(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 516 390**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/30 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.04.2010 E 13177763 (3)**

(97) Fecha y número de publicación de la concesión europea: **10.09.2014 EP 2658165**

(54) Título: **Sistema criptográfico, método de comunicación criptográfico, aparato de cifrado, aparato de generación de clave, aparato de descifrado, servidor de contenidos, programa, y medio de almacenamiento**

(30) Prioridad:

24.04.2009 JP 2009106008
24.04.2009 JP 2009106016
24.04.2009 JP 2009106028

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.10.2014

(73) Titular/es:

NIPPON TELEGRAPH AND TELEPHONE CORPORATION (100.0%)
3-1, Otemachi 2-chome, Chiyoda-ku
Tokyo 100-8116, JP

(72) Inventor/es:

TAKEUCHI, KAKU;
KOBAYASHI, TETSUTARO y
CHIKARA, SAKAE

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema criptográfico, método de comunicación criptográfico, aparato de cifrado, aparato de generación de clave, aparato de descifrado, servidor de contenidos, programa, y medio de almacenamiento

CAMPO TÉCNICO

La presente invención se refiere a una tecnología de comunicación criptográfica, y más específicamente, a una tecnología de comunicación criptográfica basada en cifrado de predicado.

ANTECEDENTES DE LA TÉCNICA

Las tecnologías criptográficas conocidas incluyen un sistema criptográfico de clave común y un sistema criptográfico de clave pública.

En el sistema criptográfico de clave común, un remitente de mensaje cifra un mensaje con una clave común para obtener un mensaje cifrado, y el receptor descifra el mensaje cifrado con la misma clave común para obtener el mensaje original. Por lo tanto, es necesario establecer un procedimiento para que el remitente y el receptor posean la clave común de manera segura.

En el sistema criptográfico de clave pública (1) un receptor prepara una clave pública y una clave privada correspondiente a la misma, (2) un remitente cifra un mensaje con la clave pública para obtener un mensaje cifrado, y (3) el receptor descifra el mensaje cifrado con la clave privada para obtener el mensaje original. Por lo tanto, el remitente necesita obtener la clave pública preparada por el receptor antes de cifrar el mensaje. En otras palabras, el cifrado es imposible a menos que el receptor genere la clave pública.

El cifrado de predicado ha sido propuesto recientemente. En el cifrado de predicado, la información X se incorpora en un mensaje cifrado durante el cifrado por el remitente, el receptor que tiene una información Y que tiene una relación especial con la información X puede descifrar el mensaje cifrado u obtener información relacionada con el mensaje sin conocer el mensaje. El remitente no necesita conocer necesariamente la información Y poseída por el receptor durante el cifrado. Además, el remitente no necesita determinar necesariamente el receptor antes del cifrado. El remitente puede determinar la información X activamente, libremente y con iniciativa. En teoría, la información X se llama atributo I (variable) y la información Y se llama predicado f (función de proposición o función Booleana). La relación específica que la información X y la información Y necesitan satisfacer durante el descifrado es, por ejemplo, f(I) = verdadero.

BIBLIOGRAFÍA DE LA TÉCNICA ANTERIOR

BIBLIOGRAFÍA QUE NO ES DE PATENTES

Bibliografía que no es de patente 1: Proyecto de Seguridad de Información de los Laboratorios de Plataforma de Compartición de Información de NTT, “NTT Cryptographic Primitives”, URL: http://info.isl.ntt.co.jp/crypt/, recuperado el 14 de abril de 2009.

Bibliografía que no es de patente 2: Tatsuaki Okamoto y Hirosuke Yamamoto, “Information Science Mathematics Series: Modern Cryptography”, Tercera edición, Sangyo-Tosyo Corporation, 2000.

Bibliografía que no es de patente 3: J. Katz, A. Sahai, y B. Waters, “Predicate Encryption Supporting Disjunction, Polynomial Equations, and Inner Products”, Eurocrypt 2008, páginas 146-162.

DESCRIPCIÓN DE LA INVENCIÓN

Problemas a ser resueltos por la invención

Un objeto de la presente invención es proporcionar una tecnología de comunicación criptográfica que permita que una información de cifrado cifrada con el cifrado de predicado sea distribuida y que pueda operar de manera flexible.

MEDIOS PARA RESOLVER LOS PROBLEMAS

La presente invención se perfilará más abajo.

En un sistema criptográfico que usa cifrado de predicado e incluye, al menos, uno o una pluralidad de aparatos de cifrado, uno o una pluralidad de aparatos de generación de clave, y una pluralidad de aparatos de descifrado, una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; uno o una pluralidad de de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en lo sucesivo llamada información de designación de predicado) a una

información de predicado usada en el algoritmo de cifrado de predicado; y se identifica por adelantado una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado.

Cada uno del uno o la pluralidad de aparatos de cifrado realiza un primer proceso de adquisición de información de lógica de predicado de uso de un tipo de información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, el un tipo de información de regla de conversión que se selecciona junto con la información de política según si la información de entrada introducida al aparato de cifrado es o bien una información de designación de atributo o bien una información de asignación de predicado, para obtener una información de atributo (en lo sucesivo llamada primera información de atributo) o una información de predicado (en lo sucesivo llamada primera información de predicado) a partir de la información de entrada; y un proceso de cifrado de uso de la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave, para obtener una clave común y una información de cifrado que corresponde a la clave común o que corresponde a información usada para generar la clave común, según el algoritmo de cifrado de predicado.

Cada uno del uno o la pluralidad de aparatos de generación de clave realiza un segundo proceso de adquisición de información de lógica de predicado de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (en lo sucesivo llamada segunda información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del aparato de descifrado; y un proceso de generación de clave de uso de la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave, para generar una clave de descifrado usada para descifrar la información de cifrado.

Cada uno del uno o la pluralidad de aparatos de descifrado usa la clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado. El aparato de descifrado también realiza un proceso de transferencia de transferencia de la información de cifrado a otro aparato de descifrado. La información de cifrado a ser transferida se puede enviar desde el aparato de cifrado o se puede transferir desde otro aparato de descifrado. Al menos una parte de los aparatos de descifrado incluidos en el sistema criptográfico tiene una función de realización del proceso de transferencia, pero no se requieren que todos los aparatos de descifrado tengan esta función. Un aparato de descifrado que ha recibido la información de cifrado transferida pide al aparato de generación de clave generar la clave de descifrado, si es necesario, y realiza el proceso de descifrado.

Alternativamente, la presente invención se perfilará más abajo.

En un sistema criptográfico que usa cifrado de predicado e incluye, al menos, uno o una pluralidad de aparatos de cifrado, uno o una pluralidad de aparatos de generación de clave, y una pluralidad de aparatos de descifrado, una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en lo sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo de cifrado de predicado; y se determina por adelantado una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado.

Cada uno del uno o la pluralidad de aparatos de cifrado realiza un primer proceso de adquisición de información de lógica de predicado de uso de un tipo de información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, el un tipo de información de regla de conversión que se selecciona junto con la información de política según si la información de entrada introducida al aparato de cifrado es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener información de atributo (en lo sucesivo llamada primera información de atributo) o información de predicado (en lo sucesivo llamada primera información de predicado) a partir de la información de entrada; y un proceso de cifrado de uso de la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave, para obtener una clave común e información de cifrado que corresponde a la clave común o que corresponde a información usada para generar la clave común, según el algoritmo de cifrado de predicado.

Cada uno del uno o la pluralidad de aparatos de descifrado realiza un segundo proceso de adquisición de

información de lógica de predicado de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (en lo sucesivo llamada segunda información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del aparato de descifrado; y usa una clave de descifrado enviada desde el aparato de generación de clave para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado.

Cada uno del uno o la pluralidad de aparatos de generación de clave realiza un proceso de generación de clave de uso de la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave, para generar la clave de descifrado usada para descifrar la información de cifrado.

El aparato de descifrado también realiza un proceso de transferencia de transferencia de la información de cifrado a otro aparato de descifrado. La información de cifrado a ser transferida se puede enviar desde el aparato de cifrado o se puede transferir desde otro aparato de descifrado. Al menos una parte de los aparatos de descifrado incluidos en el sistema criptográfico tiene una función de realización del proceso de transferencia, pero no se requiere que todos los aparatos de descifrado tengan esta función. Un aparato de descifrado que ha recibido la información de cifrado transferida pide al aparato de generación de clave generar la clave de descifrado, si es necesario, y realiza el proceso de descifrado.

Alternativamente, la presente invención se perfilará más abajo.

En un sistema criptográfico que usa cifrado de predicado e incluye, al menos, uno o una pluralidad de aparatos de cifrado, uno o una pluralidad de aparatos de generación de clave, y una pluralidad de aparatos de descifrado, se determinan por adelantado una clave privada y una clave pública que corresponde a la clave privada para cada uno del uno o la pluralidad de aparatos de generación de clave; se determinan por adelantado uno o una pluralidad de pares de información de regla de conversión, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en lo sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo de cifrado de predicado; y se determina por adelantado una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado.

Cada uno del uno o la pluralidad de aparatos de cifrado realiza un primer proceso de adquisición de información de lógica de predicado de uso de un tipo de información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, el un tipo de información de regla de conversión que se selecciona junto con la información de política según si la información de entrada introducida al aparato de cifrado es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo (en lo sucesivo llamada primera información de atributo) o una información de predicado (en lo sucesivo llamada primera información de predicado) a partir de la información de entrada; y un proceso de cifrado de uso de la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave y texto plano, para obtener una información de cifrado que corresponde al texto plano según el algoritmo de cifrado de predicado.

Cada uno del uno o la pluralidad de aparatos de generación de clave realiza un segundo proceso de adquisición de información de lógica de predicado de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (en lo sucesivo llamada segunda información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del aparato de descifrado; y un proceso de generación de clave de uso de la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave, para generar una clave de descifrado usada para descifrar la información de cifrado.

Cada uno del uno o la pluralidad de aparatos de descifrado usa la clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado. El aparato de descifrado también realiza un proceso de transferencia de transferencia de la información de cifrado a otro aparato de descifrado. La información de cifrado a ser transferida se puede enviar desde el aparato de cifrado o se puede transferir desde otro aparato de descifrado. Al menos una parte de los aparatos de descifrado incluidos en el sistema criptográfico tiene una función de realización del proceso de transferencia, pero no se requiere que todos los aparatos de descifrado tengan esta función. Un aparato de descifrado que ha recibido la información de cifrado transferida pide al aparato de generación de clave generar la clave de descifrado, si es necesario, y realiza el proceso de descifrado.

Alternativamente, la presente invención se perfilará más abajo.

En un sistema criptográfico que usa cifrado de predicado e incluye, al menos, uno o una pluralidad de aparatos de cifrado, uno o una pluralidad de aparatos de generación de clave, y una pluralidad de aparatos de descifrado, una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; se determinan por adelantado uno o una pluralidad de pares de información de regla de conversión, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo y una información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en lo sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo de cifrado de predicado; y se determina por adelantado una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado.

Cada uno del uno o la pluralidad de aparatos de cifrado realiza un primer proceso de adquisición de información de lógica de predicado de uso de un tipo de información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, el un tipo de información de regla de conversión que se selecciona junto con la información de política según si la información de entrada introducida al aparato de cifrado es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo (en lo sucesivo llamada primera información de atributo) o una información de predicado (en lo sucesivo llamada primera información de predicado) a partir de la información de entrada; y un proceso de cifrado de uso de la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave y texto plano, para obtener una información de cifrado que corresponde al texto plano según el algoritmo de cifrado de predicado.

Cada uno del uno o la pluralidad de aparatos de descifrado realiza un segundo proceso de adquisición de información de lógica de predicado de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (en lo sucesivo llamada segunda información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del aparato de descifrado; y usa una clave de descifrado enviada desde el aparato de generación de clave para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado.

Cada uno del uno o la pluralidad de aparatos de generación de clave realiza un proceso de generación de clave de uso de la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave, para generar una clave de descifrado usada para descifrar la información de cifrado.

El aparato de descifrado también realiza un proceso de transferencia de transferencia de la información de cifrado a otro aparato de descifrado. La información de cifrado a ser transferida se puede enviar desde el aparato de cifrado o se puede transferir desde otro aparato de descifrado. Al menos una parte de los aparatos de descifrado incluidos en el sistema criptográfico tiene una función de realización del proceso de transferencia, pero no se requieren que todos los aparatos de descifrado tengan esta función. Un aparato de descifrado que ha recibido la información de cifrado transferida pide al aparato de generación de clave generar la clave de descifrado, si es necesario, y realiza el proceso de descifrado.

