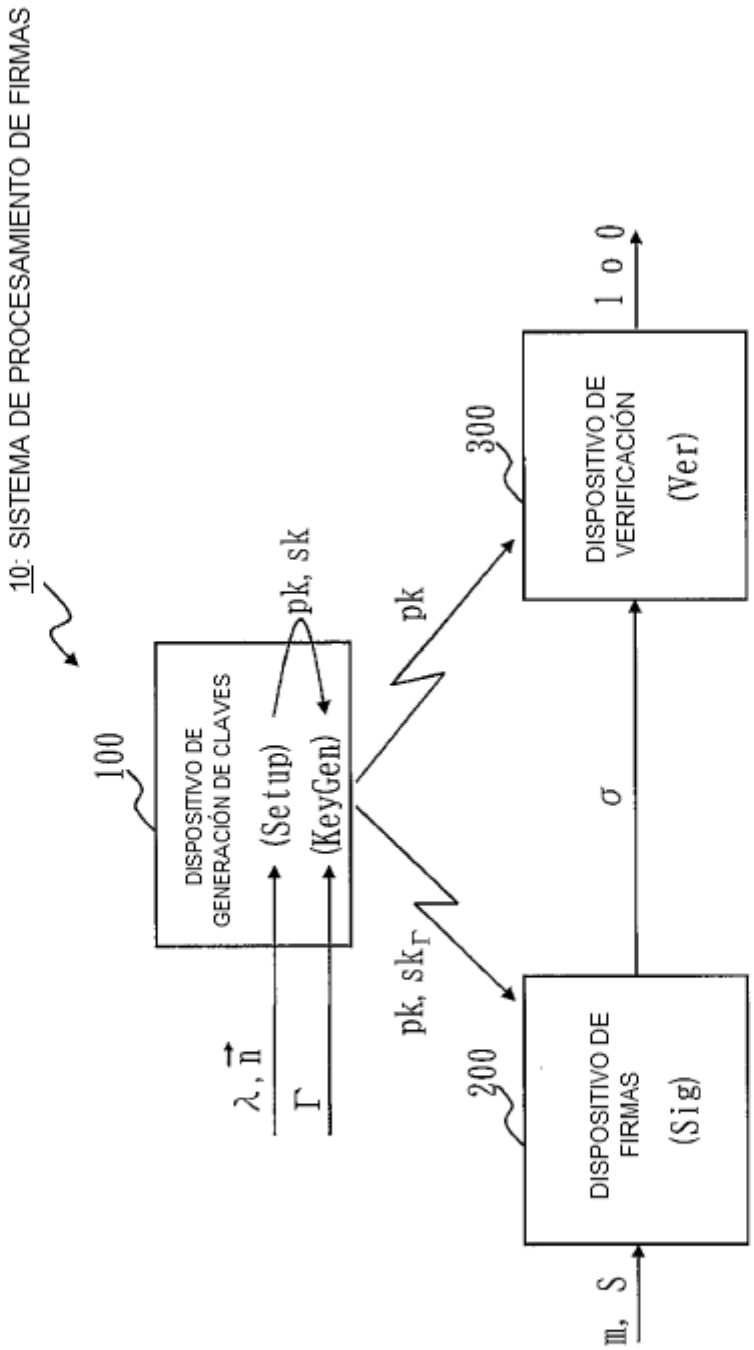

10: SISTEMA DE PROCESAMIENTO DE FIRMAS
100
DISPOSITIVO DE GENERACIÓN DE CLAVES
(Setup)
(KeyGen)
pk, sk
λ, n
Γ
pk
pk, skΓ
200
DISPOSITIVO DE FIRMAS
(Sig)
m, S
σ
300
DISPOSITIVO DE VERIFICACIÓN
(Ver)
1 o 0

Fig. 6

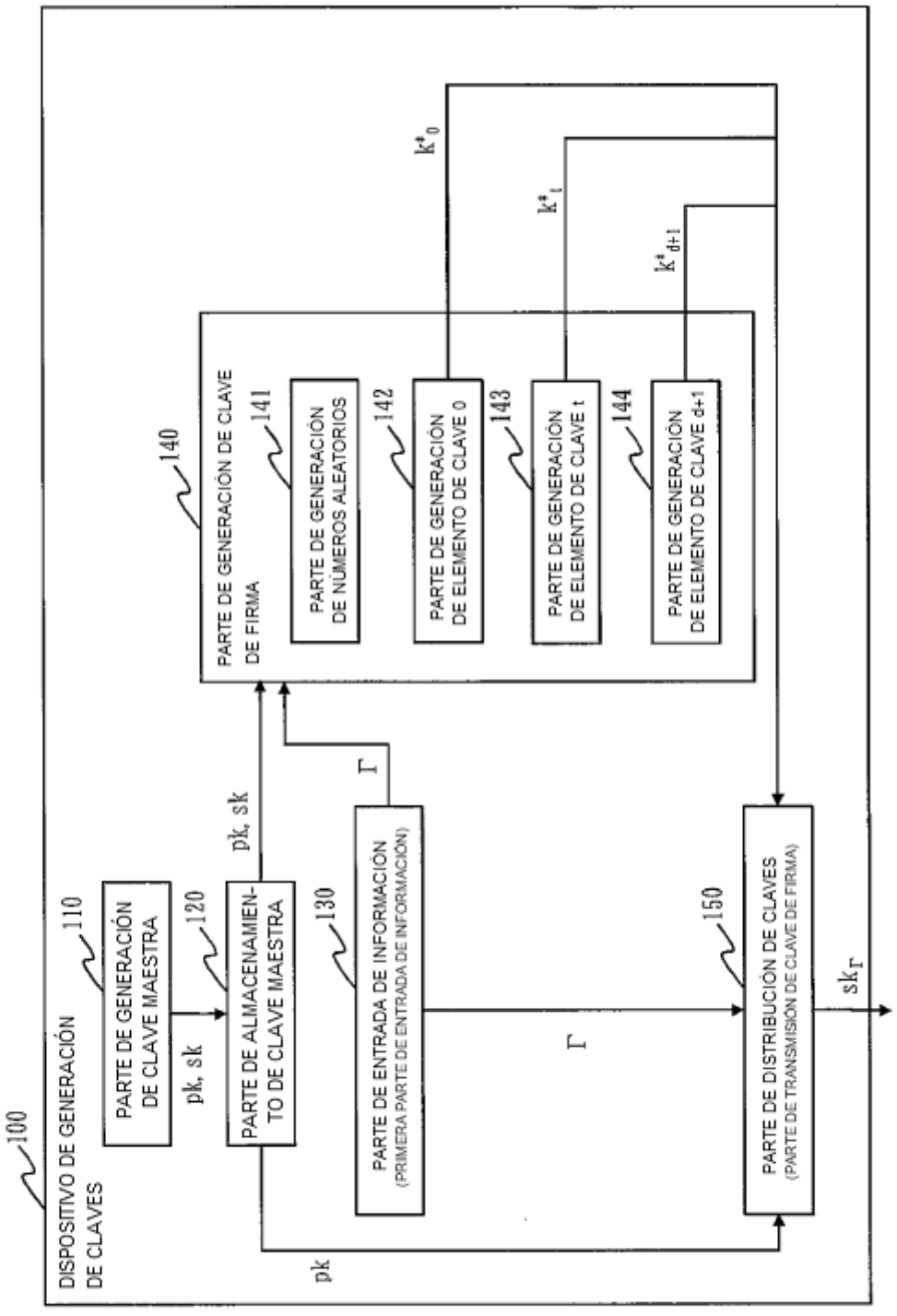

100
DISPOSITIVO DE GENERACIÓN DE CLAVES
110
PARTE DE GENERACIÓN DE CLAVE MAESTRA
pk, sk
120
PARTE DE ALMACENAMIENTO DE CLAVE MAESTRA
pk, sk
130
PARTE DE ENTRADA DE INFORMACIÓN
(PRIMERA PARTE DE ENTRADA DE INFORMACIÓN)
Γ
140
PARTE DE GENERACIÓN DE CLAVE DE FIRMA
141
PARTE DE GENERACIÓN DE NÚMEROS ALEATORIOS
142
PARTE DE GENERACIÓN DE ELEMENTO DE CLAVE 0
143
PARTE DE GENERACIÓN DE ELEMENTO DE CLAVE t
144
PARTE DE GENERACIÓN DE ELEMENTO DE CLAVE d+1
k^*_0
k^*_t
k^*_{d+1}
150
PARTE DE DISTRIBUCIÓN DE CLAVES
(PARTE DE TRANSMISIÓN DE CLAVE DE FIRMA)
Γ
sk_Γ
pk

Fig. 7

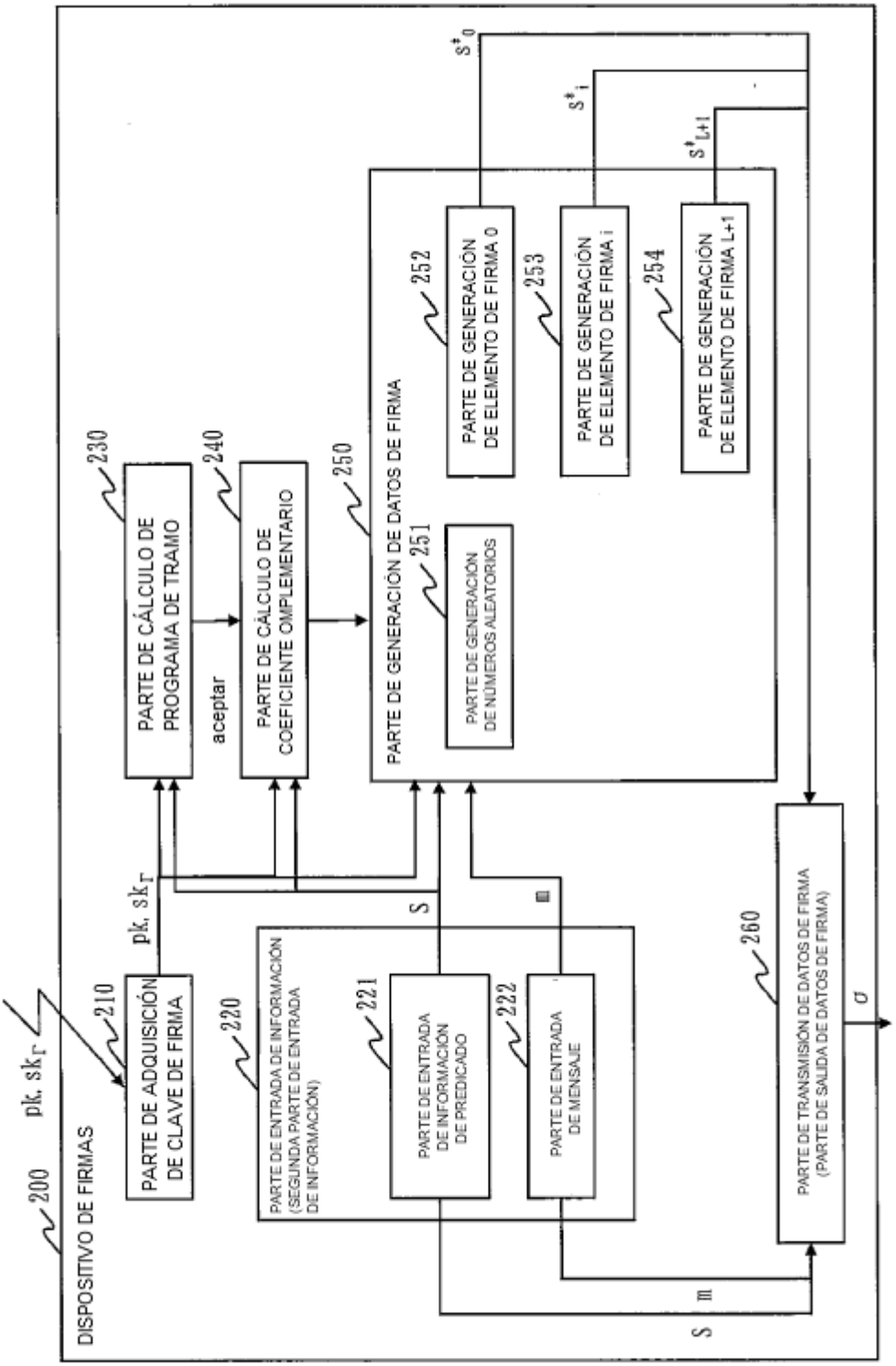

DISPOSITIVO DE FIRMAS
200
pk, sk_Γ
PARTE DE ADQUISICIÓN DE CLAVE DE FIRMA
210
PARTE DE CÁLCULO DE PROGRAMA DE TRAMO
230
aceptar
PARTE DE CÁLCULO DE COEFICIENTE OMPLEMENTARIO
240
PARTE DE GENERACIÓN DE DATOS DE FIRMA
250
PARTE DE GENERACIÓN DE NÚMEROS ALEATORIOS
251
PARTE DE GENERACIÓN DE ELEMENTO DE FIRMA 0
252
PARTE DE GENERACIÓN DE ELEMENTO DE FIRMA i
253
PARTE DE GENERACIÓN DE ELEMENTO DE FIRMA L+1
254
PARTE DE ENTRADA DE INFORMACIÓN (SEGUNDA PARTE DE ENTRADA DE INFORMACIÓN)
220
PARTE DE ENTRADA DE INFORMACIÓN DE PREDICADO
221
PARTE DE ENTRADA DE MENSAJE
222
PARTE DE TRANSMISIÓN DE DATOS DE FIRMA (PARTE DE SALIDA DE DATOS DE FIRMA)
260
pk, sk_Γ
S
m
S
m
σ
s⁺0
s⁺i
s⁺L+1

Fig. 8

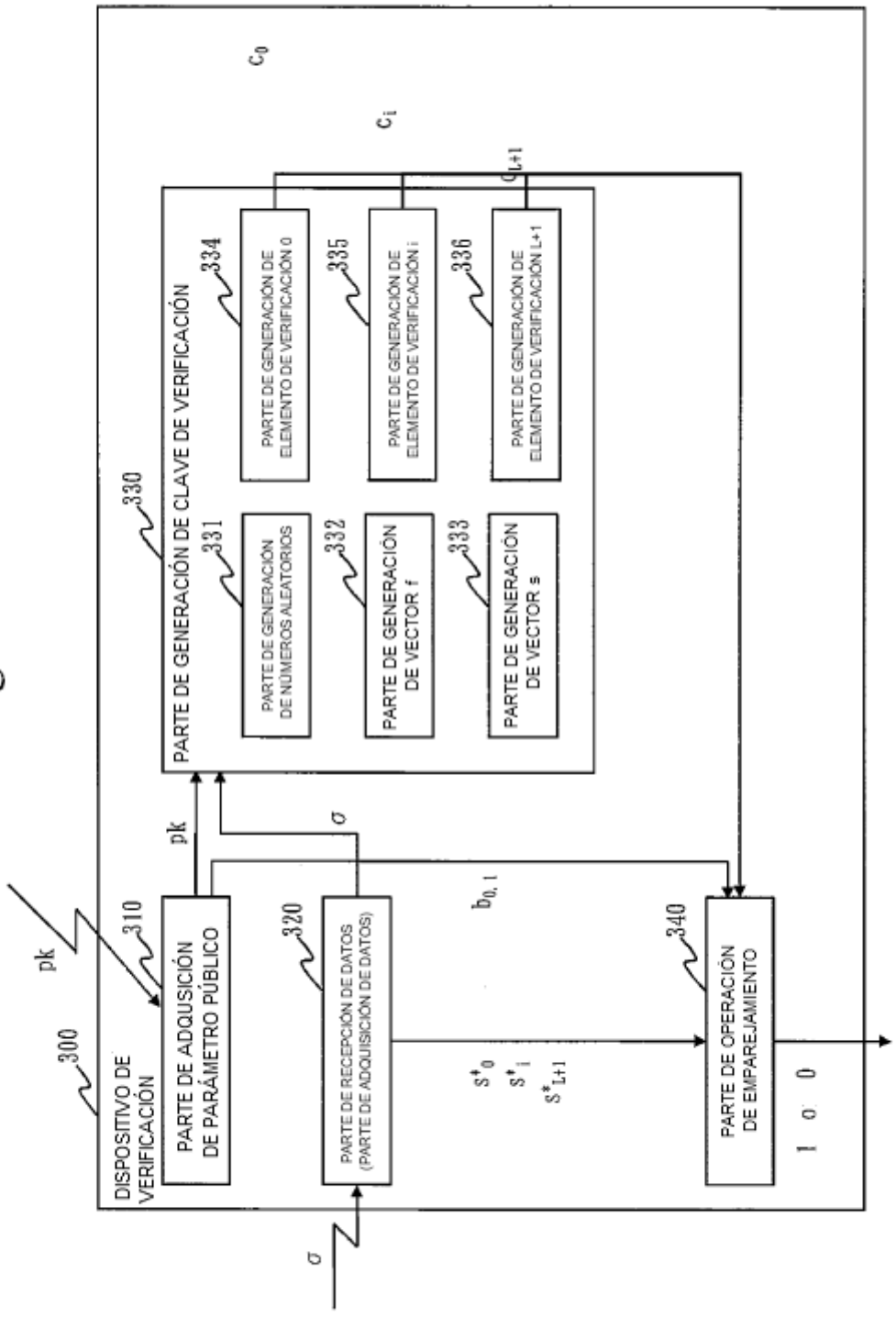

DISPOSITIVO DE VERIFICACIÓN
300
PARTE DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
310
PARTE DE RECEPCIÓN DE DATOS (PARTE DE ADQUISICIÓN DE DATOS)
320
PARTE DE GENERACIÓN DE CLAVE DE VERIFICACIÓN
330
PARTE DE GENERACIÓN DE NÚMEROS ALEATORIOS
331
PARTE DE GENERACIÓN DE VECTOR f
332
PARTE DE GENERACIÓN DE VECTOR s
333
PARTE DE GENERACIÓN DE ELEMENTO DE VERIFICACIÓN 0
334
PARTE DE GENERACIÓN DE ELEMENTO DE VERIFICACIÓN i
335
PARTE DE GENERACIÓN DE ELEMENTO DE VERIFICACIÓN L+1
336
PARTE DE OPERACIÓN DE EMPAREJAMIENTO
340
pk
pk
σ
σ
$b_{0,1}$
s^*_0
s^*_i
s^*_{L+1}
c_0
c_i
c_{L+1}
1 o 0

Fig. 9

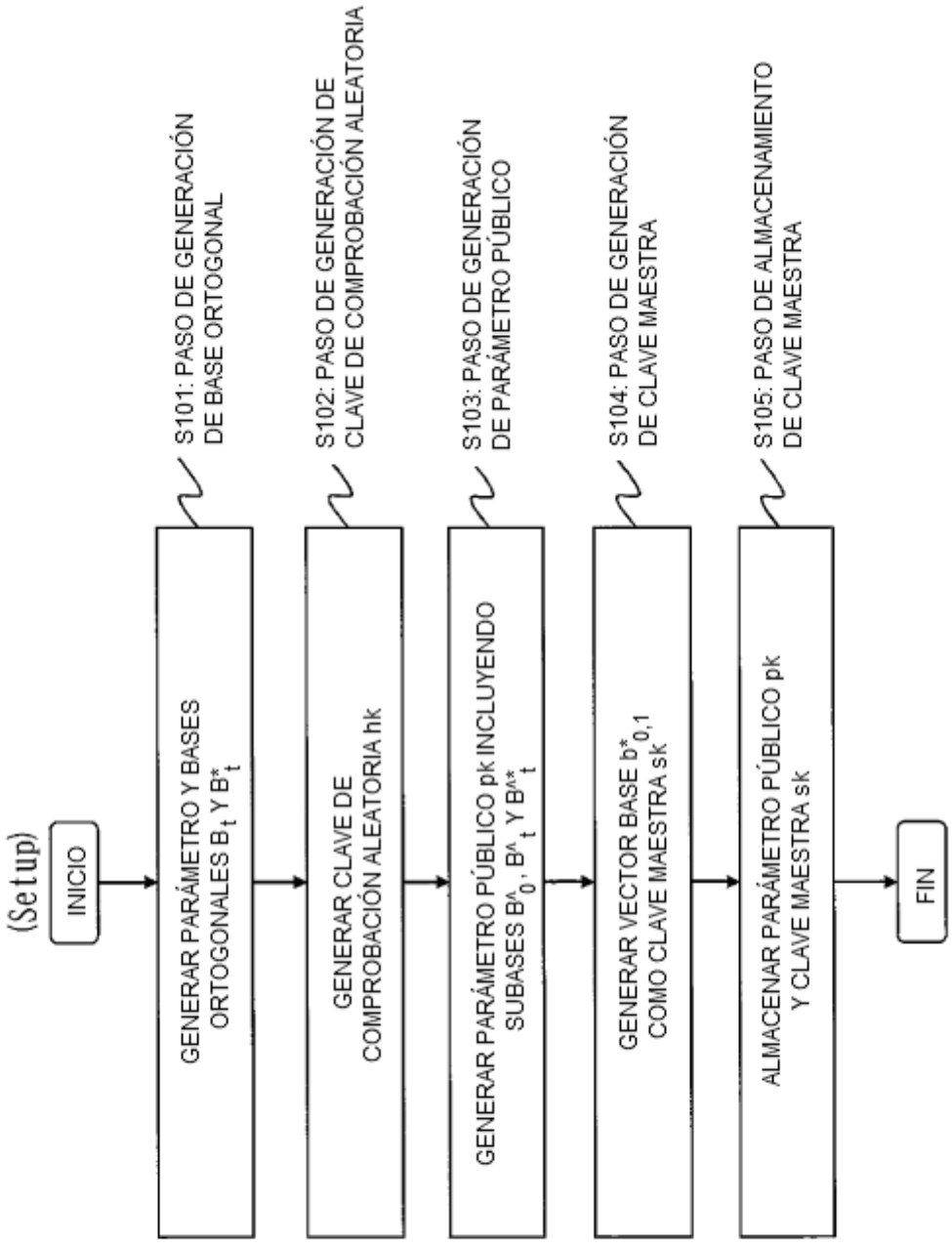

(Setup)
INICIO
GENERAR PARÁMETRO Y BASES ORTOGONALES B_t Y B^*_t
S101: PASO DE GENERACIÓN DE BASE ORTOGONAL
GENERAR CLAVE DE COMPROBACIÓN ALEATORIA hk
S102: PASO DE GENERACIÓN DE CLAVE DE COMPROBACIÓN ALEATORIA
GENERAR PARÁMETRO PÚBLICO pk INCLUYENDO SUBASES $B^\wedge_0$, $B^\wedge_t$ Y $B^{\wedge *}_t$
S103: PASO DE GENERACIÓN DE PARÁMETRO PÚBLICO
GENERAR VECTOR BASE $b^*_{0,1}$ COMO CLAVE MAESTRA sk^*
S104: PASO DE GENERACIÓN DE CLAVE MAESTRA
ALMACENAR PARÁMETRO PÚBLICO pk Y CLAVE MAESTRA sk
S105: PASO DE ALMACENAMIENTO DE CLAVE MAESTRA
FIN