EFECTOS DE LA INVENCIÓN

Según la presente invención, usando una parte de una información de regla de conversión seleccionada en base a si una información de entrada introducida a un aparato de cifrado es en una información de designación de atributo o una información de designación de predicado, donde la una parte de una información de regla de conversión es o bien una de una información de regla de conversión de atributo y una información de regla de conversión de predicado contenida en un par de información de regla de conversión seleccionado a partir de pares de información de regla de conversión, la información de atributo o la información de predicado se obtiene a partir de la información de entrada; por lo tanto, una comunicación criptográfica en base a un cifrado de predicado se puede operar de una manera flexible. Además, se puede distribuir una información de cifrado cifrada con el cifrado de predicado debido a que un aparato de descifrado tiene una función de transferencia.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es una vista estructural de un sistema criptográfico según cada ejemplo en un primer aspecto

relativo a la presente invención;
La Figura 2 es una vista (Nº 1) que muestra un procedimiento de procesamiento de un método de comunicación criptográfico según cada ejemplo en el primer aspecto;
La Figura 3 es una vista (Nº 2) que muestra el procedimiento de procesamiento del método de comunicación criptográfico según cada ejemplo en el primer aspecto;
La Figura 4 es una vista (Nº 3) que muestra el procedimiento de procesamiento del método de comunicación criptográfico según cada ejemplo en el primer aspecto;
La Figura 5 es un diagrama de bloques funcional de un aparato de cifrado según un primer ejemplo del primer aspecto;
La Figura 6 es la vista que muestra un procedimiento de procesamiento detallado de un proceso de cifrado según el primer ejemplo del primer aspecto;
La Figura 7 es un diagrama de bloques funcional de un aparato de descifrado según el primer ejemplo del primer aspecto;
La Figura 8 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de descifrado según el primer ejemplo del primer aspecto;
La Figura 9 es un diagrama de bloques funcional de un aparato de generación de clave según el primer ejemplo del primer aspecto;
La Figura 10 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de generación de clave según el primer ejemplo del primer aspecto;
La Figura 11 es una vista que muestra cómo obtener una información de atributo o una información de predicado a partir de una información de entrada o una información de usuario usando un esquema correspondiente a una política;
La Figura 12 es una vista que muestra cómo obtener una información de atributo a partir de una información de designación de atributo usando un esquema de atributo;
La Figura 13 es una vista que muestra cómo obtener una información de predicado a partir de una información de designación de predicado usando un esquema de predicado;
La Figura 14 es una vista que muestra ejemplos de políticas;
La Figura 15 es una vista que muestra un ejemplo de tabla de claves de descifrado;
La Figura 16 es una vista que muestra un ejemplo de tabla de autenticación;
La Figura 17 es una vista que muestra un ejemplo de tablas de información de usuario;
La Figura 18 es un diagrama de bloques funcional de un aparato de descifrado según un segundo ejemplo del primer aspecto;
La Figura 19 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de descifrado según el segundo ejemplo del primer aspecto;
La Figura 20 es un diagrama de bloques funcional de un aparato de generación de clave según el segundo ejemplo del primer aspecto;
La Figura 21 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de generación de clave según el segundo ejemplo del primer aspecto;
La Figura 22 es un diagrama de bloques funcional de un aparato de cifrado según un tercer ejemplo del primer aspecto;
La Figura 23 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de cifrado según el tercer ejemplo del primer aspecto;
La Figura 24 es un diagrama de bloques funcional de un aparato de descifrado según el tercer ejemplo del primer aspecto;
La Figura 25 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de descifrado según el tercer ejemplo del primer aspecto;
La Figura 26 es un diagrama de bloques funcional de un aparato de descifrado según un cuarto ejemplo del primer aspecto;
La Figura 27 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de descifrado según el cuarto ejemplo del primer aspecto;
La Figura 28 es una vista estructural de un sistema criptográfico según cada realización en un segundo aspecto de la presente invención;
La Figura 29 es una vista (Nº 1) que muestra un procedimiento de procesamiento de un método de comunicación criptográfico según cada realización en el segundo aspecto;
La Figura 30 es una vista (Nº 2) que muestra el procedimiento de procesamiento del método de comunicación criptográfico según cada realización en el segundo aspecto;
La Figura 31 es una vista (Nº 3) que muestra el procedimiento de procesamiento del método de comunicación criptográfico según cada realización en el segundo aspecto;
La Figura 32 es una vista (Nº 4) que muestra el procedimiento de procesamiento del método de comunicación criptográfico según cada realización en el segundo aspecto;
La Figura 33 es un diagrama de bloques funcional de un aparato de cifrado según una primera realización del segundo aspecto;
La Figura 34 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de cifrado según la primera realización del segundo aspecto;
La Figura 35 es un diagrama de bloques funcional de un primer aparato de descifrado según la primera

realización del segundo aspecto;
La Figura 36 es una vista que muestra un procedimiento de procesamiento detallado de un primer proceso de descifrado según la primera realización del segundo aspecto;
La Figura 37 es un diagrama de bloques funcional de un segundo aparato de descifrado según la primera realización del segundo aspecto;
La Figura 38 es una vista que muestra un procedimiento de procesamiento detallado de un segundo proceso de descifrado según la primera realización del segundo aspecto;
La Figura 39 es un diagrama de bloques funcional de un aparato de generación de clave según la primera realización del segundo aspecto;
La Figura 40 es una vista que muestra un procedimiento de procesamiento detallado (que corresponde al primer aparato de descifrado) de un proceso de generación de clave según la primera realización del segundo aspecto;
La Figura 41 es una vista que muestra un procedimiento de procesamiento detallado (que corresponde al segundo aparato de descifrado) de un proceso de generación de clave según la primera realización del segundo aspecto;
La Figura 42 es un diagrama de bloques funcional de un primer aparato de descifrado según una segunda realización del segundo aspecto;
La Figura 43 es una vista que muestra un procedimiento de procesamiento detallado de un primer proceso de descifrado según la segunda realización del segundo aspecto;
La Figura 44 es un diagrama de bloques funcional de un segundo aparato de descifrado según la segunda realización del segundo aspecto;
La Figura 45 es una vista que muestra un procedimiento de procesamiento detallado de un segundo proceso de descifrado según la segunda realización del segundo aspecto;
La Figura 46 es un diagrama de bloques funcional de un aparato de generación de clave según la segunda realización del segundo aspecto;
La Figura 47 es una vista que muestra un procedimiento de procesamiento detallado (que corresponde al primer aparato de descifrado) de un proceso de generación de clave según la segunda realización del segundo aspecto;
La Figura 48 es una vista que muestra un procedimiento de procesamiento detallado (que corresponde al segundo aparato de descifrado) de un proceso de generación de clave según la segunda realización del segundo aspecto;
La Figura 49 es un diagrama de bloques funcional de un aparato de cifrado según una tercera realización del segundo aspecto;
La Figura 50 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de cifrado según la tercera realización del segundo aspecto;
La Figura 51 es un diagrama de bloques funcional de un primer aparato de descifrado según la tercera realización del segundo aspecto;
La Figura 52 es una vista que muestra un procedimiento de procesamiento detallado de un primer proceso de descifrado según la tercera realización del segundo aspecto;
La Figura 53 es un diagrama de bloques funcional de un segundo aparato de descifrado según la tercera realización del segundo aspecto;
La Figura 54 es una vista que muestra un procedimiento de procesamiento detallado de un segundo proceso de descifrado según la tercera realización del segundo aspecto;
La Figura 55 es un diagrama de bloques funcional de un primer aparato de descifrado según una cuarta realización del segundo aspecto;
La Figura 56 es una vista que muestra un procedimiento de procesamiento detallado de un primer proceso de descifrado según la cuarta realización del segundo aspecto;
La Figura 57 es un diagrama de bloques funcional de un segundo aparato de descifrado según la cuarta realización del segundo aspecto;
La Figura 58 es una vista que muestra un procedimiento de procesamiento detallado de un segundo proceso de descifrado según la cuarta realización del segundo aspecto;
La Figura 59 es una vista que muestra una estructura ejemplo de datos intercambiados cuando la presente invención se aplica a un sistema de correo electrónico o un sistema de mensajería instantánea;
La Figura 60 es una vista estructural de un sistema criptográfico según cada ejemplo en un tercer aspecto relativo a la presente invención;
La Figura 61 es una vista (Nº 1) que muestra un procedimiento de procesamiento de un método de comunicación criptográfico según cada ejemplo en el tercer aspecto;
La Figura 62 es una vista (Nº 2) que muestra el procedimiento de procesamiento del método de comunicación criptográfico según cada ejemplo en el tercer aspecto;
La Figura 63 es una vista (Nº 3) que muestra el procedimiento de procesamiento del método de comunicación criptográfico según cada ejemplo en el tercer aspecto;
La Figura 64 es una vista (Nº 4) que muestra el procedimiento de procesamiento del método de comunicación criptográfico según cada ejemplo en el tercer aspecto;
La Figura 65 es un diagrama de bloques funcional de un aparato de cifrado según un primer ejemplo del tercer aspecto;

La Figura 66 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de cifrado según el primer ejemplo del tercer aspecto;
La Figura 67 es un diagrama de bloques funcional de un servidor de contenido según el primer ejemplo del tercer aspecto;
La Figura 68 es un diagrama de bloques funcional de un aparato de descifrado según el primer ejemplo del tercer aspecto;
La Figura 69 es una vista que muestra un procedimiento de procesamiento detallado de un segundo proceso de descifrado según el primer ejemplo del tercer aspecto;
La Figura 70 es un diagrama de bloques funcional de un aparato de generación de clave según el primer ejemplo del tercer aspecto;
La Figura 71 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de generación de clave según el primer ejemplo del tercer aspecto;
La Figura 72 es un diagrama de bloques funcional de un aparato de descifrado según un segundo ejemplo del tercer aspecto;
La Figura 73 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de descifrado según el segundo ejemplo del tercer aspecto;
La Figura 74 es un diagrama de bloques funcional de un aparato de generación de clave según el segundo ejemplo del tercer aspecto;
La Figura 75 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de generación de clave según el segundo ejemplo del tercer aspecto;
La Figura 76 es un diagrama de bloques funcional de un aparato de cifrado según un tercer ejemplo del tercer aspecto;
La Figura 77 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de cifrado según el tercer ejemplo del tercer aspecto;
La Figura 78 es un diagrama de bloques funcional de un aparato de descifrado según el tercer ejemplo del tercer aspecto;
La Figura 79 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de descifrado según el tercer ejemplo del tercer aspecto;
La Figura 80 es un diagrama de bloques funcional de un aparato de descifrado según un cuarto ejemplo del tercer aspecto;
La Figura 81 es una vista que muestra un procedimiento de procesamiento detallado de un proceso de descifrado según el cuarto ejemplo del tercer aspecto; y
La Figura 82 es una vista que muestra una estructura ejemplo de datos intercambiados en un sistema de entrega de contenidos en base al tercer aspecto.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES

Se describirán primero ejemplos según un primer aspecto relativo a la presente invención que se refiere a una tecnología de comunicación criptográfica que se basa en un cifrado de predicado y que puede operar flexiblemente.

(Primer ejemplo según el primer aspecto)

Un primer ejemplo según el primer aspecto se describirá más abajo con referencia a la Figura 1 hasta la Figura 17.

Como se muestra en la Figura 1, un sistema criptográfico 1 incluye una pluralidad de aparatos clientes 10 y 30, uno o una pluralidad de aparatos de generación de clave 20, uno o una pluralidad de aparatos de gestión de información de usuario 40 (en lo sucesivo cada uno llamado aparato de gestión), aparatos de gestión de par de información de regla de conversión 50 (en lo sucesivo cada uno llamado aparato de registro), uno o una pluralidad de aparatos de mantenimiento 80, y uno o una pluralidad de aparatos de autenticación 90. Estos aparatos pueden comunicar unos con otros a través de una red de comunicación 5, tal como Internet.

Los aparatos cliente funcionan como aparatos de cifrado o aparatos de descifrado en base a sus funciones de procesamiento. A la luz de sus funciones, los aparatos cliente se llaman aparatos de cifrado 10 o aparatos de descifrado 30. El sistema criptográfico 1 puede incluir aparatos cliente que funcionan solamente como aparatos de cifrado y/o aparatos cliente que funcionan solamente como aparatos de descifrado.

En el sistema criptográfico 1, el cifrado y el descifrado se realizan usando cifrado de predicado. En el primer aspecto, el algoritmo de cifrado de predicado a ser usado no está limitado, y se puede usar el algoritmo de cifrado de predicado descrito en la Bibliografía que no es de patente 3, por ejemplo. En el primer ejemplo del primer aspecto, se usará un algoritmo de cifrado de predicado de tipo KEM (el mecanismo de encapsulación de claves).

Un método de comunicación criptográfico usado en el sistema criptográfico 1 se describirá con referencia a las Figura 2, 3, 4, 6, 8, y 10. Ver las Figura 5, 7, y 9 para la estructura funcional de cada aparato.

<<Proceso de preparación>>

Una unidad de generación de parámetros (no mostrada) del aparato de generación de clave 20 genera una clave privada y una entrada usada en el algoritmo de cifrado de predicado (paso S1). La entrada incluye un parámetro

público (abreviado como un P público en las figuras) usado en el algoritmo de cifrado de predicado, la dirección del aparato de generación de clave 20, una lista de políticas que se pueden usar por el aparato de generación de clave 20, y una lista de esquemas que se pueden usar por el aparato de generación de clave 20.

El parámetro público incluye, por ejemplo, generar los elementos g_1, g_2, y g_T de los grupos cíclicos G_1, G_2, y G_T que tienen un orden q, una correspondencia bilineal no degenerada e: $G_1 \times G_2 \rightarrow G_T$ (donde $e(g_1, g_2) = g_T$), el orden q, y la base ortogonal B de un espacio de vector (n+1) dimensional V. La clave privada incluye la base ortogonal B* de un espacio de vector dual V*. Cuando la estructura algebraica es un campo finito F_q, q es un número primo o una potencia de un número primo. La correspondencia bilineal e es, por ejemplo, un emparejamiento Tate o un emparejamiento Weil.

La base ortogonal B y la base ortogonal B* se describirán a continuación. Se supone que un elemento arbitrario del espacio de vector (n+1) dimensional V se expresa como un elemento de un producto directo (n+1) dimensional G_1^{n+1} del grupo cíclico G_1, como se muestra la Expresión (1). Un elemento arbitrario de espacio de vector (n+1) dimensional V también se puede expresar usando la base canónica A del espacio de vector (n+1) dimensional V, como se muestra en la Expresión (2), donde a_i es un elemento del producto directo (n+1) dimensional G_1^{n+1}, z_i es un elemento de un producto directo (n+1) dimensional F_q^{n+1}, y 1 indica una identidad aditiva.

$$V : (g_1^{z_1}, \cdots, g_1^{z_{n+1}}) \in G_1^{n+1} \qquad (1)$$

$$V : z_1 a_1 + \cdots + z_{n+1} a_{n+1} \qquad (2)$$

$$A = (a_1, \cdots, a_{n+1}) = \begin{pmatrix} g_1 & 1 & \cdots & 1 \\ 1 & g_1 & & \vdots \\ \vdots & & \ddots & 1 \\ 1 & \cdots & 1 & g_1 \end{pmatrix}, \quad a_i \in G_1^{n+1}$$

$$z_i \in F_q^{n+1}$$

La base ortogonal B se obtiene aplicando una matriz cuadrada (n +1) dimensional X a la base canónica A, como se muestra en la Expresión (3), donde el símbolo T indica una transposición. La matriz X se mantiene secreta como la clave privada.

$$B = X \cdot A \qquad (3)$$

$$B = {}^T(b_1, \cdots, b_{n+1})$$

$$X = {}^T(x_1, \cdots, x_{n+1}) = (\chi_{ij})_{(n+1)\times(n+1)}, \quad \chi_{ij} \in F_q$$

$$x_i = (\chi_{i1}, \cdots, \chi_{i(n+1)})$$

$$b_i = \sum_{j=1}^{n+1} \chi_{ij} a_j = (g_1^{x_{i1}}, \cdots, g_1^{x_{i(n+1)}})$$

También se supone que un elemento arbitrario del espacio de vector dual V* que corresponde al espacio de vector V se expresa como un elemento de un producto directo (n +1) dimensional G_2^{n+1} del grupo cíclico G_2, como se muestra en la Expresión (4). Un elemento arbitrario del espacio de vector dual V* también se puede expresar usando la base canónica A* del espacio de vector dual V*, como se muestra en la Expresión (5), donde a_i* es un elemento del producto directo (n+1) dimensional G_2^{n+1}, y_i* es un elemento del producto directo (n+1) dimensional F_q^{n+1}, y 1 indica una identidad aditiva.

$$V^* : (g_2{}^{y_1}, \cdots, g_2{}^{y_{n+1}}) \in G_2{}^{n+1} \qquad (4)$$

$$V^* : y_1 a_1^* + \cdots + y_{n+1} a_{n+1}^* \qquad (5)$$

$$A^* = \left(a_1^*, \cdots, a_{n+1}^*\right) = \begin{pmatrix} g_2 & 1 & \cdots & 1 \\ 1 & g_2 & & \vdots \\ \vdots & & \ddots & 1 \\ 1 & \cdots & 1 & g_2 \end{pmatrix}, \quad a_i^* \in G_2{}^{n+1}$$

$$y_i \in F_q{}^{n+1}$$

La base ortogonal B* se obtiene aplicando una matriz cuadrada (n+1) dimensional ${}^T(X^{-1})$ a la base canónica A*, como se muestra en la Expresión (6), donde el símbolo E indica una matriz unidad.

$$B^* = {}^T(X^{-1}) \cdot A^* \qquad (6)$$

$$B^* = {}^T(b_1^*, \cdots, b_{n+1}^*)$$

$$b_i^* = \left(g_2{}^{x_{i1}^*}, \cdots, g_2{}^{x_{i(n+1)}^*}\right)$$

$$X \cdot {}^T(X^*) = E, \quad X^* = {}^T(X^{-1})$$

La lista de esquemas se describirá a continuación. Un par de elementos de información de regla de conversión se llama par de esquemas (ver las Figura 11 a 13): uno de los elementos de información de regla de conversión es una información (información de regla de conversión de atributo, o esquema de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (información de designación de atributo, es decir, información que identifica un atributo tal como un nombre o una fecha de nacimiento específicamente y únicamente, también llamado valor de atributo) a una información de atributo usada en el algoritmo de cifrado de predicado, y el otro de los elementos de información de regla de conversión es una información (información de regla de conversión de predicado, o esquema de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (información de designación de predicado, es decir, información que especifica una condición relacionada con un atributo, tal como una edad o una autoridad específicamente mediante una expresión lógica, también llamada función proposicional) a una información de predicado usada en el algoritmo de cifrado de predicado. Un conjunto (lista de datos) de uno o una pluralidad de pares de esquemas se llama lista de esquemas. Cada aparato de generación de clave 20 puede determinar una lista de esquemas de una manera deseada. Cada elemento de datos incluido en cada esquema en la lista de esquemas se escribe, por ejemplo, en XML (el Lenguaje de Marcas Extensible) o ASN.1 (el Número de Notación Abstracto Uno).

Un ejemplo del esquema de atributo mostrado en la Figura 12 se describirá más abajo. La información de designación de atributo de usuario (valor de atributo) está asociada con un nombre de atributo y un tipo de datos. En el ejemplo mostrado en la Figura 12, se especifica un tipo de datos 'cadena de caracteres' para un nombre de atributo 'correo electrónico 1', y el nombre de atributo 'correo electrónico 1' y el tipo de datos 'cadena de caracteres' se asocian con un valor de atributo 'XXX@XXX.ntt.co.jp', por ejemplo.

El esquema de atributo prescribe una regla de conversión en la que un número de elemento está asociado con un nombre de atributo y una función de conversión de tipo. En el ejemplo mostrado en la Figura 12, un número de elemento '1' está asociado con un nombre de atributo 'tipo de sangre' y una función de conversión de tipo, por ejemplo. La función de conversión de tipo que corresponde al número de elemento '1' convierte el valor de atributo a 0 cuando el valor de atributo del tipo de sangre es 'O', a 1 cuando el valor de atributo del tipo de sangre es 'A', a 2 cuando el valor de atributo del tipo de sangre es 'B', y a 3 cuando el valor de atributo del tipo de sangre es 'AB'. Los números de elemento '2' y '3' están asociados con un nombre de atributo "fecha de nacimiento" y funciones de conversión de tipo. Las funciones de conversión de tipo que corresponden a los números de elemento '2' y '3' convierten el año del valor de atributo de la fecha de nacimiento al valor de una función de cálculo de claves que tiene el año como la entrada para el número de elemento '2' y el día y el mes del valor de atributo de la fecha de nacimiento al valor de la función de cálculo de claves que tiene el día y el mes como la entrada para el número de elemento '3'.

Cuando se aplica el esquema de atributo ejemplo mostrado en la Figura 12 a la información de designación de atributo ejemplo (valor de atributo) de un usuario mostrado en la Figura 12, se obtiene una información de atributo ejemplo (información de vector) mostrada en la Figura 12. Esta información de atributo se puede considerar como un vector disponiendo las salidas de las funciones de conversión de tipo usando los números de elemento del esquema de atributo como los números de elemento del vector.

En la descripción anterior, las salidas de las funciones de conversión de tipo son enteros y los valores de salida de la función de cálculo de claves. En realidad, las salidas de las funciones de conversión de tipo dependen del algoritmo de cifrado de predicado y son, por ejemplo, elementos del campo finito F_q.

Un ejemplo del esquema de predicado mostrado en la Figura 13 se describirá más abajo. Como información de designación de predicado, se dan las expresiones lógicas que especifican condiciones para los atributos. En el ejemplo mostrado en la Figura 13, se da la información de designación de predicado de 'nombre = Taro Tanaka Y edad = 20 o más' que significa que el valor de atributo de un nombre de atributo 'nombre' es 'Taro Tanaka' y el valor de atributo de un nombre de atributo 'edad' es 20 o más.

El esquema de predicado prescribe una regla de conversión en la que un número de elemento está asociado con un nombre de atributo y una función de conversión de tipo. El ejemplo mostrado en la Figura 13, un número de elemento '1' está asociado con un nombre de atributo 'tipo de sangre' y una función de conversión de tipo, por ejemplo. La función de conversión de tipo que corresponde al número de elemento '1' convierte el valor de atributo a 0 cuando el valor de atributo del tipo de sangre es 'O', a 1 cuando el valor de atributo del tipo de sangre es 'A', a 2 cuando el valor de atributo del tipo de sangre es 'B', y a 3 cuando el valor de atributo del tipo de sangre es 'AB'. Los números de elemento '2' y '3' están asociados con un nombre de atributo "fecha de nacimiento" y funciones de conversión de tipo. Las funciones de conversión de tipo que corresponden a los números de elemento '2' y '3' convierten el año del valor de atributo de la fecha de nacimiento al valor de una función de cálculo de claves que tiene el año como la entrada para el número de elemento '2' y el día y el mes del valor de atributo de la fecha de nacimiento al valor de la función de cálculo de claves que tiene el día y el mes como la entrada para el número de elemento '3'.

Cuando el esquema de predicado ejemplo mostrado en la Figura 13 se aplica a la información de designación de predicado ejemplo mostrada en la Figura 13, se obtiene una información de predicado ejemplo (información de vector) mostrada en la Figura 13. Específicamente, en este ejemplo, el esquema de predicado se aplica a la información de designación de predicado para obtener un polinomio de variable múltiple f que tiene variables que corresponden a los números de elemento, y el polinomio de variable múltiple f se convierte a una información de vector para obtener una información de predicado (información de vector). Este proceso se describirá más abajo usando la información de designación de predicado ejemplo mostrada en la Figura 13. Cuando se aplica el esquema de predicado a la información de designación de predicado de 'nombre = Taro Tanaka Y edad = 20 o más', se obtienen el valor de salida 'Cálculo de clave(Taro Tanaka)' de la función de conversión de tipo que corresponde a un número de elemento '0' y el valor de salida '1' de la función de conversión de tipo que corresponde a un número de elemento '23'. Un polinomio con un grado de uno con respecto a una variable X_0 que corresponde al número de elemento '0', que tiene el valor de salida 'Cálculo de clave(Taro Tanaka)' de función de conversión de tipo que corresponde al número de elemento '0' como un cero, y un polinomio con un grado de uno con respecto a una variable X_{23} que corresponde al número de elemento '23', que tiene el valor de salida '1' de la función de conversión de tipo que corresponde al número de elemento '23' como un cero, se combinan linealmente para obtener un polinomio de variable múltiple $f = r_1(X_0 - H(\text{Taro Tanaka})) + r_2(X_{23}-1)$, donde r_1 y r_2 son números aleatorios. Entonces, este polinomio de variable múltiple f se expande y los coeficientes de los términos se disponen a convertir el polinomio de variable múltiple f a una información de vector. El ejemplo de la información de predicado (información de vector) mostrado en la Figura 13 se obtiene de esta manera.

En la descripción anterior, las salidas de las funciones de conversión de tipo son enteros o los valores de salida de la función de cálculo de claves. En realidad, las salidas de las funciones de conversión de tipo dependen del algoritmo de cifrado de predicado y son, por ejemplo, elementos del campo finito F_q.

Ambos esquemas que constituyen un par de esquemas necesitan tener las mismas combinaciones de nombres de atributo y funciones de conversión de tipo, los mismos tipos de datos de valores de atributo a ser introducidos, y similares.

La lista de políticas se describirá a continuación con referencia a la Figura 14. Una información que identifica o bien el esquema de atributo o bien el esquema de predicado se llama información de política (en lo sucesivo llamada sólo política). Una lista de datos en la que está escrita la política se llama lista de política. Cuando el aparato de generación de clave 20 usa tanto el esquema de atributo como el esquema de predicado, se preparan dos tipos de políticas:

Cipher_Text_Policy y Key_Policy. Cuando el aparato de generación de clave 20 usa solamente el esquema

de atributo, sólo se prepara un tipo de política:

Key_Policy. Cuando el aparato de generación de clave 20 usa solamente el esquema de predicado, sólo se prepara un tipo de política:
Cipher_Text_Policy. La política se escribe, por ejemplo, con XML (el Lenguaje de Marcas Extensible) o ASN.1 (el Número de Notación Abstracto Uno). El aparato de generación de clave 20 puede determinar libremente el objetivo de política: solamente el esquema de atributo, solamente el esquema de predicado, o tanto el esquema de atributo como el esquema de predicado.

Después del proceso del paso S1, una unidad de transmisor del aparato de generación de clave 20 envía la entrada al aparato de autenticación 90, y una unidad de receptor del aparato de autenticación 90 recibe la entrada (paso S2). Una unidad de asignación de firmas (no mostrada) del aparato de autenticación 90 asigna una firma electrónica a la entrada con, por ejemplo, un método convencional (paso S3), una unidad de transmisor del aparato de autenticación 90 envía la entrada con la firma al aparato de generación de clave 20, y una unidad de receptor del aparato de generación de clave 20 recibe la entrada con la firma (paso S4). Entonces, la unidad de transmisor del aparato de generación de clave 20 envía la entrada con la firma al aparato de mantenimiento 80, y una unidad de receptor del aparato de mantenimiento 80 recibe la entrada con la firma (paso S5).

Una unidad de transmisor del aparato de mantenimiento 80 envía una consulta de búsqueda, la cual incluye información (tal como una dirección) que identifica el aparato de generación de clave 20, al aparato de registro 50, y una unidad de receptor del aparato de registro 50 recibe la consulta de búsqueda (paso S6). Una unidad de búsqueda (no mostrada) del aparato de registro 50 busca el contenido registrado (entrada) que concierne al aparato de generación de clave 20 (paso S7), una unidad de transmisor del aparato de registro 50 envía un resultado de la búsqueda, el cual incluye si se ha hecho un registro y el contenido registrado, al aparato de mantenimiento 80, y la unidad de receptor del aparato de mantenimiento 80 recibe el resultado de la búsqueda (paso S8).

Una unidad de comprobación (no mostrada) del aparato de mantenimiento 80 compara la entrada con la firma recibida en el proceso del paso S5 con el resultado de la búsqueda recibido en el proceso del paso S8 para comprobar si la entrada ya ha sido registrada (paso S9). Si se determina que la entrada no ha sido registrada aún, la unidad de transmisor del aparato de mantenimiento 80 envía la entrada con la firma al aparato de registro 50, y la unidad de receptor del aparato de registro 50 recibe la entrada con la firma (paso S10). Una unidad de registro (no mostrada) del aparato de registro 50 almacena la entrada con la firma en una unidad de almacenamiento del aparato de registro 50 en asociación con el aparato de generación de clave 20 (paso S11). La unidad de transmisor del aparato de registro 50 envía el resultado del registro al aparato de mantenimiento 80, y la unidad de receptor del aparato de mantenimiento 80 recibe el resultado del registro (paso S12). La unidad de transmisor del aparato de mantenimiento 80 envía el resultado de registro al aparato de generación de clave 20, y el aparato de generación de clave 20 recibe el resultado del registro (paso S13).

Cuando se proporciona una pluralidad de aparatos de generación de clave 20, cada uno de la pluralidad de aparatos de generación de clave 20 realiza separadamente los procesos del paso S1 al paso S13. Por ejemplo, cada aparato de generación de clave especifica un parámetro público y una clave privada. No obstante, esto no impide que cada aparato de generación de clave tenga un parámetro público común y una clave privada común. Los aparatos de generación de clave pueden registrar sus entradas en el mismo aparato de registro 50 o en diferentes aparatos de registro 50.

Cuando la clave privada y la entrada se especifican por adelantado y la entrada se registra en el aparato de registro 50 por adelantado, se pueden omitir los procesos desde el paso S1 al paso S13.

El aparato de autenticación 90 y aparato de mantenimiento 80 pueden ser la misma entidad hardware. El sistema criptográfico 1 puede tener una estructura de sistema que no tiene ningún aparato de mantenimiento 80, ningún aparato de autenticación 90, o ningún aparato de mantenimiento 80 y ningún aparato de autenticación 90 cuando no se requiere autenticación para registrar una entrada o cuando se garantiza que una unicidad de la entrada se registra en el aparato de registro 50.

La descripción del <<proceso de preparación>> finaliza aquí.

<<Proceso de cifrado>>
Bajo el control de una unidad de controlador, no mostrada, una unidad de transmisor 14 del aparato de cifrado 10 envía una consulta de búsqueda al aparato de registro 50, y la unidad de recepción del aparato de registro 50 recibe la consulta de búsqueda (paso S14). La unidad de búsqueda del aparato de registro 50 busca algunas o todas las entradas registradas en la unidad de almacenamiento del aparato de registro 50 y elige una entrada (paso S15). La unidad de transmisor del aparato de registro 50 envía la entrada al aparato de cifrado 10, y una unidad de receptor del aparato de cifrado 10 recibe la entrada (paso S16). Esta entrada incluye la dirección del aparato de generación de clave, el parámetro público y el aparato de generación de clave, la lista de políticas que se puede usar por el aparato de generación de clave, y la lista de esquemas que se puede usar por el aparato de generación de clave. La

entrada recibida se almacena en una memoria 11 del aparato de cifrado 10.