Fig. 10

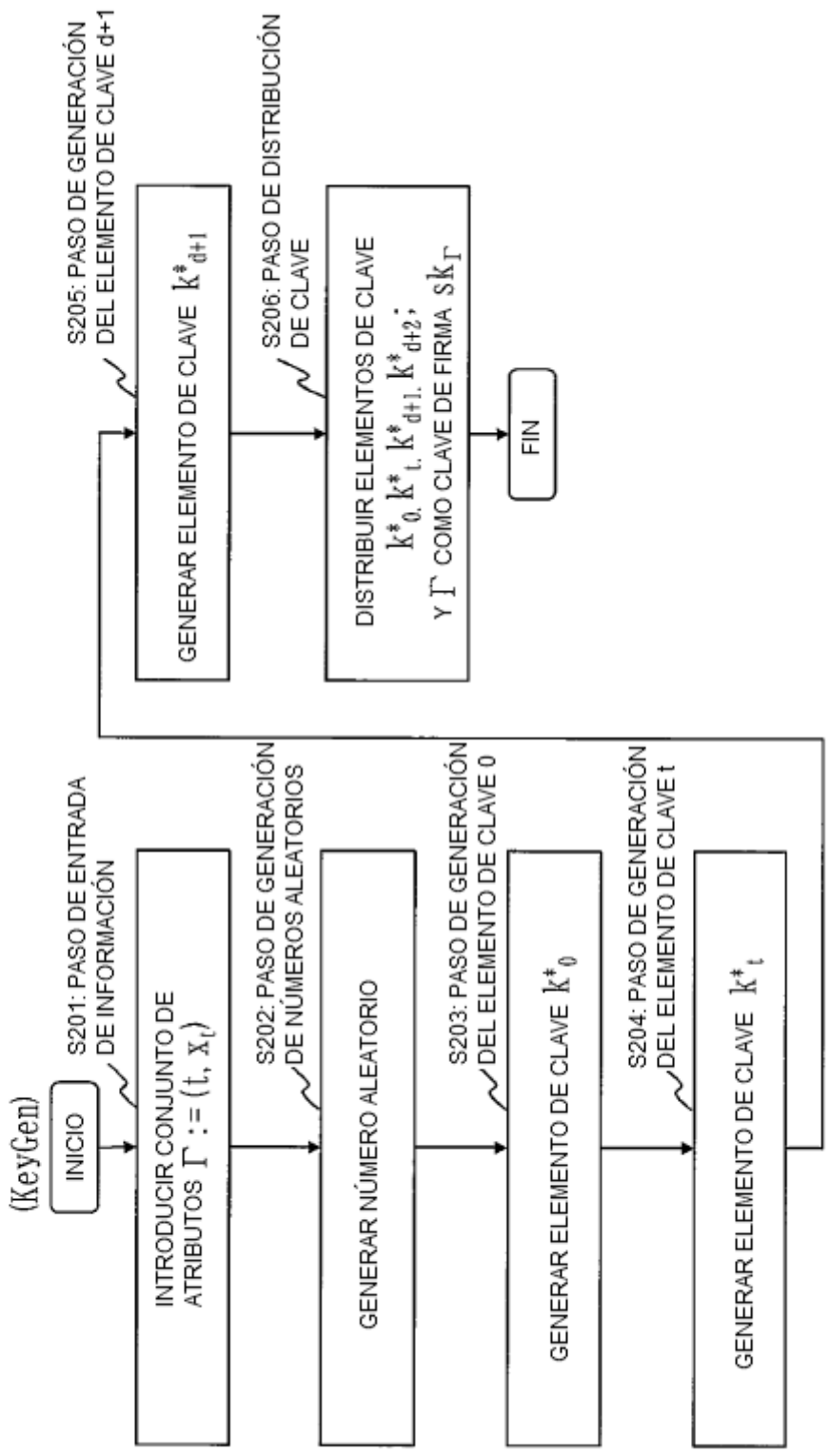

(KeyGen)
INICIO
S201: PASO DE ENTRADA DE INFORMACIÓN
INTRODUCIR CONJUNTO DE ATRIBUTOS $\Gamma := (t, x_t)$
S202: PASO DE GENERACIÓN DE NÚMEROS ALEATORIOS
GENERAR NÚMERO ALEATORIO
S203: PASO DE GENERACIÓN DEL ELEMENTO DE CLAVE 0
GENERAR ELEMENTO DE CLAVE k^*_0
S204: PASO DE GENERACIÓN DEL ELEMENTO DE CLAVE t
GENERAR ELEMENTO DE CLAVE k^*_t
S205: PASO DE GENERACIÓN DEL ELEMENTO DE CLAVE d+1
GENERAR ELEMENTO DE CLAVE k^*_{d+1}
S206: PASO DE DISTRIBUCIÓN DE CLAVE
DISTRIBUIR ELEMENTOS DE CLAVE $k^*_0, k^*_t, k^*_{d+1}, k^*_{d+2}$; Y Γ COMO CLAVE DE FIRMA sk_Γ
FIN

Fig. 11

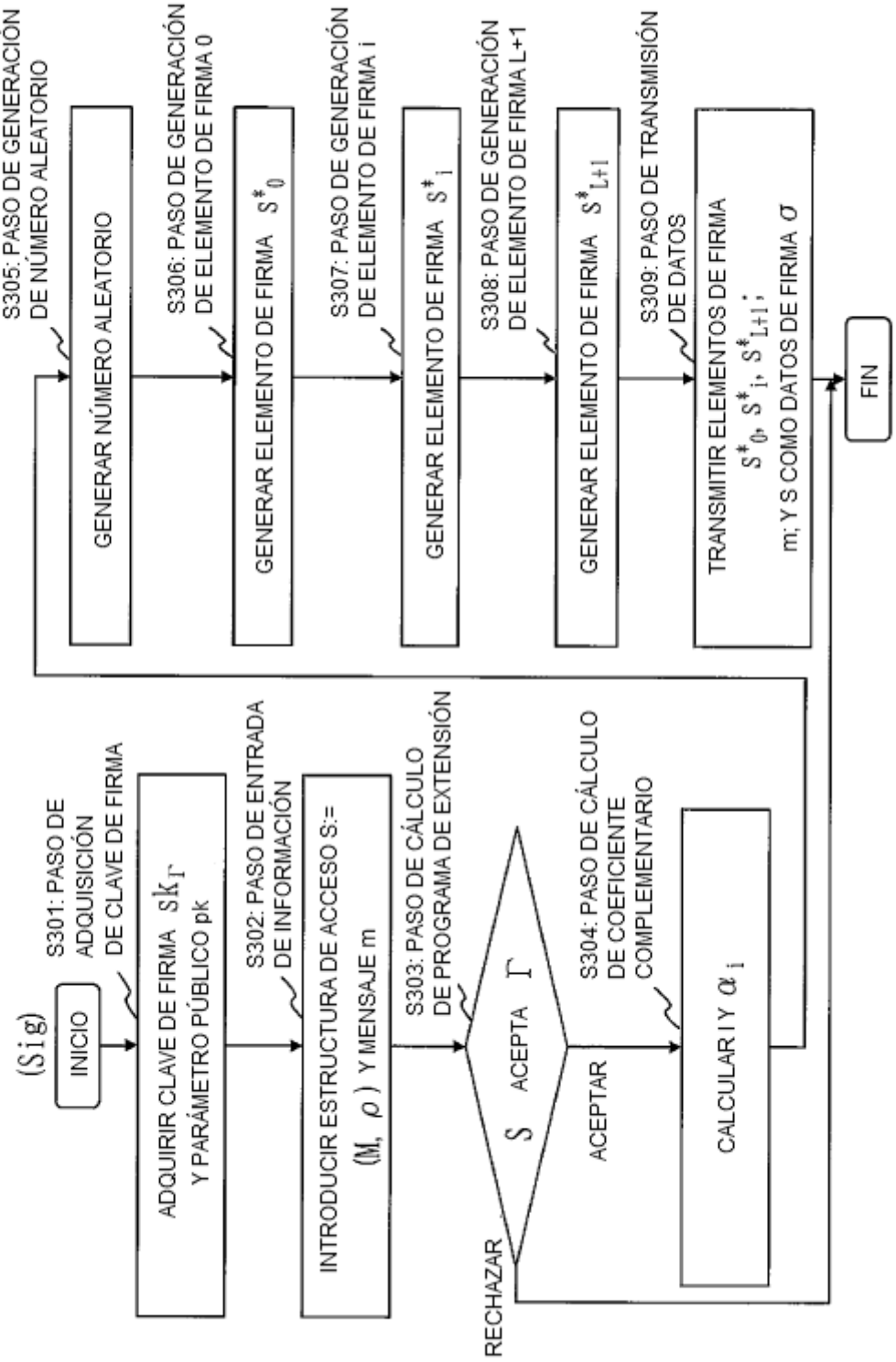

(Sig)
INICIO
S301: PASO DE ADQUISICIÓN DE CLAVE DE FIRMA
ADQUIRIR CLAVE DE FIRMA sk_Γ Y PARÁMETRO PÚBLICO pk
S302: PASO DE ENTRADA DE INFORMACIÓN
INTRODUCIR ESTRUCTURA DE ACCESO S:= (M, ρ) Y MENSAJE m
S303: PASO DE CÁLCULO DE PROGRAMA DE EXTENSIÓN
S ACEPTA Γ
RECHAZAR
ACEPTAR
S304: PASO DE CÁLCULO DE COEFICIENTE COMPLEMENTARIO
CALCULAR I Y α_i
S305: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMERO ALEATORIO
S306: PASO DE GENERACIÓN DE ELEMENTO DE FIRMA 0
GENERAR ELEMENTO DE FIRMA S^*_0
S307: PASO DE GENERACIÓN DE ELEMENTO DE FIRMA i
GENERAR ELEMENTO DE FIRMA S^*_i
S308: PASO DE GENERACIÓN DE ELEMENTO DE FIRMA L+1
GENERAR ELEMENTO DE FIRMA S^*_{L+1}
S309: PASO DE TRANSMISIÓN DE DATOS
TRANSMITIR ELEMENTOS DE FIRMA S^*_0, S^*_i, S^*_{L+1}, m; Y S COMO DATOS DE FIRMA σ
FIN

Fig. 12

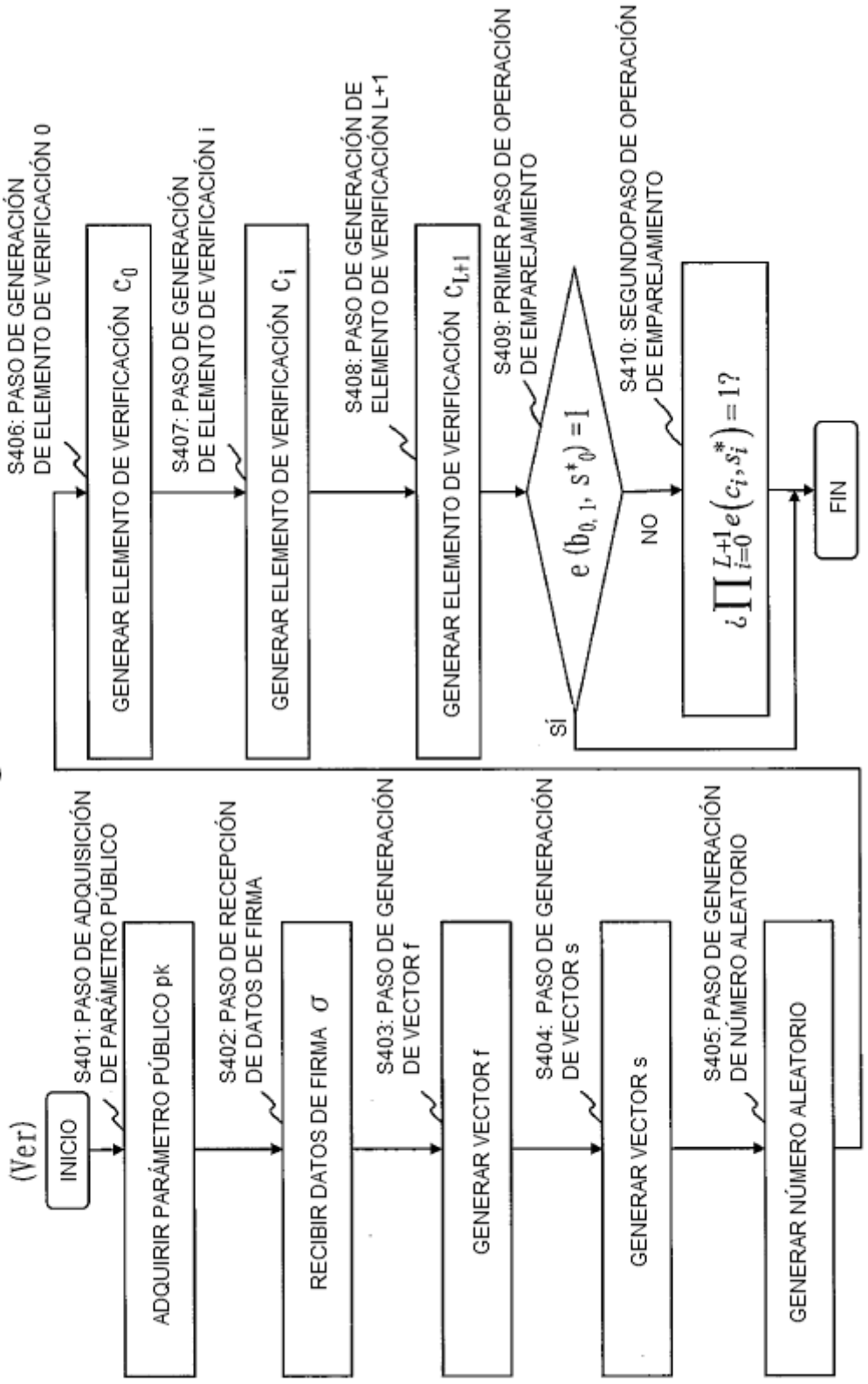

(Ver)
INICIO
S401: PASO DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
ADQUIRIR PARÁMETRO PÚBLICO pk
S402: PASO DE RECEPCIÓN DE DATOS DE FIRMA
RECIBIR DATOS DE FIRMA σ
S403: PASO DE GENERACIÓN DE VECTOR f
GENERAR VECTOR f
S404: PASO DE GENERACIÓN DE VECTOR s
GENERAR VECTOR s
S405: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMERO ALEATORIO
S406: PASO DE GENERACIÓN DE ELEMENTO DE VERIFICACIÓN 0
GENERAR ELEMENTO DE VERIFICACIÓN c_0
S407: PASO DE GENERACIÓN DE ELEMENTO DE VERIFICACIÓN i
GENERAR ELEMENTO DE VERIFICACIÓN c_i
S408: PASO DE GENERACIÓN DE ELEMENTO DE VERIFICACIÓN L+1
GENERAR ELEMENTO DE VERIFICACIÓN c_{L+1}
S409: PRIMER PASO DE OPERACIÓN DE EMPAREJAMIENTO
$e(b_{0,1}, s^*_0) = 1$
Sí
NO
S410: SEGUNDOPASO DE OPERACIÓN DE EMPAREJAMIENTO
$\prod_{i=0}^{L+1} e(c_i, s_i^*) = 1$?
FIN

Fig. 13

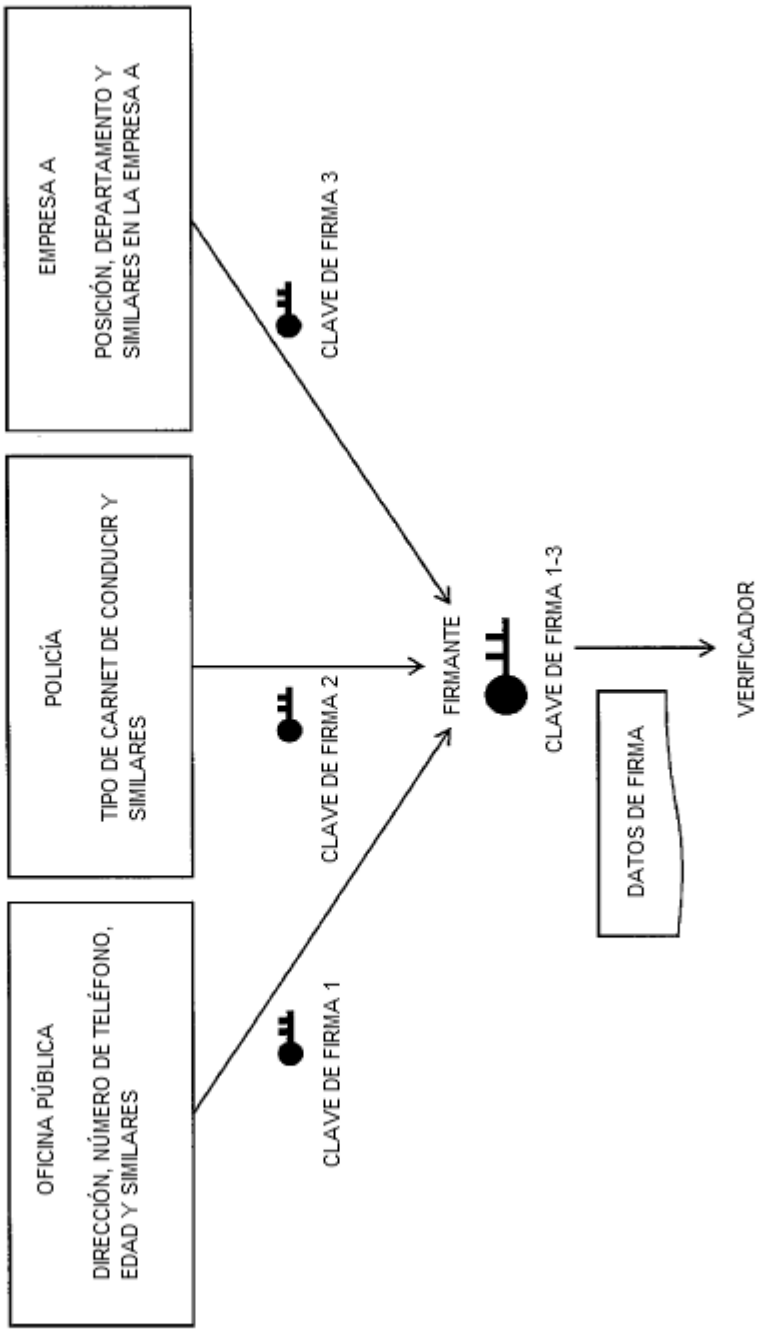

EMPRESA A
POSICIÓN, DEPARTAMENTO Y SIMILARES EN LA EMPRESA A
POLICÍA
TIPO DE CARNET DE CONDUCIR Y SIMILARES
OFICINA PÚBLICA
DIRECCIÓN, NÚMERO DE TELÉFONO, EDAD Y SIMILARES
CLAVE DE FIRMA 3
CLAVE DE FIRMA 2
CLAVE DE FIRMA 1
FIRMANTE
CLAVE DE FIRMA 1-3
DATOS DE FIRMA
VERIFICADOR