Cuando el aparato de cifrado 10 tiene el parámetro público, la lista de esquemas, la lista de políticas, y una dirección de cada aparato de generación de clave 20 por adelantado, se omiten los procesos de los pasos S14 a S16. Se debería señalar que el sistema criptográfico 1 puede no tener aparato de registro 50.

Una primera unidad de adquisición de información de lógica de predicado 12 del aparato de cifrado 10 lee la información de entrada, la política, y los esquemas de la memoria 11 y obtiene una información de atributo (en lo sucesivo llamada primera información de atributo) y una información de predicado (en lo sucesivo llamada primera información de predicado) (paso S17a). Los detalles de este proceso se describirán más abajo con referencia a las Figura 12 y 13.

Cuando la lista de esquemas tiene una pluralidad de pares de esquemas, se selecciona un par de esquemas en base al uso o similar. El usuario del aparato de cifrado 10 puede seleccionar un par de esquemas y una información de designación de entrada del mismo. Alternativamente, la primera unidad de adquisición de información de lógica de predicado 12 puede seleccionar un par de esquemas según una regla predeterminada.

Según si la información de entrada es una información de designación de atributo o una información de designación de predicado, se selecciona uno de los esquemas junto con la política. El usuario del aparato de cifrado 10 puede seleccionar la política y uno de los esquemas y una información de designación de entrada de los mismos. Alternativamente, la primera unidad de adquisición de información de lógica de predicado 12 puede seleccionar la política y uno de los esquemas según una regla predeterminada. Cuando solamente se prepara un tipo de política en el aparato de generación de clave 20, se selecciona un esquema del par de esquemas según la política. Si el esquema seleccionado no corresponde al tipo de la información de entrada, necesita ser seleccionado de nuevo un par de esquemas de la lista de esquemas o necesita ser proporcionada de nuevo una entrada por el aparato de registro 50.

La información de entrada puede ser una información introducida por el usuario del aparato de cifrado 10 o una información adquirida por una unidad de adquisición (no mostrada) del aparato de cifrado 10 desde un medio de almacenamiento tal como una tarjeta IC 39.

Entonces, la primera unidad de adquisición de información de lógica de predicado 12 usa el esquema seleccionado a partir del par de esquemas según la política para obtener la primera información de atributo o la primera información de predicado a partir de la información de entrada. Cuando la política es Key_Policy y el esquema seleccionado es un esquema de atributo, se obtiene la primera información de atributo. Cuando la política es Cipher_Text_Policy y el esquema seleccionado es un esquema de predicado, se obtiene la primera información de predicado. La primera información de atributo y la primera información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes en el primer ejemplo según el primer aspecto (ver las Figura 11 a 13). El esquema se usa para extraer o disponer los valores de atributos necesarios a partir de la información de entrada.

A continuación, una unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, una base ortogonal B (clave pública sustancial) incluida en el parámetro público leído de la memoria 11, y un texto plano M para obtener una clave común K, información de cifrado C_1, y texto de cifrado C_2 (pasos S17b y S17c). Los detalles de estos procesos se describirán más abajo. Cuando el primer ejemplo del primer aspecto se dedica a la entrega de la clave común K, no es necesario generar el texto de cifrado C_2.

Una primera unidad de cifrado 13a genera unos números aleatorios r y ρ que son elementos del campo finito F_q según el algoritmo de cifrado de predicado, especifica la clave común K como se muestra por la Expresión (7), y obtiene la información de cifrado C_1 según la Expresión (8) (paso S17b), donde H indica, por ejemplo, una función de cálculo de claves. En este ejemplo, se usa la primera información de atributo v. Para usar la primera información de predicado, v necesita ser sustituida con w en la Expresión (8). En este ejemplo, la información de cifrado C_1 corresponde a ρ usado para generar la clave común K. La información de cifrado C_1 puede corresponder a la clave común K.

$$K = H(g_T{}^{\rho}) \qquad (7)$$

$$C_1 = r\sum_{i=1}^{n} v_i b_i + \rho b_{n+1} \qquad (8)$$

A continuación, la segunda unidad de cifrado 13b usa la clave común K y el texto plano M para obtener el texto de cifrado C_2 según la Expresión (9) (paso S17c). Un método de cifrado Enc_k que usa la clave privada puede ser un

método conocido. Por ejemplo, puede ser el método descrito en la Bibliografía que no es de patente 1. Como se describió anteriormente, cuando el primer ejemplo del primer aspecto se dedica a la entrega de la clave común K, se omite el proceso del paso S17c. En otras palabras, el aparato de cifrado 10 tiene incluso la función de la segunda unidad de cifrado 13b pero no realiza el proceso del paso S17c.

$$C_2 = Enc_K(M) \qquad (9)$$

A continuación, bajo el control de la unidad de controlador, la unidad de transmisor 14 del aparato de cifrado 10 genera un mensaje cifrado que incluye la información de cifrado C_1 y el texto de cifrado C_2 (si es necesario), junto con el par de esquemas, la política, el parámetro público, y la dirección del aparato de generación de clave leídos de la memoria 11 (paso S17d). La unidad de transmisor 14 del aparato de cifrado 10 envía entonces el mensaje cifrado al aparato de descifrado 30, y una unidad de receptor del aparato de descifrado 30 recibe el mensaje cifrado (paso S18).

La descripción del <<proceso de cifrado>> finaliza aquí.

<<Proceso de descifrado>>
Bajo el control de una unidad de controlador, no mostrada, una unidad de transmisor 34 del aparato de descifrado 30 envía una consulta de búsqueda que incluye la dirección del aparato de generación de clave, la dirección que se incluye en el mensaje cifrado, al aparato de registro 50, y la unidad de recepción del aparato de registro 50 recibe la consulta de búsqueda (paso S19). La unidad de búsqueda del aparato de registro 50 busca la entrada del aparato de generación de clave especificada por la dirección y la selecciona (paso S20). La unidad de transmisor del aparato de registro 50 envía la entrada del resultado de la búsqueda al aparato de descifrado 30, y la unidad de receptor del aparato de descifrado 30 recibe la entrada (paso S21). Esta entrada incluye la dirección del aparato de generación de clave, el parámetro público del aparato de generación de clave, la lista de políticas que se pueden usar por el aparato de generación de clave, y la lista de esquemas que se pueden usar por el aparato de generación de clave. La entrada recibida se almacena en una memoria 31 del aparato de descifrado 30.

Cuando el aparato de descifrado 30 tiene el parámetro público, la lista de esquemas, la lista de políticas, y la dirección de cada aparato de generación de clave 20 por adelantado, se omiten los procesos de los pasos S19 a S21. En ese caso, el aparato de descifrado 30 busca en la memoria 31 la entrada del aparato de generación de clave que corresponde a la dirección incluida en el mensaje cifrado y la recupera.

Bajo el control de la unidad de controlador, una unidad de verificación (no mostrada) del aparato de descifrado 30 verifica que el par de esquemas y la política incluidos en el mensaje cifrado se incluyen en la lista de esquemas y la lista de políticas incluidas en la entrada obtenida desde el aparato de registro 50 (paso S22a). Si esta verificación falla, el proceso finaliza con un fallo de procesamiento de descifrado (paso S22g).

Cuando la verificación tiene éxito, una unidad de adquisición 32 del aparato de descifrado 30 lee la información de designación de atributo o la información de designación de predicado que corresponde al usuario del aparato de descifrado 30 de un medio de almacenamiento tal como la tarjeta IC 39 (paso S22f). Si se lee la información de designación de atributo o la información de designación de predicado depende de la política incluida en el mensaje cifrado. Más específicamente, la información de designación leída corresponde al contenido de la política que identifica un esquema emparejado con el otro esquema identificado por la política incluida en el mensaje cifrado. Cuando la política es Cipher_Text_Policy, la unidad de adquisición 32 lee la información de designación de atributo del medio de almacenamiento. Cuando la política es Key_Policy, la unidad de adquisición 32 lee la información de designación de predicado del medio de almacenamiento. La información de designación leída en lo sucesivo se llama información de usuario. La unidad de adquisición 32 del aparato de descifrado 30 puede leer del aparato de gestión 40 la información de designación de atributo o la información de designación de predicado que corresponde al usuario del aparato de descifrado 30, de la misma forma que en <<un proceso de adquisición de información de usuario>> en el aparato de generación de clave 20, descrito más tarde. En el primer ejemplo del primer aspecto, se puede omitir el proceso del paso S22f. Cuando el aparato de descifrado 30 tiene la información de designación de atributo y la información de designación de predicado que corresponde al usuario por adelantado, o bien la información de designación de atributo o bien la información de designación de predicado sirve como información de usuario, según la política.

A continuación, la unidad de verificación del aparato de descifrado 30 verifica que el aparato descifrado 30 tiene la clave de descifrado a ser usada para descifrar la información de cifrado incluida en el mensaje de cifrado (paso S22b).

El aparato de descifrado 30 almacena una tabla de claves de descifrado en la memoria 31. En la tabla de claves de descifrado, como se muestra en la Figura 15, por ejemplo, el identificador de cada aparato de generación de clave está asociado con el parámetro público, el par de esquemas, el objetivo de clave de descifrado, la información de designación de predicado, y la clave de descifrado. La unidad de verificación verifica que el aparato de descifrado 30

tiene la clave de descifrado que corresponde al identificador del aparato de generación de clave determinado a partir de la dirección incluida en el mensaje cifrado, al parámetro público, al par de esquemas, y al objetivo de clave de descifrado (que corresponde al contenido de la política que identifica un esquema emparejado con el otro esquema identificado por la política incluida en el mensaje cifrado). Cuando el aparato de descifrado 30 tiene la clave de descifrado, se realizará el proceso del paso S29. Si el aparato de descifrado 30 no tiene la clave de descifrado, se realizará el proceso del paso S23.

La descripción del <<proceso de descifrado>> se detiene temporalmente aquí y se describirá más abajo <<un proceso de generación de clave>>.

Si el aparato de descifrado 30 no tiene la clave de descifrado, la unidad de trasmisor 34 del aparato de descifrado 30 genera, bajo el control de la unidad de controlador, un mensaje de petición de clave que incluye el parámetro público, la política, el par de esquemas, la información de usuario (en su caso), y la información de autenticación, todos estos elementos que se leen de la memoria 31. La información de autenticación incluye, por ejemplo, el ID del usuario y una contraseña. La unidad de trasmisor 34 del aparato de descifrado 30 envía el mensaje de petición de clave al aparato de generación de clave que ha leído la dirección de la memoria 31, y la unidad de receptor del aparato de generación de clave 20 recibe el mensaje de petición de clave (paso S23). El mensaje de petición de clave recibido se almacena en una memoria 21 del aparato de generación de clave 20.

Bajo el control de una unidad de controlador, una unidad de verificación (no mostrada) del aparato de generación de clave 20 verifica que el par de esquemas y la política incluida en el mensaje de petición de clave se incluyen en la lista de esquemas y la lista de políticas incluidas en la entrada propiedad del aparato de generación de clave 20 (por ejemplo, la entrada generada en el paso S1) y que el parámetro público incluido en el mensaje de petición de clave es idéntico al parámetro público del aparato de generación de clave 20 (paso S24a). Si esta verificación falla, el proceso finaliza con un fallo del proceso de generación de clave (paso S24g). Cuando la información de autenticación se incluye en el mensaje de petición de clave, la información de autenticación también se verifica en el proceso del paso S24a. El aparato de generación de clave 20 almacena una tabla de autenticación en la memoria 21. En la tabla de autenticación, como se muestra la Figura 16, por ejemplo, cada ID de usuario está asociado con una contraseña. La unidad de verificación verifica que el ID de usuario y la contraseña incluidos en el mensaje de petición de clave son idénticos al ID de usuario y la contraseña incluidos en la tabla de autenticación. Si la verificación falla, se realiza el proceso del paso S24g.

Cuando esta verificación tiene éxito, la unidad de verificación del aparato de generación de clave 20 verifica que el mensaje de petición de clave incluye la información de usuario (paso S24b). Cuando el mensaje de petición de clave incluye la información de usuario, se realizará el proceso del paso S24c. Si el mensaje de petición de clave no incluye la información de usuario, se realizará el proceso del paso S25. Cuando se emplea un método en el que un mensaje de petición de clave siempre incluye una información de usuario, el proceso del paso S24b y <<un proceso de adquisición de información de usuario>>, descritos más tarde, son innecesarios.

La descripción del <<proceso de generación de clave>> se detiene temporalmente aquí y el <<proceso de adquisición de información de usuario>> se describirá más abajo.

La unidad de trasmisor 24 del aparato de generación de clave 20 envía una petición que incluye la política y la información de autenticación (en su caso) incluidas en el mensaje de petición de clave al aparato de gestión 40, y el aparato de gestión 40 recibe la petición (paso S25). La petición recibida se almacena en una memoria del aparato de gestión 40.

El aparato de gestión 40 almacena una tabla de autenticación en la memoria. De la misma forma que en la tabla de autenticación descrita anteriormente, el ID de usuario se asocia con la contraseña en esta tabla de autenticación (ver la Figura 16). Una unidad de verificación (no mostrada) del aparato de gestión 40 verifica que el ID de usuario y la contraseña incluidos en la petición son idénticos al ID de usuario y la contraseña incluidos en la tabla de autenticación.

Cuando esta verificación tiene éxito, una unidad de búsqueda (no mostrada) del aparato de gestión 40 busca una tabla de información de usuario almacenada en la memoria de la información de designación de atributo o la información de designación de predicado según la política incluida en la petición (paso S26). La tabla de información de usuario incluye, por ejemplo, una primera tabla formada de cada ID de usuario, y un nombre de atributo y una información de designación de atributo asociados con el ID del usuario, y una segunda tabla formada del ID de usuario y la información de designación de predicado asociada con el ID de usuario (ver la Figura 17). Si se lee la información de designación de atributo o la información de designación de predicado se determina por la política incluida en la petición. Más específicamente, la información leída corresponde al contenido de una política que identifica el esquema emparejado con el otro esquema identificado por la política incluida en la petición. Cuando la política es Cipher_Text_Policy, la unidad de búsqueda lee la información de designación de atributo que corresponde al ID de usuario incluido en la petición de la primera tabla. Cuando la política es Key_Policy, la unidad de búsqueda lee la información de designación de predicado que corresponde al ID de usuario incluido en la petición

de la segunda tabla. La información de designación leída se llama en lo sucesivo información de usuario.