Fig. 14

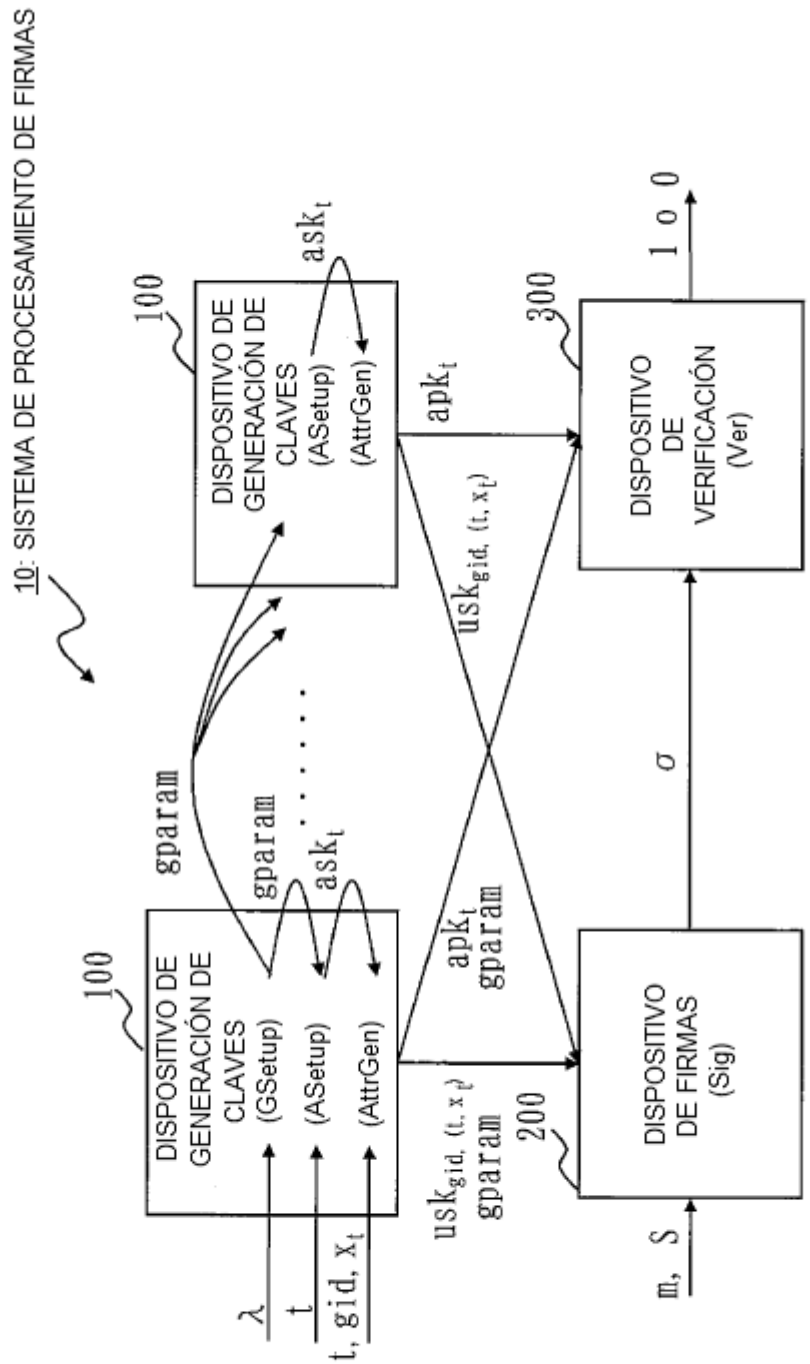

10: SISTEMA DE PROCESAMIENTO DE FIRMAS
100
DISPOSITIVO DE GENERACIÓN DE CLAVES (GSetup) (ASetup) (AttrGen)
gparam
ask_t
100
DISPOSITIVO DE GENERACIÓN DE CLAVES (ASetup) (AttrGen)
ask_t
apk_t
usk_gid, (t, x_t)
300
DISPOSITIVO DE VERIFICACIÓN (Ver)
1 o 0
σ
apk_t gparam
usk_gid, (t, x_t) gparam
200
DISPOSITIVO DE FIRMAS (Sig)
λ
t
t, gid, x_t
m, S

Fig. 15

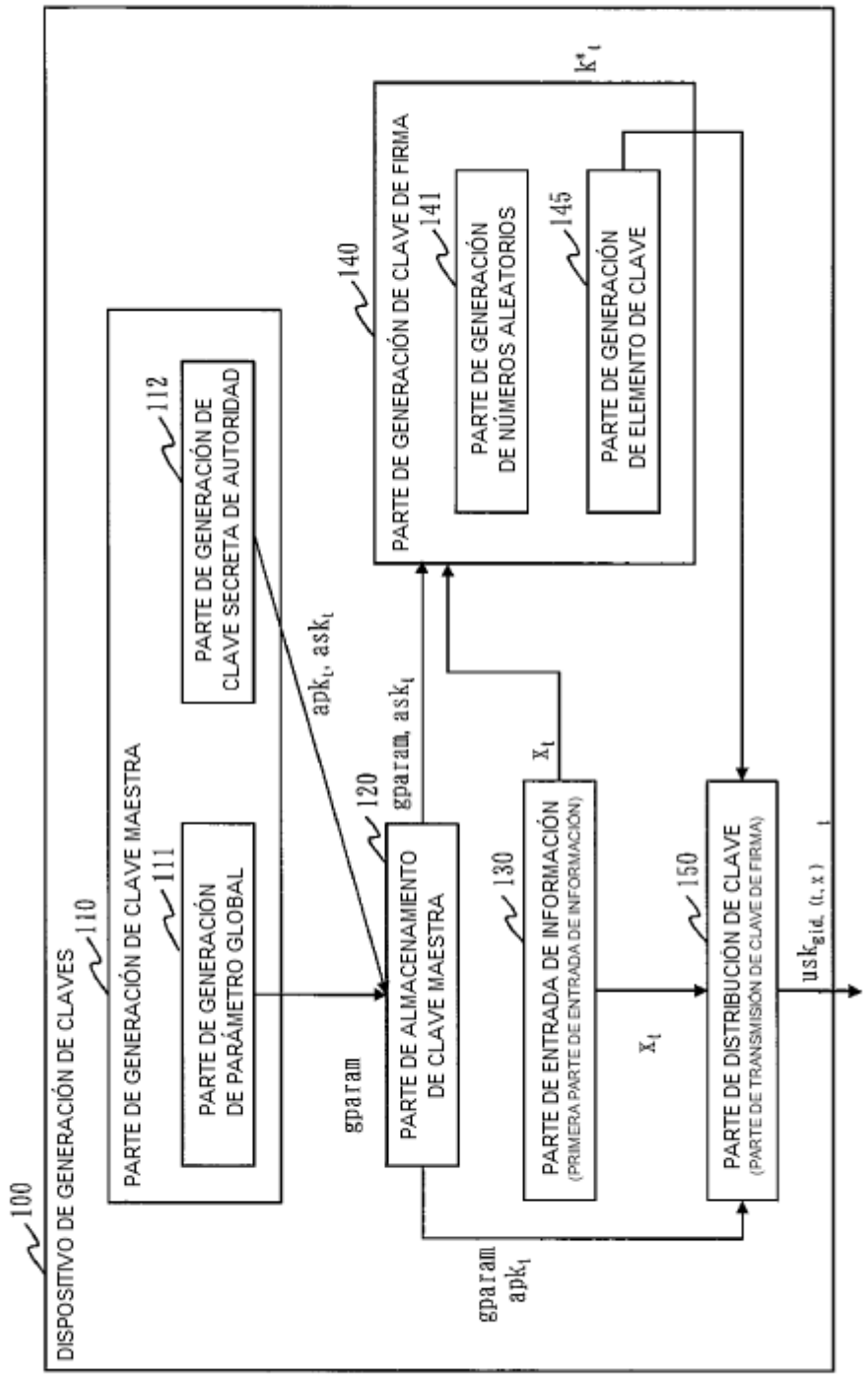

100
DISPOSITIVO DE GENERACIÓN DE CLAVES
110
PARTE DE GENERACIÓN DE CLAVE MAESTRA
111
PARTE DE GENERACIÓN DE PARÁMETRO GLOBAL
112
PARTE DE GENERACIÓN DE CLAVE SECRETA DE AUTORIDAD
140
PARTE DE GENERACIÓN DE CLAVE DE FIRMA
141
PARTE DE GENERACIÓN DE NÚMEROS ALEATORIOS
145
PARTE DE GENERACIÓN DE ELEMENTO DE CLAVE
120
PARTE DE ALMACENAMIENTO DE CLAVE MAESTRA
130
PARTE DE ENTRADA DE INFORMACIÓN
(PRIMERA PARTE DE ENTRADA DE INFORMACIÓN)
150
PARTE DE DISTRIBUCIÓN DE CLAVE
(PARTE DE TRANSMISIÓN DE CLAVE DE FIRMA)
gparam
gparam, ask_t
apk_t, ask_t
x_t
gparam
apk_t
x_t
k*_t

Fig. 16

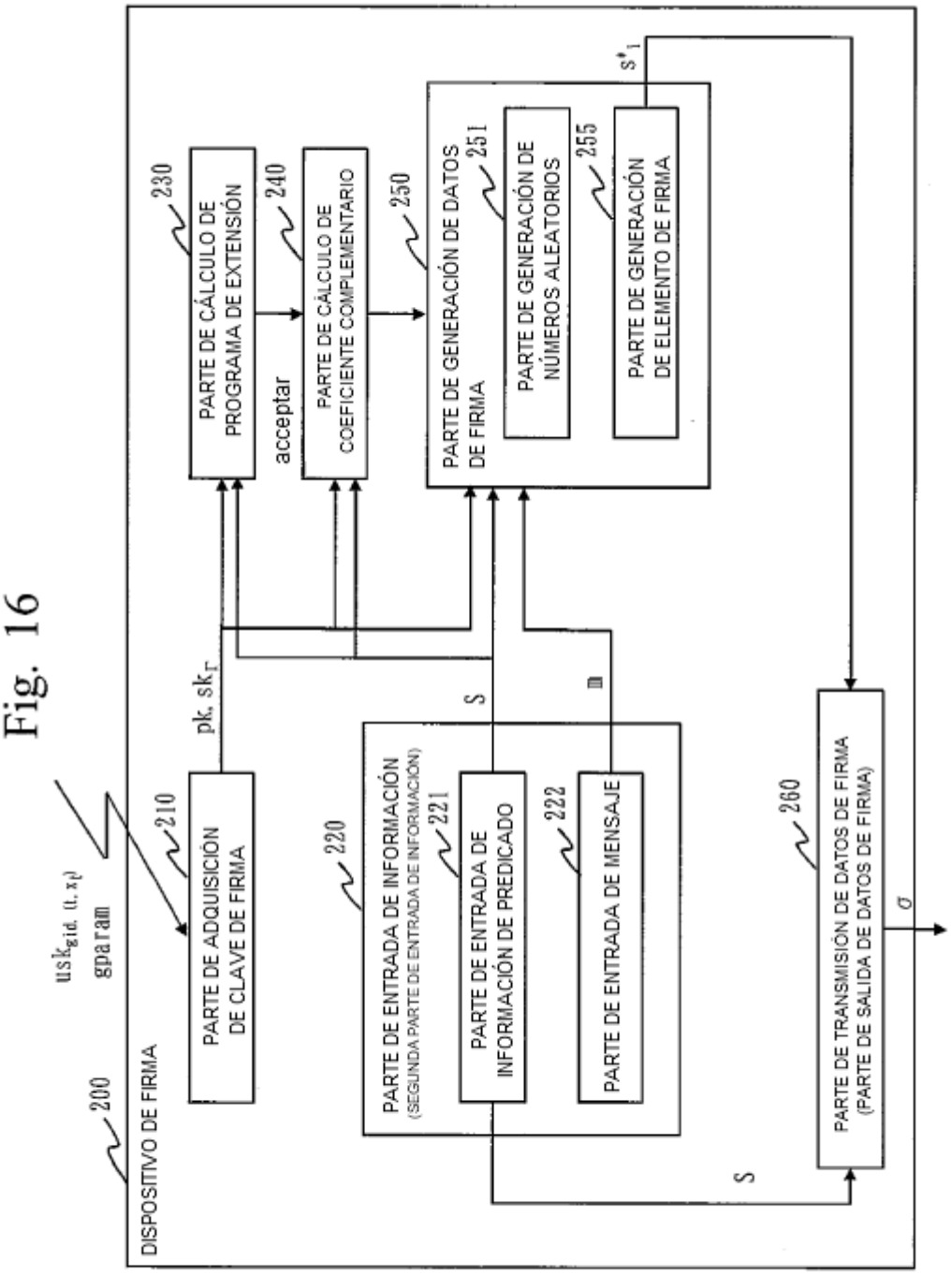

DISPOSITIVO DE FIRMA
200
$usk_{gid.\ (t.\ x_t)}$
gparam
PARTE DE ADQUISICIÓN DE CLAVE DE FIRMA
210
pk, sk_Γ
PARTE DE ENTRADA DE INFORMACIÓN
(SEGUNDA PARTE DE ENTRADA DE INFORMACIÓN)
220
PARTE DE ENTRADA DE INFORMACIÓN DE PREDICADO
221
PARTE DE ENTRADA DE MENSAJE
222
S
M
S
PARTE DE CÁLCULO DE PROGRAMA DE EXTENSIÓN
230
acceptar
PARTE DE CÁLCULO DE COEFICIENTE COMPLEMENTARIO
240
PARTE DE GENERACIÓN DE DATOS DE FIRMA
250
PARTE DE GENERACIÓN DE NÚMEROS ALEATORIOS
251
PARTE DE GENERACIÓN DE ELEMENTO DE FIRMA
255
s'_1
PARTE DE TRANSMISIÓN DE DATOS DE FIRMA
((PARTE DE SALIDA DE DATOS DE FIRMA)
260
σ