Bajo el control de una unidad de controlador, una unidad de trasmisor del aparato de gestión 40 envía la información de usuario al aparato de generación de clave 20, y la unidad de receptor del aparato de generación de clave 20 recibe la información de usuario (paso S27). La información de usuario recibida se almacena en la memoria 21 del aparato de generación de clave 20.

La descripción del <<proceso de adquisición de información de usuario>> finaliza aquí, y se resumirá la descripción del <<proceso de generación de clave>>.

Cuando el aparato de generación de clave 20 ya tiene la información de usuario o recibe la información de usuario a través del proceso de adquisición de información de usuario (paso S27), una segunda unidad de adquisición de información de lógica de predicado 23 del aparato de generación de clave 20 lee la política, el par de esquemas, el parámetro público, y la información de usuario de la memoria 21, y obtiene una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (segunda información de predicado) a partir de la información de usuario (paso S24c). En este proceso, el esquema emparejado con el esquema identificado por la política se aplica a la información de usuario. Cuando la política es Cipher_Text_Policy, el esquema (esquema de atributo) emparejado con el esquema (esquema de predicado) identificado por Cipher_Text_Policy se usa para obtener la segunda información de atributo a partir de la información de usuario (información de designación de atributo). Cuando la política es Key_Policy, el esquema (esquema de predicado) emparejado con el esquema (esquema de atributo) identificado por Key_Policy se usa para obtener la segunda información de predicado a partir de la información de usuario (información de designación de predicado). Se debería señalar que el esquema emparejado con el esquema usado en el paso S17a se usa en este proceso. En el primer ejemplo del primer aspecto, la segunda información de atributo y la segunda información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes (ver las Figura 11 a 13). El esquema se usa para extraer y disponer los valores de atributos necesarios a partir de la información de entrada.

A continuación, una unidad de generación de clave 25 del aparato de generación de clave 20 genera un número aleatorio α que es un elemento del campo finito F_q, en base al parámetro público q según el algoritmo de cifrado de predicado, y usa el numero aleatorio α, la segunda información de atributo $v_{(p)} = (v_{(p)1}, \ldots, v_{(p)n})$ o la segunda información de predicado $w_{(p)} = (w_{(p)1}, \ldots, w_{(p)n})$ leídos de la memoria 21 y una clave privada B* del aparato de generación de clave para obtener una clave de descifrado R según la Expresión (10) (paso S24d). La segunda información de predicado $w_{(p)}$ se usa en este ejemplo debido a que la información de entrada usada en el proceso de cifrado es la información de designación de atributo. Cuando la información de entrada es la información de designación de predicado, se usa la segunda información de atributo $v_{(p)}$. Por lo tanto, $w_{(p)}$ necesita ser sustituida con $v_{(p)}$ en la Expresión (10).

$$R = \alpha \sum_{i=1}^{n} w_{(p)i} b_i^* + b_{n+1}^* \qquad (10)$$

A continuación, bajo el control de la unidad de controlador, la unidad de transmisor 24 del aparato de generación de clave 20 envía la clave de descifrado R al aparato de descifrado 30, y la unidad de receptor del aparato de descifrado 30 recibe la clave de descifrado R (paso S28). La clave de descifrado R recibida se almacena en la memoria 31 del aparato de descifrado 30.

La descripción del <<proceso de generación de clave>> finaliza aquí, y se resumirá la descripción del <<proceso de descifrado>>.

Cuando el aparato de descifrado 30 ya tiene la clave de descifrado o recibe la clave de descifrado a través del proceso de generación de clave (paso S28), una unidad de descifrado 33 del aparato de descifrado 30 lee el parámetro público, la clave de descifrado R, la información de cifrado C_1, y el texto de cifrado C_2 (si es necesario) de la memoria 31, y obtiene la clave común K y el texto plano M (si es necesario) (paso S29).

Los detalles del proceso en el paso S29 se describirán más abajo. Una primera unidad de descifrado 33a lee el parámetro público, la clave de descifrado R, y la información de cifrado C_1 de la memoria 31, y obtiene $e(C_1, R)$ según el algoritmo de cifrado de predicado. Como se muestra en la Expresión (11), el resultado del cálculo depende del resultado de producto interior canónico de la primera información de atributo v y la segunda información de predicado $w_{(p)}$ sacada de la información de cifrado C_1 y la clave de descifrado R según una bilinealidad cuando la información de entrada es la información de designación de atributo. Cuando la información de entrada es la información de designación de predicado, v necesita ser sustituida con $v_{(p)}$ y $w_{(p)}$ necesita ser sustituida con w en la Expresión (11). El resultado del cálculo depende del resultado del producto interior canónico de la primera información de predicado w y la segunda información de atributo $v_{(p)}$ sacada de la información de cifrado C_1 y la clave de descifrado R según una bilinealidad. En la Expresión (11), $e(b_i, b_i^*)$ se define como se muestra en la

Expresión (12), donde δ_{ij} es el símbolo de la delta de Kronecker.

$$e(C_1,R) = e(r\sum_{i=1}^{n} v_i b_i, R)\cdot e(\rho b_{n+1}, R)$$
$$= \prod_{i=1}^{n} e(b_i, b_i^*)^{r\alpha v_i w_{(p)i}} \cdot e(b_{n+1}, b_{n+1}^*)^{\rho}$$
$$= g_T{}^{r\alpha \sum_{i=1}^{n} v_i w_{(p)i}} \cdot g_T{}^{\rho}$$
$$= g_T{}^{r\alpha \cdot v \cdot w_{(p)}} \cdot g_T{}^{\rho} \qquad (11)$$

$$e(b_i, b_j^*) = \prod_{j=1}^{n+1} e(g_1^{\chi_{ij}}, g_2^{\chi_{ij}^*})$$
$$= g_T{}^{\sum_{j=1}^{n+1} \chi_{ij}\chi_{ij}^*}$$
$$= g_T{}^{x_i \cdot {}^T x_j^*}$$
$$= g_T{}^{\delta_{ij}} \qquad (12)$$

Por lo tanto, cuando el producto interior canónico de la primera información de atributo v y la segunda información de predicado $w_{(p)}$ es cero (o cuando el producto interior canónico de la primera información de predicado w y la segunda información de atributo $v_{(p)}$ es cero), se obtiene el resultado del cálculo en la Expresión (11), $g_T{}^{\rho}$. Cuando se obtiene el resultado del cálculo, $g_T{}^{\rho}$, la primera unidad de descifrado 33a del aparato de descifrado 30 obtiene la clave común K, que es correcta, según la Expresión (7) (paso S22c). Cuando el producto interior canónico de la primera información de atributo v y la segunda información de predicado $w_{(p)}$ no es cero (o cuando el producto interior canónico de la primera información de predicado w y la segunda información de atributo $v_{(p)}$ no es cero), la primera unidad de descifrado 33a obtiene un valor incorrecto según la Expresión (7). En este ejemplo, se supone que la función de cálculo de claves H es común al sistema o está incluida en el parámetro público. La información de cifrado C_1 se corresponde a la información ρ usada para generar la clave común K en este ejemplo. Cuando la información de cifrado C_1 corresponde a la clave común K, el resultado del cálculo en la Expresión (11) es la clave común K (o un valor incorrecto). En otras palabras, un usuario autorizado del aparato de descifrado 30 tiene una información de designación de predicado que da la segunda información de predicado $w_{(p)}$ que hace el producto interior canónico con la primera información de atributo v cero, o una información de designación de atributo que da la segunda información de atributo $v_{(p)}$ que hace el producto interior canónico con la primera información de predicado w cero.

Entonces, una segunda unidad de descifrado 33b usa la clave común K y el texto cifrado C_2 para calcular el texto plano M según la Expresión (13) (paso S22d). Un método de descifrado Dec_k que usa la clave privada corresponde al método de cifrado Enc_k. Como se describió anteriormente, cuando el primer ejemplo del primer aspecto se dedica a la entrega de la clave común K, se omite el proceso del paso S22d. Más específicamente, incluso si el aparato de descifrado 30 tiene la función de la segunda unidad de descifrado 33b, no realiza el proceso del paso S22d.

$$M = Dec_K(C_2) \qquad (13)$$

Si el resultado del cálculo en la Expresión (11) es un valor incorrecto, el texto plano correcto M no se puede obtener mediante la Expresión (13).

El aparato de descifrado 30 puede almacenar la clave de descifrado R en la tabla de claves de descifrado. Además, el aparato de descifrado 30 puede almacenar la clave común K en la tabla de claves de descifrado.

La descripción del <<proceso de descifrado>> finaliza aquí.

(Segundo ejemplo según el primer aspecto)
Un segundo ejemplo del primer aspecto difiere del primer ejemplo del primer aspecto en que el aparato de

descifrado 30 genera la segunda información de atributo o la segunda información de predicado. Debido a esta diferencia, el segundo ejemplo del primer aspecto difiere en varios puntos del primer ejemplo del primer aspecto. Una descripción de las partes en común entre el primer y el segundo ejemplos del primer aspecto se omite (los mismos números de referencia se asignan a los mismos componentes), y una descripción de las diferencias del primer ejemplo del primer aspecto se hará con referencia a las Figura 18 a 21.

Los procesos de los pasos S1 a S22b son los mismos que aquéllos en el primer ejemplo del primer aspecto.

Cuando la clave de descifrado no se posee en el proceso del paso S22b, una segunda unidad de adquisición de información de lógica de predicado 35 del aparato de descifrado 30 lee la política, el par de esquemas, el parámetro público, y la información de usuario de la memoria 31 y obtiene una información de atributo (llamada segunda información de atributo) o una información de predicado (llamada segunda información de predicado) a partir de la información de usuario (paso S23g). En este proceso, el esquema emparejado con el esquema identificado por la política se aplica a la información de usuario. Cuando la política es Cipher_Text_Policy, el esquema (esquema de atributo) emparejado con el esquema (esquema de predicado) identificado por Cipher_Text_Policy se usa para obtener la segunda información de atributo a partir de la información de usuario (información de designación de atributo). Cuando, la política es Key_Policy, el esquema (esquema de predicado) emparejado con el esquema (esquema de atributo) identificado por Key_Policy se usa para obtener la segunda información de predicado a partir de la información de usuario (información de designación de predicado). Se debería señalar que el esquema emparejado con el esquema usado en el paso S17a se usa en este proceso. En el segundo ejemplo del primer aspecto, la segunda información de atributo y la segunda información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes (ver las Figura 11 a 13).

Después del proceso del paso S23g, se realiza el proceso de paso 23. En este proceso, la unidad de trasmisor 34 del aparato de descifrado 30 genera un mensaje de petición de clave que incluye el parámetro público, la política, el par de esquemas, y la información de autenticación leídos de la memoria 31, y la segunda información de atributo o la segunda información de predicado, bajo el control de la unidad de controlador. La unidad de trasmisor 34 del aparato de descifrado 30 envía el mensaje de petición de clave al aparato de generación de clave que ha leído la dirección de la memoria 31, y la unidad de receptor del aparato de generación de clave 20 recibe el mensaje de petición de clave.

Cuando la verificación tiene éxito en el proceso del paso S24a, se realiza el proceso del paso S24d. Dado que el aparato de generación de clave 20 ha recibido la segunda información de atributo o la segunda información de predicado desde el aparato de descifrado 30, la función y el proceso para generar la información son innecesarios, a diferencia del primer ejemplo del primer aspecto.

Los procesos de los pasos S28 y S29, a ser realizados después del proceso del paso S24d, son los mismos que aquéllos en el primer ejemplo del primer aspecto.

(Tercer ejemplo según el primer el primer aspecto)
Un tercer ejemplo del primer aspecto difiere del primer ejemplo del primer aspecto en que la unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, junto con la clave pública incluida en el parámetro público y el texto plano M leídos de la memoria 11, para obtener un información de cifrado C_1. En otras palabras, el algoritmo de cifrado de predicado descrito en la Bibliografía que no es de patente 3, por ejemplo, se usa en el tercer ejemplo del primer aspecto. Debido a esta diferencia, el tercer ejemplo del primer aspecto difiere en varios puntos del primer ejemplo del primer aspecto. Una descripción de las partes en común entre el primer y tercer ejemplos del primer aspecto se omite (los mismos números de referencia se asignan a los mismos componentes), y una descripción de las diferencias del primer ejemplo del primer aspecto se hará con referencia a las Figura 22 a 25.

Los procesos de los pasos S1 a S17a son los mismos que aquéllos en el primer ejemplo del primer aspecto. El parámetro público y alguna otra información se requieren por el algoritmo de cifrado de predicado del tercer ejemplo del primer aspecto. Para una información específica requerida, ver la Bibliografía que no es de patente 3, descrita anteriormente, por ejemplo.

En el proceso del paso S17b1, que sigue al proceso del paso S17a, la unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, junto con la clave pública incluida en el parámetro público y el texto plano M leídos de la memoria 11, para obtener una información de cifrado C_1 según el algoritmo de cifrado de predicado (paso S17b1).

Después del proceso del paso S17b1, se realiza el proceso del paso S17d. En este proceso, la unidad de trasmisor 14 del aparato de cifrado 10 genera un mensaje cifrado que incluye la información de cifrado C_1, y el par de esquemas, la política, el parámetro público, y la dirección del aparato de generación de clave leídos de la memoria 31, bajo el control de la unidad de controlador (paso S17d). Los procesos de los pasos S18 a S28, que siguen al proceso del paso S17d, son los mismos que aquéllos en el primer ejemplo del primer aspecto.

En el proceso del paso S22c1, que sigue al proceso del paso S28, la unidad de descifrado 33 del aparato de descifrado 30 lee el parámetro público, la clave de descifrado R, y la información de cifrado C_1 de la memoria 31 para calcular el texto plano M según el algoritmo de cifrado de predicado (paso S22c1).

(Cuarto ejemplo según el primer aspecto)

Un cuarto ejemplo del primer aspecto corresponde a una combinación del segundo ejemplo del primer aspecto y el tercer ejemplo del primer aspecto. El cuarto ejemplo del primer aspecto difiere del primer ejemplo del primer aspecto en que (1) el aparato de descifrado 30 genera la segunda información de atributo o la segunda información de predicado, y (2) la unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, junto con la clave pública incluida en el parámetro público y el texto plano M leídos de la memoria 11, para obtener una información de cifrado C_1. Debido a estas diferencias, el cuarto ejemplo del primer aspecto difiere en varios puntos del primer ejemplo del primer aspecto. Una descripción de las partes en común entre el primer y cuarto ejemplos del primer aspecto se omite (los mismos números de referencia se asignan a los mismos componentes), y una descripción de las diferencias del primer ejemplo del primer aspecto se hará con referencia a las Figura 26 y 27.