Fig. 17

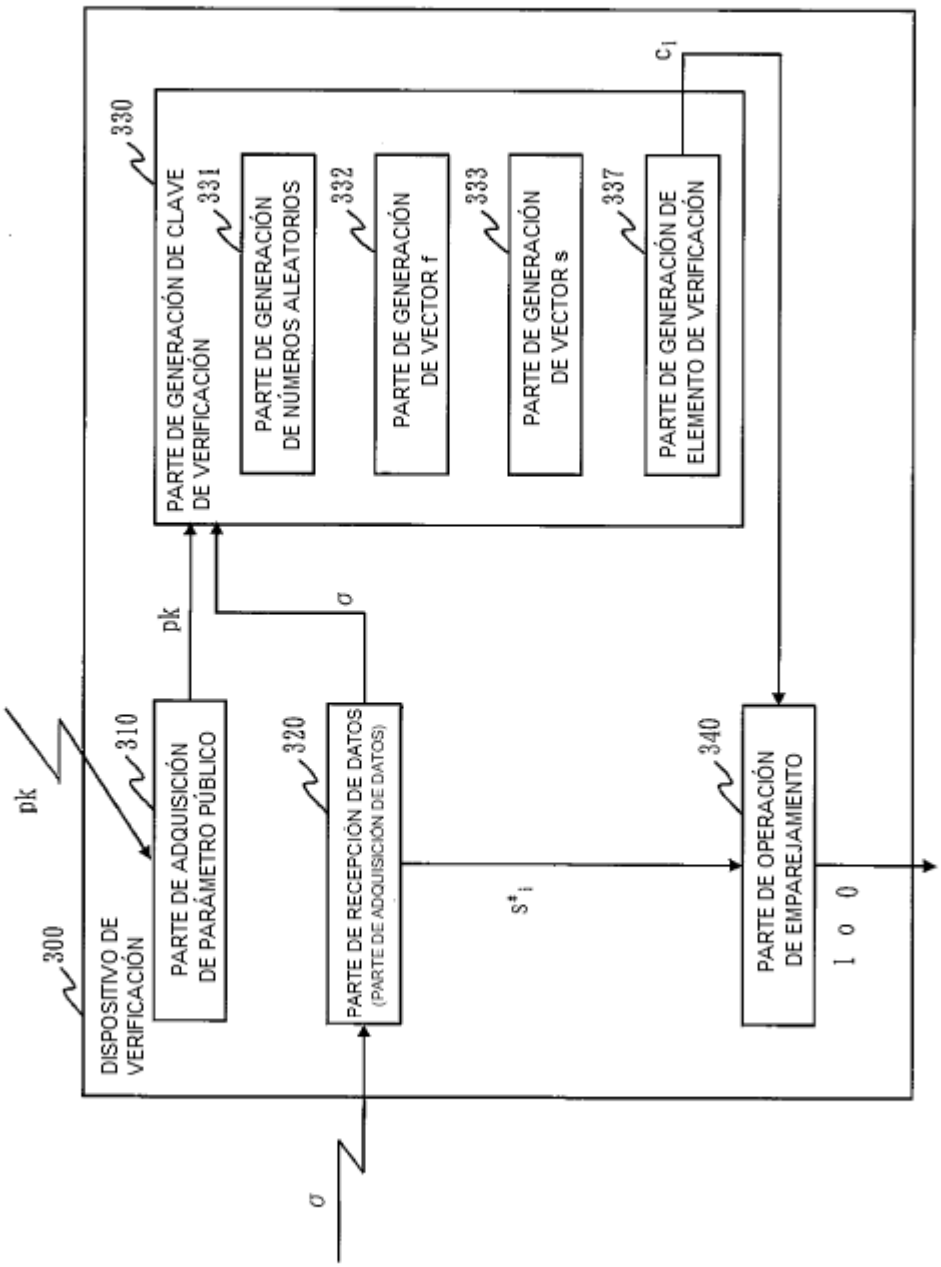

pk
σ
DISPOSITIVO DE VERIFICACIÓN
300
PARTE DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
310
PARTE DE RECEPCIÓN DE DATOS
(PARTE DE ADQUISICIÓN DE DATOS)
320
PARTE DE GENERACIÓN DE CLAVE DE VERIFICACIÓN
330
PARTE DE GENERACIÓN DE NÚMEROS ALEATORIOS
331
PARTE DE GENERACIÓN DE VECTOR f
332
PARTE DE GENERACIÓN DE VECTOR s
333
PARTE DE GENERACIÓN DE ELEMENTO DE VERIFICACIÓN
337
PARTE DE OPERACIÓN DE EMPAREJAMIENTO
340
s'_i
c_i
1 o 0

Fig. 18

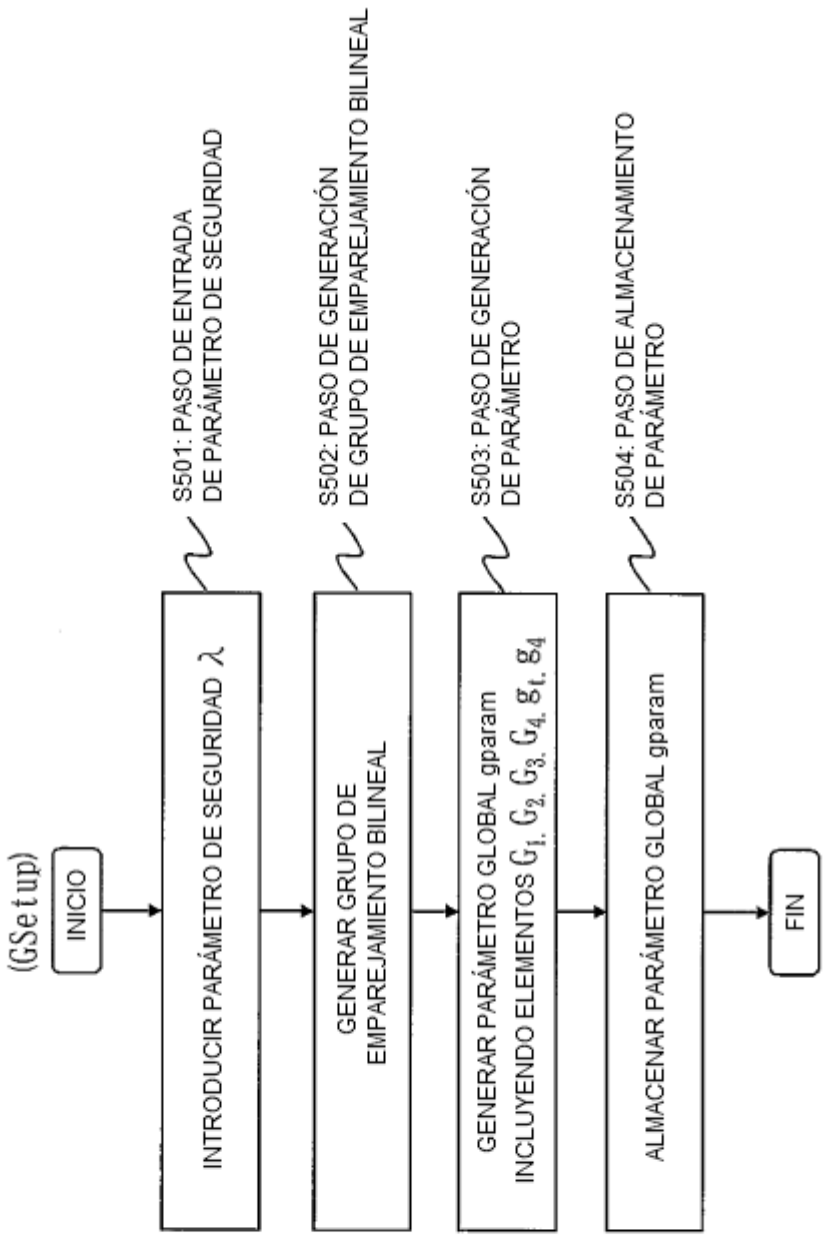

(GSetup)
INICIO
INTRODUCIR PARÁMETRO DE SEGURIDAD λ
S501: PASO DE ENTRADA DE PARÁMETRO DE SEGURIDAD
GENERAR GRUPO DE EMPAREJAMIENTO BILINEAL
S502: PASO DE GENERACIÓN DE GRUPO DE EMPAREJAMIENTO BILINEAL
GENERAR PARÁMETRO GLOBAL gparam INCLUYENDO ELEMENTOS G_1, G_2, G_3, G_4, g_t, g_4
S503: PASO DE GENERACIÓN DE PARÁMETRO
ALMACENAR PARÁMETRO GLOBAL gparam
S504: PASO DE ALMACENAMIENTO DE PARÁMETRO
FIN

Fig. 19

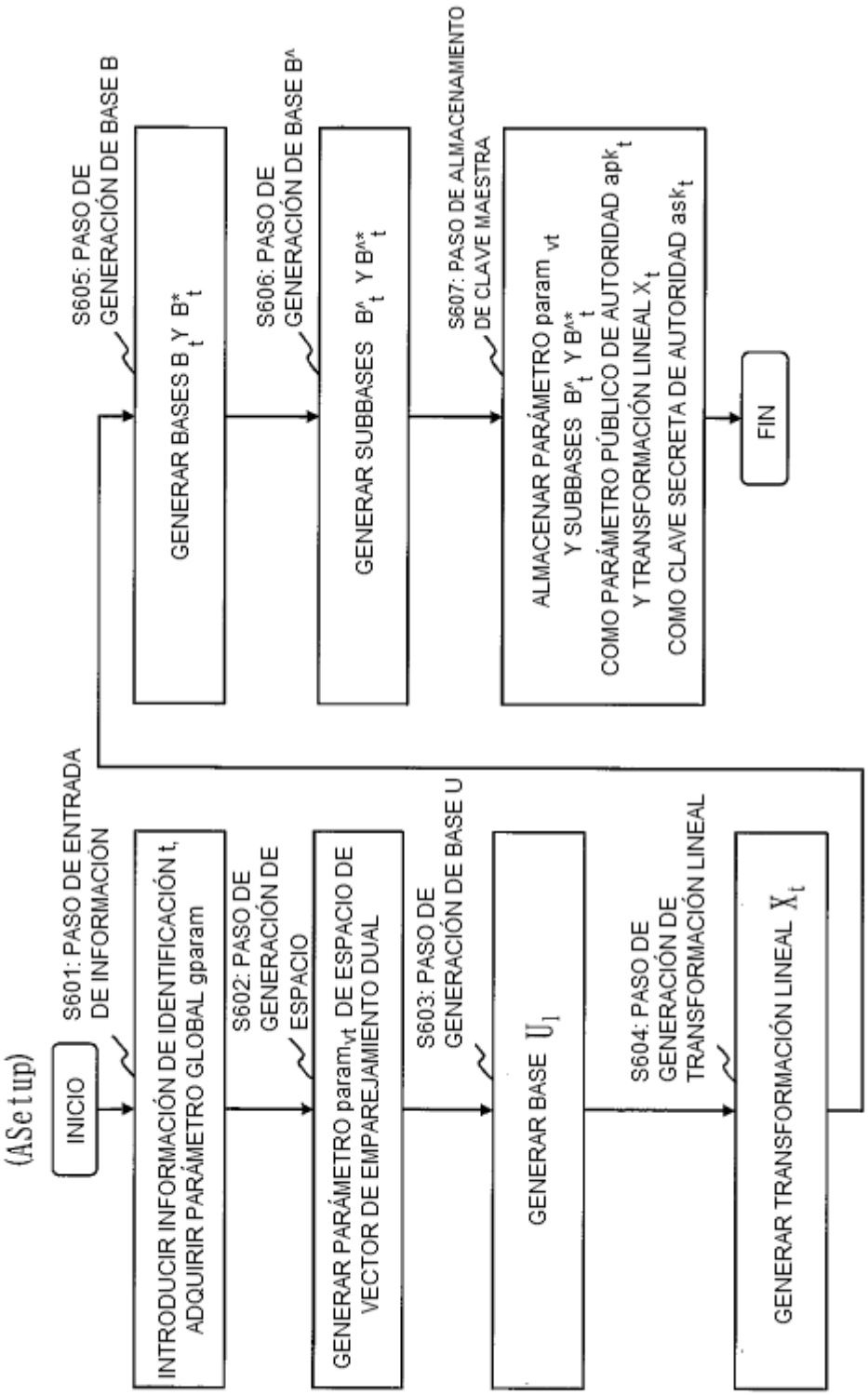

(ASetup)
INICIO
S601: PASO DE ENTRADA DE INFORMACIÓN
INTRODUCIR INFORMACIÓN DE IDENTIFICACIÓN t, ADQUIRIR PARÁMETRO GLOBAL gparam
S602: PASO DE GENERACIÓN DE ESPACIO
GENERAR PARÁMETRO param$_{vt}$ DE ESPACIO DE VECTOR DE EMPAREJAMIENTO DUAL
S603: PASO DE GENERACIÓN DE BASE U
GENERAR BASE U_j
S604: PASO DE GENERACIÓN DE TRANSFORMACIÓN LINEAL
GENERAR TRANSFORMACIÓN LINEAL X_t
S605: PASO DE GENERACIÓN DE BASE B
GENERAR BASES B $_t$ Y B* $_t$
S606: PASO DE GENERACIÓN DE BASE B^
GENERAR SUBBASES B^ $_t$ Y B^* $_t$
S607: PASO DE ALMACENAMIENTO DE CLAVE MAESTRA
ALMACENAR PARÁMETRO param $_{vt}$ Y SUBBASES B^ $_t$ Y B^* $_t$ COMO PARÁMETRO PÚBLICO DE AUTORIDAD apk_t Y TRANSFORMACIÓN LINEAL X_t COMO CLAVE SECRETA DE AUTORIDAD ask_t
FIN

Fig. 20

(AttrGen)