Los procesos de los pasos S1 a S17a son los mismos que aquéllos en el primer ejemplo del primer aspecto. El parámetro público y alguna otra información se requieren por el algoritmo de cifrado de predicado del cuarto ejemplo del primer aspecto. Para una información específica requerida, ver la Bibliografía que no es de patente 3, descrita anteriormente, por ejemplo.

En el proceso del paso S17b1, que sigue al proceso del paso S17a, la unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, junto con la clave pública incluida en el parámetro público y el texto plano M leídos de la memoria 11, para obtener una información de cifrado C_1 según el algoritmo de cifrado de predicado (paso S17b1).

Después del proceso del paso S17b1, se realiza el proceso del paso 17d. En este proceso, la unidad de trasmisor 14 del aparato de cifrado 10 genera un mensaje cifrado que incluye la información de cifrado C_1, y el par de esquemas, la política, el parámetro público, y la dirección del aparato de generación de clave leídos de la memoria 31, bajo el control de la unidad de controlador (paso S17d).

Los procesos de los pasos S18 a S22b, que siguen al proceso del paso S17d, son los mismos que aquéllos en el primer ejemplo del primer aspecto.

Cuando la clave de descifrado no se posee en el proceso del paso S22b, la segunda unidad de adquisición de información de lógica de predicado 35 del aparato de descifrado 30 lee la política, el par de esquemas, el parámetro público, y la información de usuario de la memoria 31 y obtiene una información de atributo (llamada segunda información de atributo) o una información de predicado (llamada segunda información de predicado) a partir de la información de usuario (paso S23g). En este proceso, el esquema emparejado con el esquema identificado por la política se aplica a la información de usuario. Cuando la política es Cipher_Text_Policy, el esquema (esquema de atributo) emparejado con el esquema (esquema de predicado) identificado por Cipher_Text_Policy se usa para obtener la segunda información de atributo a partir de la información de usuario (información de designación de atributo). Cuando la política es Key_Policy, el esquema (esquema de predicado) emparejado con el esquema (esquema de atributo) identificado por la Key_Policy se usa para obtener la segunda información de predicado a partir de la información de usuario (información de designación de predicado). Se debería señalar que el esquema emparejado con el esquema usado en el paso S17a se usa en este proceso. En el cuarto ejemplo del primer aspecto, la segunda información de atributo y la segunda información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes (ver las Figura 11 a 13).

Después del proceso del paso S23g, se realiza el proceso del paso 23. En este proceso, la unidad de transmisor 34 del aparato de descifrado 30 genera un mensaje de petición de clave que incluye el parámetro público, la política, el par de esquemas, y la información de autenticación leídos de la memoria 31, y la segunda información de atributo o la segunda información de predicado, bajo el control de la unidad de controlador. La unidad de transmisor 34 del aparato de descifrado 30 envía el mensaje de petición de clave al aparato de generación de clave que ha leído la dirección de la memoria 31, y la unidad de receptor del aparato de generación de clave 20 recibe el mensaje de petición de claves.

Cuando la verificación tiene éxito en el proceso del paso S24a, se realiza el proceso del paso S24d. Dado que el aparato de generación de clave 20 ha recibido la segunda información de atributo o la segunda información de predicado desde el aparato de descifrado 30, son innecesarios la función y el proceso para generar la información.

El proceso del paso S28, que sigue al proceso del paso S24d, es el mismo que en el primer ejemplo del primer aspecto.

En el proceso del paso S22c1, que sigue al proceso del paso S28, la unidad de descifrado 33 del aparato de descifrado 30 lee el parámetro público, la clave de descifrado R, y la información de descifrado C_1 de la memoria 31 para calcular el texto plano M según el algoritmo de cifrado de predicado (paso S22c1).

Las realizaciones según la invención (en lo sucesivo, que se conocen como “realización(es) según el segundo aspecto de la presente invención” por razones de conveniencia), que se refieren a una tecnología de comunicación criptográfica que puede operar de manera flexible, que se basa en un cifrado de predicado, y que permite que una información de cifrado cifrada con el cifrado de predicado sea distribuida se describirán a continuación mientras que se pone atención a la tecnología de comunicación criptográfica del primer aspecto, descrito anteriormente. Dado que un aparato de descifrado tiene una función de transferencia en la tecnología de comunicación criptográfica del segundo aspecto, se puede distribuir una información de cifrado cifrada con el cifrado de predicado.

La descripción de la tecnología de comunicación criptográfica del segundo aspecto y la descripción de la tecnología de comunicación criptográfica del primer aspecto tienen muchas partes en común sustanciales, pero, para evitar referirse a la descripción de la tecnología de comunicación criptográfica del primer aspecto, la tecnología de comunicación criptográfica del segundo aspecto se describirá más abajo con explicaciones y figuras solapadas que se incluyen tanto como sea posible. Por lo tanto, en ambas descripciones, se usan números de expresión idénticos, números de referencia idénticos asignados a bloques de función, y números de referencia idénticos asignados a pasos. Debido a que los contenidos son diferentes, no debería haber riesgo de confusión.

(Primera realización según el segundo aspecto)
Una primera realización según el segundo aspecto de la presente invención se describirá más abajo con referencia a la Figura 28 hasta la Figura 41.

Como se muestra en la Figura 28, un sistema criptográfico 1 según el segundo aspecto incluye una pluralidad de aparatos cliente 10, 30-1, y 30-2, o una pluralidad de aparatos de generación de clave 20, uno o una pluralidad de aparatos de gestión de información de usuario 40 (en lo sucesivo cada uno llamado aparato de gestión), aparatos de gestión de par de información de regla de conversión 50 (en lo sucesivo cada uno llamado aparato de registro), uno o una pluralidad de aparatos de mantenimiento 80, y uno o una pluralidad de aparatos de autenticación 90. Estos aparatos pueden comunicar unos con otros a través de una red de comunicación 5, tal como Internet.

Los aparatos cliente funcionan como aparatos de cifrado o como aparatos de descifrado en base a sus funciones de procesamiento. A la luz de sus funciones, los aparatos cliente se llaman aparatos de cifrado 10 o aparatos de descifrado. Los aparatos de descifrado incluyen un primer aparato de descifrado 30-1 que sirve como un aparato para intercambiar un mensaje cifrado, descrito más tarde, con el aparato de cifrado 10 y un segundo aparato de descifrado 30-2 que no realiza tal intercambio. El sistema criptográfico 1 según el segundo aspecto puede incluir aparatos cliente que funcionan solamente como aparatos de cifrado y/o aparatos cliente que funcionan solamente como aparatos de descifrado.

En el sistema criptográfico 1 según el segundo aspecto, se realizan un cifrado y un descifrado usando un cifrado de predicado. En el segundo aspecto de la presente invención, el algoritmo de cifrado de predicado a ser usado no está limitado, y se puede usar el algoritmo de cifrado de predicado descrito en la Bibliografía que no es de patente 3, por ejemplo. En la primera realización del segundo aspecto, se usará un algoritmo de cifrado de predicado de tipo KEM (el mecanismo de encapsulación de clave).

Un método de comunicación criptográfico usado en el sistema criptográfico 1 según el segundo aspecto se describirá con referencia a las Figura 29, 30, 31, 32, 34, 36, 38, 40, y 41. Ver las Figura 33, 35, 37, y 39 para la estructura funcional de cada aparato.

<<Proceso de preparación>>
La descripción entera del <<proceso de preparación>> en el primer ejemplo del primer aspecto se incorpora aquí y se omite una descripción del <<proceso de preparación>>. Ver la Figura 29 para el proceso de preparación, las Figura 11 a 13 para pares de esquemas, y la Figura 14 para listas de políticas. La descripción del proceso de preparación finaliza aquí.

<<Proceso de cifrado>>
Bajo el control de una unidad de controlador, no mostrada, una unidad de transmisor 14 del aparato de cifrado 10 envía una consulta de búsqueda al aparato de registro 50, y la unidad de recepción del aparato de registro 50 recibe la consulta de búsqueda (paso S14). La unidad de búsqueda del aparato de registro 50 busca algunas o todas las entradas registradas en la unidad de almacenamiento del aparato de registro 50 y elige una entrada (paso S15). La unidad de transmisor del aparato de registro 50 envía la entrada al aparatos de cifrado 10, y una unidad de receptor del aparato de cifrado 10 recibe la entrada (paso S16). Esta entrada incluye la dirección del aparato de generación de clave, el parámetro público del aparato de generación de clave, la lista de políticas que se puede usar por el aparato de generación de clave, y la lista de esquemas que se puede usar por el aparato de generación de clave. La entrada recibida se almacena en una memoria 11 del aparato de cifrado 10.

Cuando el aparato de cifrado 10 tiene el parámetro público, la lista de esquemas, la lista de políticas, y la dirección de cada aparato de generación de clave 20 por adelantado, se omiten los procesos de los pasos S14 a S16. Se debería señalar que el sistema criptográfico 1 puede no tener un aparato de registro 50.

Una primera unidad de adquisición de información de lógica de predicado 12 del aparato de cifrado 10 lee la información de entrada, la política, y los esquemas desde la memoria 11 y obtiene una información de atributo (en lo sucesivo llamada primera información de atributo) y una información de predicado (en lo sucesivo llamada primera información de predicado) (paso S17a). Los detalles de este proceso se describirán más abajo con referencia a las Figura 12 y 13.

Cuando la lista de esquemas tiene una pluralidad de pares de esquemas, se selecciona un par de esquemas en base al uso o similar. El usuario del aparato de cifrado 10 puede seleccionar un par de esquemas y una información de designación de entrada del mismo. Alternativamente, la primera unidad de adquisición de información de lógica de predicado 12 puede seleccionar un par de esquemas según una regla predeterminada.

Según si la información de entrada es una información de designación de atributo o una información de designación de predicado, se selecciona uno de los esquemas junto con la política. El usuario del aparato de cifrado 10 puede seleccionar la política y uno de los esquemas y una información de designación de entrada de los mismos. Alternativamente, la primera unidad de adquisición de información de lógica de predicado 12 puede seleccionar la política y uno de los esquemas según una regla predeterminada. Cuando solamente está preparado un tipo de política en el aparato de generación de clave 20, se selecciona un esquema del par de esquemas según la política. Si el esquema seleccionado no corresponde al tipo de la información de entrada, un par de esquemas necesita ser seleccionado de nuevo de la lista de esquemas o una entrada necesita ser proporcionada de nuevo por el aparato de registro 50.

La información de entrada puede ser una información introducida por el usuario del aparato de cifrado 10 o una información adquirida por una unidad de adquisición (no mostrada) del aparato de cifrado 10 desde un medio de almacenamiento tal como una tarjeta IC 39.

Entonces, la primera unidad de adquisición de información de lógica de predicado 12 usa el esquema seleccionado del par de esquemas según la política para tener la primera información de atributo o la primera información de predicado a partir de la información de entrada. Cuando la política es Key_Policy y el esquema seleccionado es un esquema de atributo, se obtiene la primera información de atributo. Cuando la política es Cipher_Text_Policy y el esquema seleccionado es un esquema de predicado, se obtiene la primera información de predicado. La primera información de atributo y la primera información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes en la primera realización según el segundo aspecto (ver las Figura 11 a 13). El esquema se usa para extraer o disponer valores de atributos necesarios a partir de la información de entrada.

A continuación, una unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, una base ortogonal B (clave pública sustancial) incluida en el parámetro público leído de la memoria 11, y un texto plano M para obtener una clave común K, una información de cifrado C_1 y un texto cifrado C_2 (pasos S17b y S17c). Los detalles de estos procesos se describirán más abajo. Cuando la primera realización del segundo aspecto se dedica a la entrega de la clave común K, no es necesario generar el texto de cifrado C_2.

Una primera unidad de cifrado 13a genera los números aleatorios r y ρ que son elementos del campo finito F_q según el algoritmo de cifrado de predicado, especifica la clave común K como se muestra por la Expresión (7), y obtiene la información de cifrado C_1 según la Expresión (8) (paso S17b), donde H indica, por ejemplo, una función de cálculo de claves. En este ejemplo, se usa la primera información de atributo v. Para usar la primera información de predicado, v necesita ser sustituida con w en la Expresión (8). En este ejemplo, la información de cifrado C_1 corresponde a ρ usado para generar la clave común K. La información de cifrado C_1 puede corresponder a la clave común K.

A continuación, la segunda unidad de cifrado 13b usa la clave común K y el texto plano M para obtener el texto de cifrado C_2 según la Expresión (9) (paso S17c). Un método de cifrado Enc_k que usa la clave privada puede ser un método conocido. Por ejemplo, puede ser el método descrito en la Bibliografía que no es de patente 1. Como se describió anteriormente, cuando la primera realización del segundo aspecto se dedica a la entrega de la clave común K, se omite el proceso del paso S17c. En otras palabras, el aparato de cifrado 10 tiene incluso la función de la segunda unidad de cifrado 13b pero no realiza el proceso del paso S17c.

A continuación, bajo el control de la unidad de controlador, la unidad de transmisor 14 del aparato de cifrado 10 genera un mensaje cifrado que incluye la información de cifrado C_1 y el texto cifrado C_2 (si es necesario), junto con el par de esquemas, la política, el parámetro público, y la dirección del aparato de generación de clave leídos de la memoria 11 (paso S17d). La unidad de transmisor 14 del aparato de cifrado 10 entonces envía el mensaje cifrado al

primer aparato de descifrado 30-1, y una unidad de receptor del primer aparato de descifrado 30-1 recibe el mensaje cifrado (paso S18). Se permite al aparato de cifrado 10 enviar un mensaje cifrado a una pluralidad de primeros aparatos de descifrado 30-1.

La descripción del <<proceso de cifrado>> finaliza aquí.

<<Primer proceso de descifrado>>
Bajo el control de una unidad de controlador, no mostrada, una unidad de transmisor 34 del primer aparato de descifrado 30-1 envía una consulta de búsqueda que incluye la dirección del aparato de generación de clave, la dirección que se incluye en el mensaje cifrado, al aparato de registro 50, y la unidad de recepción del aparato de registro 50 recibe la consulta de búsqueda (paso S19). La unidad de búsqueda del aparato de registro 50 busca la entrada del aparato de generación de clave especificada por la dirección y la selecciona (paso S20). La unidad de transmisor del aparato de registro 50 envía la entrada del resultado de búsqueda al primer aparato de descifrado 30-1, y la unidad del receptor del primer aparato de descifrado 30-1 recibe la entrada (paso S21). Esta entrada incluye la dirección del aparato de generación de clave, el parámetro público del aparato de generación de clave, la lista de políticas que se puede usar por el aparato de generación de clave, y la lista de esquemas que se puede usar por el aparato de generación de clave. La entrada recibida se almacena en una memoria 31 del primer aparato de descifrado 30-1.