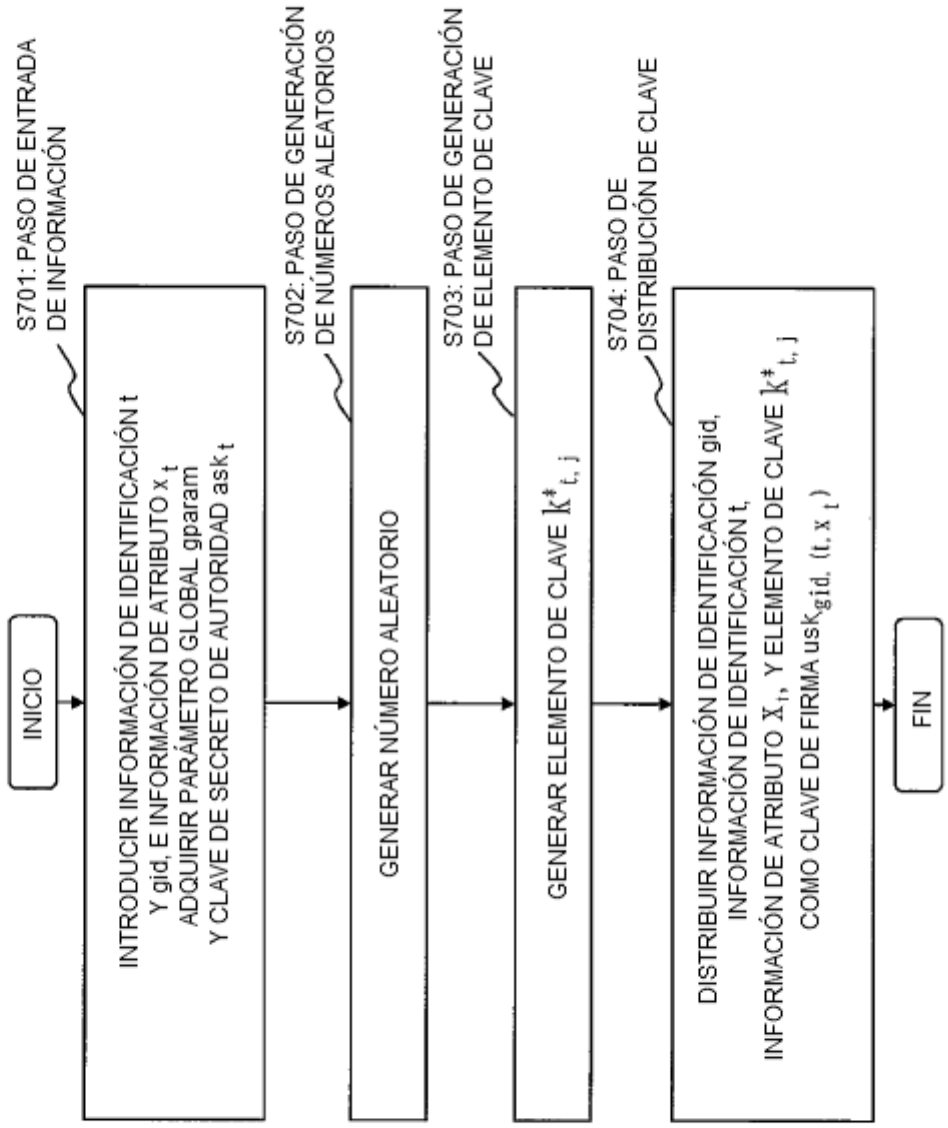


Fig. 21

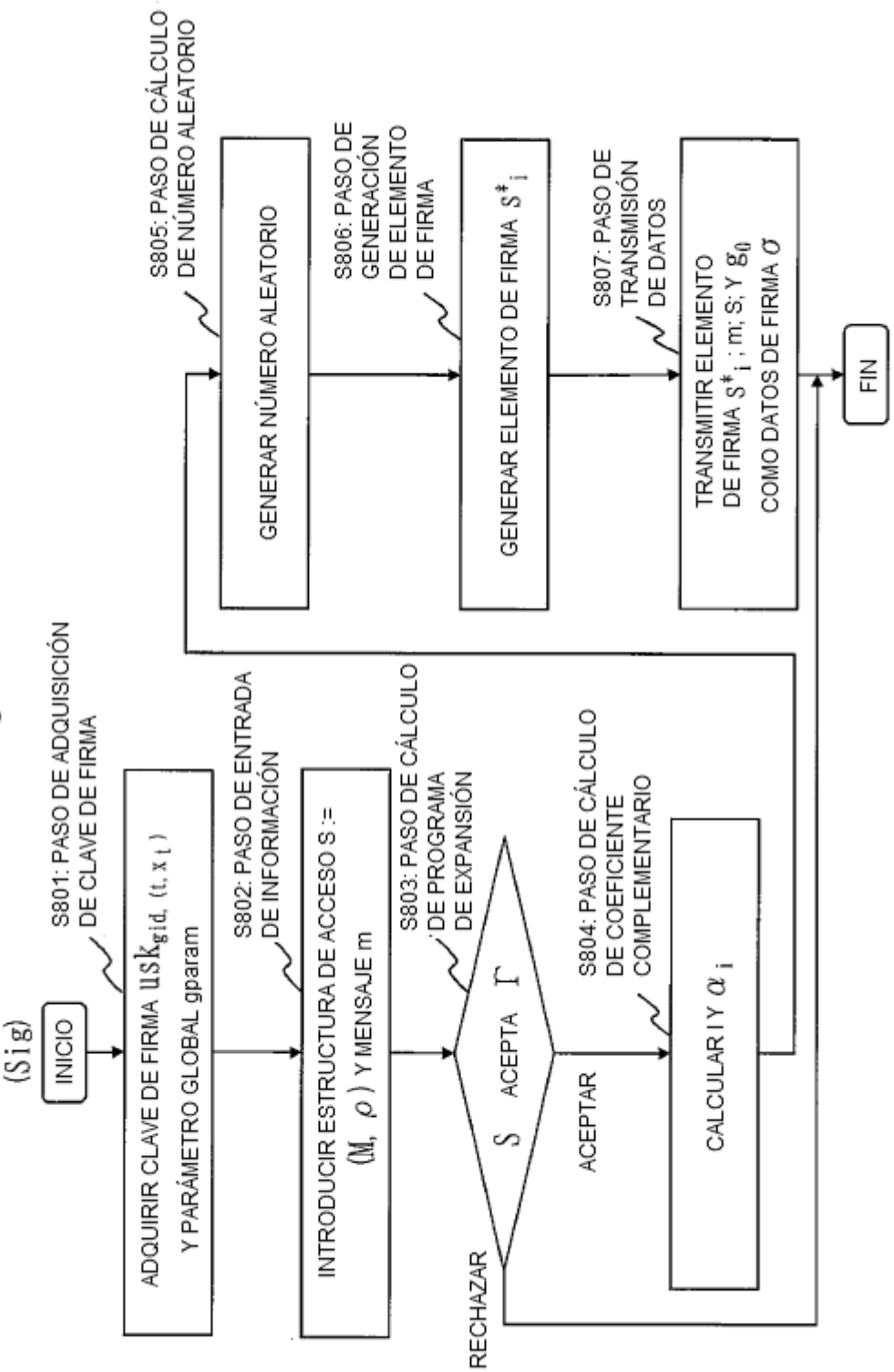

(Sig)
INICIO
S801: PASO DE ADQUISICIÓN DE CLAVE DE FIRMA
ADQUIRIR CLAVE DE FIRMA $usk_{gid,(t,x_t)}$ Y PARÁMETRO GLOBAL gparam
S802: PASO DE ENTRADA DE INFORMACIÓN
INTRODUCIR ESTRUCTURA DE ACCESO S := (M, ρ) Y MENSAJE m
S803: PASO DE CÁLCULO DE PROGRAMA DE EXPANSIÓN
S ACEPTA Γ
RECHAZAR
ACEPTAR
S804: PASO DE CÁLCULO DE COEFICIENTE COMPLEMENTARIO
CALCULAR I Y α_i
S805: PASO DE CÁLCULO DE NÚMERO ALEATORIO
GENERAR NÚMERO ALEATORIO
S806: PASO DE GENERACIÓN DE ELEMENTO DE FIRMA
GENERAR ELEMENTO DE FIRMA S^*_i
S807: PASO DE TRANSMISIÓN DE DATOS
TRANSMITIR ELEMENTO DE FIRMA S^*_i; m; S; Y g_0 COMO DATOS DE FIRMA σ
FIN

Fig. 22

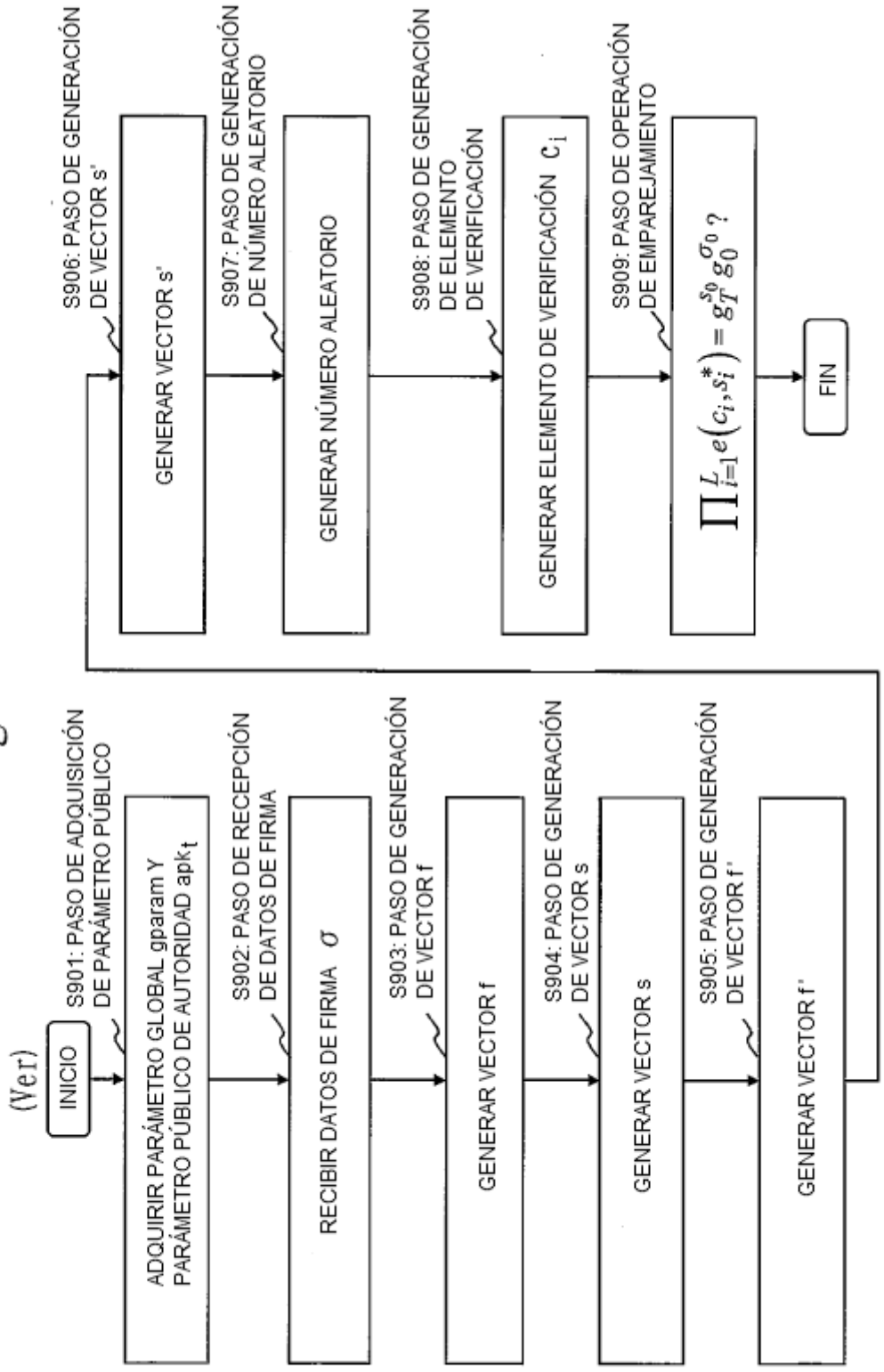
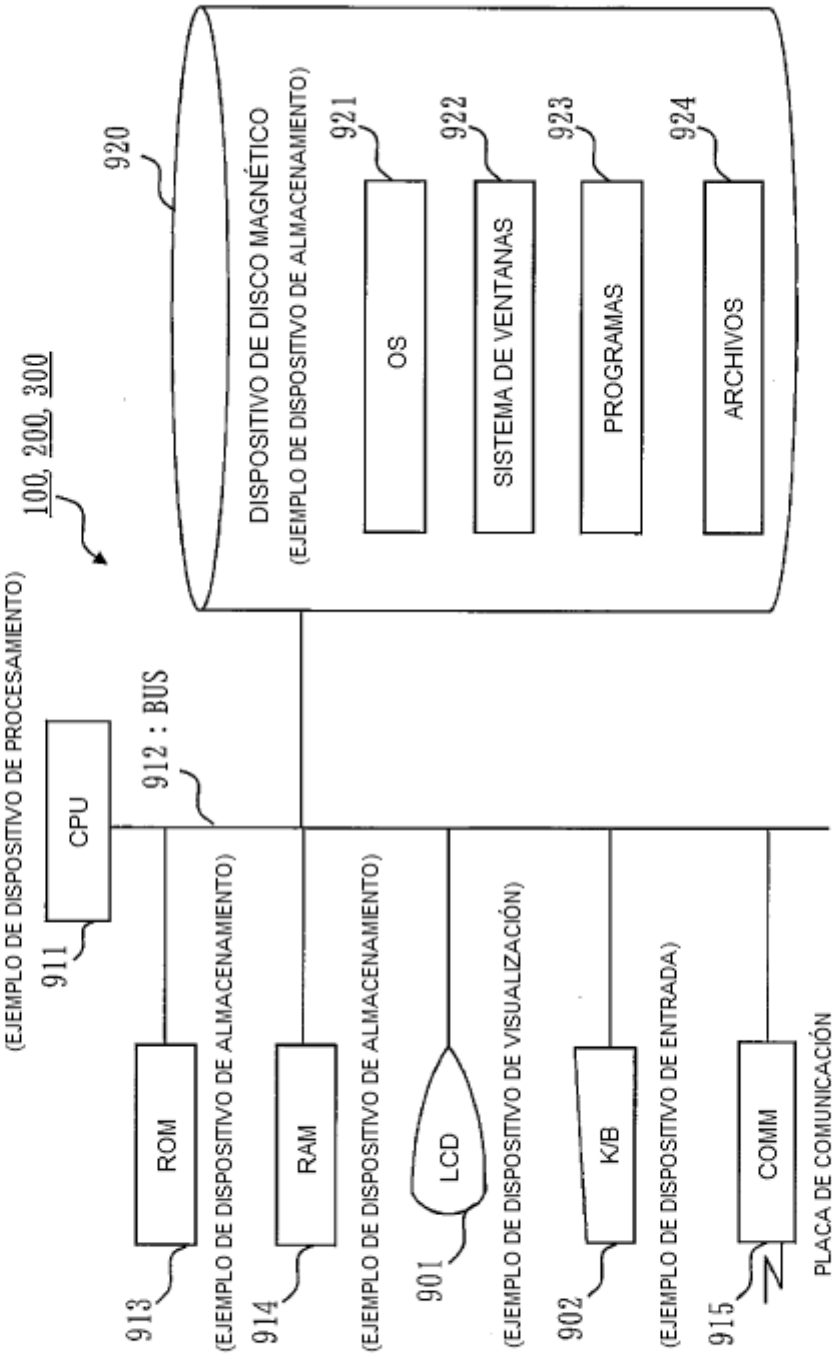

(Ver)
INICIO
S901: PASO DE ADQUISICIÓN DE PARÁMETRO PÚBLICO
ADQUIRIR PARÁMETRO GLOBAL gparam Y PARÁMETRO PÚBLICO DE AUTORIDAD apk_t
S902: PASO DE RECEPCIÓN DE DATOS DE FIRMA
RECIBIR DATOS DE FIRMA σ
S903: PASO DE GENERACIÓN DE VECTOR f
GENERAR VECTOR f
S904: PASO DE GENERACIÓN DE VECTOR s
GENERAR VECTOR s
S905: PASO DE GENERACIÓN DE VECTOR f'
GENERAR VECTOR f'
S906: PASO DE GENERACIÓN DE VECTOR s'
GENERAR VECTOR s'
S907: PASO DE GENERACIÓN DE NÚMERO ALEATORIO
GENERAR NÚMERO ALEATORIO
S908: PASO DE GENERACIÓN DE ELEMENTO DE VERIFICACIÓN
GENERAR ELEMENTO DE VERIFICACIÓN c_i
S909: PASO DE OPERACIÓN DE EMPAREJAMIENTO
$\prod_{i=1}^{L} e(c_i, s_i^*) = g_T^{s_0} g_0^{\sigma_0}$?
FIN

Fig. 23


100, 200, 300
920
DISPOSITIVO DE DISCO MAGNÉTICO
(EJEMPLO DE DISPOSITIVO DE ALMACENAMIENTO)
921
OS
922
SISTEMA DE VENTANAS
923
PROGRAMAS
924
ARCHIVOS
(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