Cuando el primer aparato de descifrado 30-1 tiene el parámetro público, la lista de esquemas, la lista de políticas, y la dirección de cada aparato de generación de clave 20 por adelantado, se omiten los procesos de los pasos S19 a S21. En ese caso, el primer aparato de descifrado 30-1 busca en la memoria 31 la entrada del aparato de generación de clave que corresponde a la dirección incluida en el mensaje cifrado y la recupera.

Bajo el control de la unidad de controlador, una unidad de verificación (no mostrada) del primer aparato de descifrado 30-1 verifica que el par de esquemas y la política incluida en el mensaje cifrado están incluidos en la lista de esquemas y la lista de políticas incluida en la entrada obtenida a partir del aparato de registro 50 (paso S22a). Si esta verificación falla, el proceso finaliza con un fallo de procesamiento de descifrado (paso S22g).

Cuando la verificación tiene éxito, una unidad de adquisición 32 del primer aparato de descifrado 30-1 lee la información de designación de atributo o la información de designación de predicado que corresponde al usuario del primer aparato de descifrado 30-1 desde un medio de almacenamiento tal como la tarjeta IC 39 (paso S22f). Si se lee la información de designación de atributo o la información de designación de predicado depende de la política incluida en el mensaje cifrado. Más específicamente, la información de designación de lectura corresponde al contenido de la política que identifica un esquema emparejado con el otro esquema identificado por la política incluida en el mensaje cifrado. Cuando la política es Cipher_Text_Policy, la unidad de adquisición 32 lee la información de designación de atributo desde el medio de almacenamiento. Cuando la política es Key_Policy, la unidad de adquisición 32 lee la información de designación de predicado desde el medio de almacenamiento. La información de designación leída en lo sucesivo se llama información de usuario. La unidad de adquisición 32 del primer aparato de descifrado 30-1 puede leer desde el aparato de gestión 40 la información de designación de atributo o la información de designación de predicado que corresponde al usuario del primer aparato de descifrado 30-1, de la misma forma que en <<un proceso de adquisición de información de usuario>> en el aparato de generación de clave 20 descrito más tarde. En la primera realización del segundo aspecto, se puede omitir el proceso del paso S22f. Cuando el primer aparato de descifrado 30-1 tiene la información de designación de atributo y la información de designación de predicado que corresponde al usuario por adelantado, o bien la información de designación de atributo o bien la información de designación de predicado sirve como información de usuario, según la política.

A continuación, la unidad de verificación del primer aparato de descifrado 30-1 verifica que el aparato de descifrado 30 tiene la clave de descifrado a ser usada para descifrar la información de cifrado incluida en el mensaje de cifrado (paso S22b).

El primer aparato de descifrado 30-1 almacena una tabla de claves de descifrado en la memoria 31. En la tabla de claves de descifrado, como se muestra en la Figura 15, por ejemplo, el identificador de cada aparato de generación de clave está asociado con el parámetro público, el par de esquemas, el objetivo de clave de descifrado, la información de designación de predicado, y la clave de descifrado. La unidad de verificación verifica que el aparato de descifrado 30 tiene la clave de descifrado que corresponde al identificador del aparato de generación de clave determinada a partir de la dirección incluida en el mensaje cifrado, al parámetro público, al par de esquemas, y al objetivo de clave de descifrado (que corresponde al contenido de la política que identifica un esquema emparejado con el otro esquema identificado por la política incluida en el mensaje cifrado). Cuando el aparato de descifrado 30 tiene la clave de descifrado, se realiza el proceso del paso S29. Si el aparato de descifrado 30 no tiene la clave de descifrado, se realiza el proceso del paso S23.

La descripción del <<proceso de descifrado>> se detiene temporalmente aquí y se describirá más abajo <<un proceso de generación de clave>>.

Si el primer aparato de descifrado 30-1 no tiene la clave de descifrado, la unidad de transmisor 34 del primer aparato de descifrado 30-1 genera, bajo el control de la unidad de controlador, un mensaje de petición de clave que incluye el parámetro público, la política, el par de esquemas, la información de usuario (en su caso), y la información de autenticación, todos estos elementos que se leen de la memoria 31. La información de autenticación incluye, por ejemplo, el ID del usuario y una contraseña. La unidad de transmisor 34 del primer aparato de descifrado 30-1 envía el mensaje de petición de clave al aparato de generación de clave que ha leído la dirección de la memoria 31, y la unidad de receptor del aparato de generación de clave 20 recibe el mensaje de petición de clave (paso S23). El mensaje de petición de clave recibido se almacena en una memoria 21 del aparato de generación de clave 20.

Bajo el control de una unidad de controlador, una unidad de verificación (no mostrada) del aparato de generación de clave 20 verifica que el par de esquemas y la política incluida en el mensaje de petición de claves están incluidos en la lista de esquemas y la lista de políticas incluida en la entrada propiedad del aparato de generación de clave 20 (por ejemplo, la entrada generada en el paso S1) y que el parámetro público incluido en el mensaje de petición de clave es idéntico al parámetro público del aparato de generación de clave 20 (paso S24a). Si esta verificación falla, el proceso finaliza con un fallo del proceso de generación de clave (paso S24g). Cuando la información de autenticación se incluye en el mensaje de petición de clave, la información de autenticación también se verifica en el proceso del paso S24a. El aparato de generación de clave 20 almacena una tabla de autenticación en la memoria 21. En la tabla de autenticación, como se muestra la Figura 16, por ejemplo, cada ID de usuario está asociado con una contraseña. La unidad de verificación verifica que el ID de usuario y la contraseña incluidos en el mensaje de petición de clave son idénticos al ID de usuario y la contraseña incluidos en la tabla de autenticación. Si la verificación falla, se realiza el proceso del paso S24g.

Cuando esta verificación tiene éxito, la unidad de verificación del aparato de generación de clave 20 verifica que el mensaje de petición de clave incluye la información de usuario (paso S24b). Cuando el mensaje de petición de clave incluye la información de usuario, se realiza el proceso del paso S24c. Si el mensaje de petición de clave no incluye la información de usuario, se realiza el proceso del paso S25. Cuando se emplea un método en el cual un mensaje de petición de clave siempre incluye una información de usuario, son innecesarios el proceso del paso S24b y <<un proceso de adquisición de información de usuario>>, descrito más tarde.

La descripción del <<proceso de generación de clave>> se detiene temporalmente aquí y se describirá más abajo <<el proceso de adquisición de información de usuario>>.

La unidad de transmisor 24 del aparato de generación de clave 20 envía una petición que incluye la política y la información de autenticación (en su caso) incluidas en el mensaje de petición de clave al aparato de gestión 40, y el aparato de gestión 40 recibe la petición (paso S25). La petición recibida se almacena en una memoria del aparato de gestión 40.

El aparato de gestión 40 almacena una tabla de autenticación en la memoria. De la misma forma que en la tabla de autenticación descrita anteriormente, el ID de usuario está asociado con la contraseña en esta tabla de autenticación (ver la Figura 16). Una unidad de verificación (no mostrada) del aparato de gestión 40 verifica que el ID de usuario y la contraseña incluidos en la petición son idénticos al ID de usuario y la contraseña incluidos en la tabla de autenticación.

Cuando esta verificación tiene éxito, una unidad de búsqueda (no mostrada) del aparato de gestión 40 busca una tabla de información de usuario almacenada en la memoria para la información de designación de atributo o la información de designación de predicado según la política incluida en la petición (paso S26). La tabla de información de usuario incluye, por ejemplo, una primera tabla formada de cada ID de usuario, y un nombre de atributo y una información de designación de atributo asociados con el ID de usuario, y una segunda tabla formada del ID de usuario y una información de designación de predicado asociada con el ID de usuario (ver la Figura 17). Si se lee la información de designación de atributo o la información de designación de predicado se determina por la política incluida en la petición. Más específicamente, la información leída corresponde al contenido de la política que identifica un esquema emparejado con el otro esquema identificado por la política incluida en la petición. Cuando la política es Cipher_Text_Policy, la unidad de búsqueda lee la información de designación de atributo que corresponde al ID de usuario incluido en la petición desde la primera tabla. Cuando la política es Key_Policy, la unidad de búsqueda lee la información de designación de predicado que corresponde al ID de usuario incluido en la petición desde la segunda tabla. La información de designación leída en lo sucesivo se llama información de usuario.

Bajo el control de una unidad de controlador, una unidad de transmisor del aparato de gestión 40 envía la información de usuario al aparato de generación de clave 20, y la unidad del receptor del aparato de generación de clave 20 recibe la información de usuario (paso S27). La información de usuario recibida se almacena en la memoria 21 del aparato de generación de clave 20.

La descripción del <<proceso de adquisición de información de usuario>> finaliza aquí, y se resumirá la descripción del <<proceso de generación de clave>>.

Cuando el aparato de generación de clave 20 ya tiene la información de usuario o recibe la información de usuario a través del proceso de adquisición de información de usuario (paso S27), una segunda unidad de adquisición de información de lógica de predicado 23 del aparato de generación de clave 20 lee la política, el par de esquemas, el parámetro público, y la información de usuario de la memoria 21, y obtiene una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (segunda información de predicado) a partir de la información de usuario (paso S24c). En este proceso, el esquema emparejado con el esquema identificado por la política se aplica a la información de usuario. La política es Cipher_Text_Policy, el esquema (esquema de atributo) emparejado con el esquema (esquema de predicado) identificado por Cipher_Text_Policy se usa para obtener la segunda información de atributo a partir de la información de usuario (información de designación de atributo). Cuando la política es Key_Policy, el esquema (esquema de predicado) emparejado con el esquema (esquema de atributo) identificado por Key_Policy se usa para obtener la segunda información de predicado a partir de la información de usuario (información de designación de predicado). Se debería señalar que el esquema emparejado con el esquema usado en el paso S17a se usa en este proceso. En la primera realización del segundo aspecto, la segunda información de atributo y la segunda información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes (ver las Figura 11 a 13). El esquema se usa para extraer y disponer los valores de atributos necesarios a partir de la información de entrada.

A continuación, una unidad de generación de clave 25 del aparato de generación de clave 20 genera un numero aleatorio α qué es un elemento del campo finito F_q, en base al parámetro público q según el algoritmo de cifrado de predicado, y usa el numero aleatorio α , la segunda información de atributo $v_{(p)} = (v_{(p)1}, \ldots, v_{(p)n})$ o la segunda información de predicado $w_{(p)} = (w_{(p)1}, \ldots, w_{(p)n})$ leídos de la memoria 21, y una clave privada B* del aparato de generación de clave para obtener una clave de descifrado R según la Expresión (10) (paso S24d). La segunda información de predicado $w_{(p)}$ se usa en este ejemplo debido a que la información de entrada usada en el proceso de cifrado es la información de designación de atributo. Cuando la información de entrada es la información de designación de predicado, se usa la segunda información de atributo $v_{(p)}$. Por lo tanto, $w_{(p)}$ necesita ser sustituida con $v_{(p)}$ en la Expresión (10), descrita anteriormente.

A continuación, bajo el control de la unidad de controlador, la unidad de transmisor 24 del aparato de generación de clave 20 envía la clave de descifrado R al primer aparato descifrado 30-1, y la unidad de receptor del primer aparato de descifrado 30-1 recibe la clave de descifrado R (paso S28). La clave de descifrado recibida R se almacena en la memoria 31 del primer aparato de descifrado 30-1.

La descripción del <<proceso de generación de clave>> finaliza aquí, y se resumirá la descripción del <<proceso de descifrado>>.

Cuando el primer aparato de descifrado 30-1 ya tiene la clave de descifrado o recibe la clave de descifrado a través del proceso de generación de clave (paso S28), una unidad de descifrado 33 del primer aparato de descifrado 30-1 lee el parámetro público, la clave de descifrado R, la información de cifrado C_1, y el texto descifrado C_2 (si es necesario) de la memoria 31, y obtiene la clave común K y el texto plano M (si es necesario) (paso S29).

Los detalles del proceso en el paso S29 se describirán más abajo. Una primera unidad de descifrado 33a lee el parámetro público, la clave de descifrado R, y la información de cifrado C_1 de la memoria 31, y obtiene $e(C_1, R)$ según el algoritmo de cifrado de predicado. Como se muestra en la Expresión (11), descrita anteriormente, el resultado del cálculo depende del resultado del producto interior canónico de la primera información de atributo v y la segunda información de predicado $w_{(p)}$ sacadas a partir de la información de cifrado C_1 y la clave de descifrado R según una bilinealidad cuando la información de entrada es la información de designación de atributo. Cuando la información de entrada es la información de designación de predicado, v necesita ser sustituida por con $v_{(p)}$ y $w_{(p)}$ necesita ser sustituida con w en la Expresión (11), descrita anteriormente. El resultado del cálculo depende del resultado del producto interior canónico de la primera información de predicado w y la segunda información de atributo $v_{(p)}$ sacadas a partir de la información de cifrado C_1 y la clave de descifrado R según una bilinealidad. En la Expresión (11), $e(b_i, b_i^*)$ se define como se muestra en la Expresión (12), descrita anteriormente, donde δ_{ij} es el símbolo de la delta de Kronecker.

Por lo tanto, cuando el producto interior canónico de la primera información de atributo v y la segunda información de predicado $w_{(p)}$ es cero (o cuando el producto interior canónico de la primera información de predicado w y la segunda información de atributo $v_{(p)}$ es cero), se obtiene el resultado del cálculo en la Expresión (11), g_T^{ρ} . Cuando se obtiene el resultado del cálculo, g_T^{ρ} , la primera unidad de descifrado 33a del primer aparato de descifrado 30-1 obtiene la clave común K, que es correcta, según la Expresión (7), descrita anteriormente (paso S22c). Cuando el producto interior canónico de la primera información de atributo v y la segunda información de predicado $w_{(p)}$ no es cero (o cuando el producto interior canónico de la primera información de predicado w y la segunda información de atributo $v_{(p)}$ no es cero), la unidad de descifrado 33a obtiene un valor incorrecto según la Expresión (7), descrita anteriormente. En este ejemplo, se supone que la función de cálculo de claves H es común al sistema o está incluida en el parámetro público. Esta información de cifrado C_1 corresponde a la información ρ usada para generar la clave

común K en este ejemplo. Cuando la información de cifrado C_1 corresponde a la clave común K, el resultado del cálculo en la Expresión (11), descrita anteriormente, es la clave común K (o un valor incorrecto). En otras palabras, un usuario autorizado del primer aparato de descifrado 30-1 tiene una información de designación de predicado que da la segunda información de predicado $w_{(p)}$ que hace el producto interior canónico con la primera información de atributo v cero, o una información de designación de atributo que da la segunda información de atributo $v_{(p)}$ que hace el producto interior canónico con la primera información de predicado w cero.

Entonces, una segunda unidad de descifrado 33b usa la clave común K y el texto cifrado C_2 para calcular el texto plano M según la Expresión (13), descrita anteriormente (paso S22d). Un método de descifrado Dec_k que usa la clave privada corresponde al método de cifrado Enc_k. Como se describió anteriormente, cuando la primera realización del segundo aspecto se dedica a la entrega de la clave común K, se omite el proceso del paso S22d. Más específicamente, incluso si el primer aparato de descifrado 30-1 tiene la función de la segunda unidad de descifrado 33b, no realiza el proceso del paso S22d.

Si el resultado del cálculo de la Expresión (11), descrita anteriormente, es un valor incorrecto, el texto plano correcto M no se puede obtener por la Expresión (13), descrita anteriormente.

El primer aparato de descifrado 30-1 puede almacenar la clave de descifrado R en la tabla de claves de descifrado. Además, el primer aparato de descifrado 30-1 puede almacenar la clave común K en la tabla de claves de descifrado.

La descripción del <<primer proceso de descifrado>> finaliza aquí.

<<Proceso de transferencia>>
Una unidad de transferencia 37 del primer aparato de descifrado 30-1 transfiere el mensaje cifrado recibido desde el aparato de cifrado 10, al segundo aparato de descifrado 30-2, y una unidad de receptor del segundo aparato de descifrado 30-2 recibe el mensaje cifrado (paso S30). El aparato de descifrado al cual se transfiere el mensaje cifrado no está limitado al segundo aparato de descifrado (aparato de descifrado que no intercambia un mensaje cifrado con el aparato de cifrado) y puede ser otro primer aparato de descifrado (aparato de descifrado que intercambia un mensaje cifrado con el aparato de cifrado). Por conveniencia de la descripción, el proceso del paso S30 sigue al proceso del paso S29. El proceso de paso S30, no obstante, se puede realizar en cualquier momento después de que el primer aparato de descifrado 30-1 reciba el mensaje cifrado desde el aparato de cifrado 10.

La descripción del <<proceso de transferencia>> finaliza aquí.

Un segundo proceso de descifrado (que incluye un proceso de generación de clave y, si es necesario, un proceso de adquisición de información de usuario) realizado por el segundo aparato de descifrado 30-2 se describirá más abajo. Esta serie de procesamiento es sustancialmente la misma que el primer proceso de descifrado. El segundo aparato de descifrado 30-2 tiene la misma estructura funcional que el primer aparato de descifrado 30-1 excepto que la unidad de transferencia 37 no se requiere necesariamente. Por lo tanto, los mismos números de referencia se asignan a los mismos componentes funcionales.

<<Segundo proceso de descifrado>>
Bajo el control de una unidad de controlador, no mostrada, una unidad de transmisor 34 del segundo aparato de descifrado 30-2 envía una consulta de búsqueda que incluye la dirección del aparato de generación de clave, la dirección que se incluye en el mensaje cifrado, al aparato de registro 50, y la unidad de recepción del aparato de registro 50 recibe la consulta de búsqueda (paso S31). La unidad de búsqueda del aparato de registro 50 busca la entrada del aparato de generación de clave especificada por la dirección y la selecciona (paso S32). La unidad de transmisor del aparato de registro 50 envía la entrada del resultado de la búsqueda al segundo aparato de descifrado 30-2, y la unidad de receptor del segundo aparato de descifrado 30-2 recibe la entrada (paso S33). Esta entrada incluye la dirección del aparato de generación de clave, el parámetro público del aparato de generación de clave, la lista de políticas que se puede usar por el aparato de generación de clave, y la lista de esquemas que se puede usar por el aparato de generación de clave. La entrada recibida se almacena en una memoria 31 del segundo aparato de descifrado 30-2.

Cuando el segundo aparato de descifrado 30-2 tiene el parámetro público, la lista de esquemas, la lista de políticas, y la dirección de cada aparato de generación de clave 20 por adelantado, se omiten los procesos de los pasos S31 a S33. En ese caso, el segundo aparato de descifrado 30-2 busca en la memoria 31 la entrada del aparato de generación de clave que corresponde a la dirección incluida en el mensaje cifrado y la recupera.

Bajo el control de la unidad de controlador, una unidad de verificación (no mostrada) del segundo aparato de descifrado 30-2 verifica que el par de esquemas y la política incluida en el mensaje cifrado están incluidos en la lista de esquemas y la lista de políticas incluidas en la entrada obtenida a partir del aparato de registro 50 (paso S34a). Si esta verificación falla, el proceso finaliza con un fallo de procesamiento de descifrado (paso S34g).

Cuando la verificación tiene éxito, una unidad de adquisición 32 del segundo aparato de descifrado 30-2 lee la información de designación de atributo o la información de designación de predicado que corresponde al usuario del segundo aparato de descifrado 30-2 desde un medio de almacenamiento tal como la tarjeta IC 39 (paso S34f). Si se lee la información de designación de atributo o la información de designación de predicado depende de la política incluida en el mensaje cifrado. Más específicamente, la información de designación leída corresponde al contenido de la política que identifica un esquema emparejado con el otro esquema identificado por la política incluida en el mensaje cifrado. Cuando la política es Cipher_Text_Policy, la unidad de adquisición 32 lee la información de designación de atributo desde el medio de almacenamiento. Cuando la política es Key_Policy, la unidad de adquisición 32 lee la información de designación de predicado desde el medio de almacenamiento. La información de designación leída en lo sucesivo se llama información de usuario. La unidad de adquisición 32 del segundo aparato de descifrado 30-2 puede leer desde el aparato de gestión 40 la información de designación de atributo o la información de designación de predicado que corresponde al usuario del segundo aparato de descifrado 30-2, de la misma forma que en <<un proceso de adquisición de información de usuario>> en el aparato de generación de clave 20, descrito más tarde. En la primera realización del segundo aspecto, se puede omitir el proceso del paso S34f. Cuando el segundo aparato de descifrado 30-2 tiene la información de designación de atributo y la información de designación de predicado que corresponde al usuario por adelantado, o bien la información de designación de atributo o bien la información de designación de predicado sirve como información de usuario, según la política.

A continuación, la unidad de verificación del segundo aparato de descifrado 30-2 verifica que el aparato de descifrado 30 tiene la clave de descifrado a ser usada para descifrar la información de cifrado incluida en el mensaje de cifrado (paso S34b).

El segundo aparato de descifrado 30-2 almacena una tabla de claves de descifrado en la memoria 31. En la tabla de claves de descifrado, como se muestra en la Figura 15, por ejemplo, el identificador de cada aparato de generación de clave está asociado con el parámetro público, el par de esquemas, el objetivo de clave de descifrado, la información de designación de predicado, y la clave de descifrado. La unidad de verificación verifica que el aparato de descifrado 30 tiene la clave de descifrado que corresponde al identificador del aparato de generación de clave determinado a partir de la dirección incluida en el mensaje cifrado, al parámetro público, al par de esquemas, y al objetivo de clave de descifrado (que corresponde al contenido de la política que identifica un esquema emparejado con el otro esquema identificado por la política incluida en el mensaje cifrado). Cuando el aparato de descifrado 30 tiene la clave de descifrado, se realiza el proceso del paso S41. Si el aparato de descifrado 30 no tiene la clave de descifrado, se realiza el proceso del paso S35.

La descripción del <<proceso de descifrado>> se detiene temporalmente aquí y se describirá más abajo <<un proceso de generación de clave>>.

Si el segundo aparato de descifrado 30-2 no tiene la clave de descifrado, la unidad de transmisor 34 del segundo aparato de descifrado 30-2 genera, bajo el control de la unidad de controlador, un mensaje de petición de clave que incluye el parámetro público, la política, el par de esquemas, la información de usuario (en su caso), y la información de autenticación, todos estos elementos que se leen de la memoria 31. La información de autenticación incluye, por ejemplo, el ID del usuario y una contraseña. La unidad de transmisor 34 del segundo aparato de descifrado 30-2 envía el mensaje de petición de clave al aparato de generación de clave que ha leído la dirección de la memoria 31, y la unidad de receptor del aparato de generación de clave 20 recibe el mensaje de petición de clave (paso S35). El mensaje de petición de clave recibido se almacena en una memoria 21 del aparato de generación de clave 20. Este aparato de generación de clave 20 no necesita ser necesariamente el aparato de generación de clave 20 emparejado con el primer aparato de descifrado 30-1.

Bajo el control de una unidad de controlador, una unidad de verificación (no mostrada) del aparato de generación de clave 20 verifica que el par de esquemas y la política incluida en el mensaje de petición de clave están incluidos en la lista de esquemas y la lista de políticas incluidas en la entrada propiedad del aparato de generación de clave 20 (por ejemplo, la entrada generada en el paso S1) y que el parámetro público incluido en el mensaje de petición de claves es idéntico al parámetro público del aparato de generación de clave 20 (paso S36a). Si esta verificación falla, el proceso finaliza con un fallo del proceso de generación de clave (paso S36g). Cuando la información de autenticación está incluida en el mensaje de petición de clave, la información de autenticación también se verifica en el proceso del paso S36a. El aparato de generación de clave 20 almacena una tabla de autenticación en la memoria 21. En la tabla autenticación, como se muestra la Figura 16, por ejemplo, cada ID de usuario está asociado con una contraseña. La unidad de verificación verifica que el ID de usuario y la contraseña incluidos en el mensaje de petición de clave son idénticos al ID de usuario y la contraseña incluidos en la tabla de autenticación. Si la verificación falla, se realiza el proceso del paso S36g.

Cuando esta verificación tiene éxito, la unidad de verificación del aparato de generación de clave 20 verifica que el mensaje de petición de clave incluye la información de usuario (paso S36b). Cuando el mensaje de petición de clave incluye la información de usuario, se realiza el proceso del paso S36c. Si el mensaje de petición de clave no incluye la información de usuario, se realiza el proceso del paso S37. Cuando se emplea un método en el cual un mensaje de petición de clave siempre incluye una información de usuario, el proceso del paso S36b y <<un proceso de

adquisición de información de usuario>>, descrito más tarde, son innecesarios.

La descripción del <<proceso de generación de clave>> se detiene temporalmente aquí y se describirá más abajo <<el proceso de adquisición de información de usuario>>.

La unidad de transmisor 24 del aparato de generación de clave 20 envía una petición que incluye la política y la información de autenticación (en su caso) incluidas en el mensaje de petición de clave al aparato de gestión 40, y el aparato de gestión 40 recibe la petición (paso S37). La petición recibida se almacena en una memoria del aparato de gestión 40.

El aparato de gestión 40 almacena una tabla de autenticación en la memoria. De la misma forma que en la tabla de autenticación descrita anteriormente, el ID de usuario está asociado con la contraseña en esta tabla de autenticación (ver la Figura 16). Una unidad de verificación (no mostrada) del aparato de gestión 40 verifica que el ID de usuario y la contraseña incluidos en la petición son idénticos al ID de usuario y la contraseña incluidos en la tabla de autenticación.

Cuando esta verificación tiene éxito, una unidad de búsqueda (no mostrada) del aparato de gestión 40 busca una tabla de información de usuario almacenada en la memoria para la información de designación de atributo o la información de designación de predicado según la política incluida en la petición (paso S38). La tabla de información de usuario incluye, por ejemplo, una primera tabla formada de cada ID de usuario, y un nombre de atributo y una información de designación de atributo asociada con el ID de usuario, y una segunda tabla formada del ID de usuario y la información de designación de predicado asociada con el ID de usuario (ver la Figura 17). Si se lee la información de designación de atributo o la información de designación de predicado se determina por la política incluida en la petición. Más específicamente, la información leída corresponde al contenido de la política que identifica un esquema emparejado con el otro esquema identificado por la política incluida en la petición. Cuando la política es Cipher_Text_Policy, la unidad de búsqueda lee la información de designación de atributo que corresponde al ID de usuario incluido en la petición desde la primera tabla. Cuando la política es Key_Policy, la unidad de búsqueda lee la información de designación de predicado que corresponde al ID de usuario incluido en la petición desde la segunda tabla. La información de designación leída en lo sucesivo se llamada información de usuario.

Bajo el control de una unidad de controlador, una unidad de transmisor del aparato de gestión 40 envía la información de usuario al aparato de generación de clave 20, y la unidad de receptor del aparato de generación de clave 20 recibe la información de usuario (paso S27). La información de usuario recibida se almacena en la memoria 21 del aparato de generación de clave 20.

La descripción del <<proceso de adquisición de información de usuario>> finaliza aquí, y se resumirá la descripción del <<proceso de generación de clave>>.

Cuando el aparato de generación de clave 20 ya tiene la información de usuario o recibe la información de usuario a través del proceso de adquisición de información de usuario (paso S39), una segunda unidad de adquisición de información de lógica de predicado 23 del aparato de generación de clave 20 lee la política, el par de esquemas, el parámetro público, y la información de usuario de la memoria 21, y obtiene una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (segunda información de predicado) a partir de la información de usuario (paso S36c). En general, el usuario del primer aparato de descifrado 30-1 y el usuario del segundo aparato de descifrado 30-2 son diferentes. Por lo tanto, la segunda información de atributo o segunda información de predicado obtenida en este proceso no es necesariamente la misma que la segunda información de atributo o la segunda información de predicado obtenida en el proceso del paso S24c. En este proceso, el esquema emparejado con el esquema identificado por la política se aplica a la información de usuario. Cuando la política es Cipher_Text_Policy, el esquema (esquema de atributo) emparejado con el esquema (esquema de predicado) identificado por Cipher_Text_Policy se usa para obtener la segunda información de atributo a partir de la información de usuario (información de designación de atributo). Cuando la política es Key_Policy, el esquema (esquema de predicado) emparejado con el esquema (esquema de atributo) identificado por Key_Policy se usa para obtener la segunda información de predicado a partir de la información de usuario (información de designación de predicado). Se debería señalar que el esquema emparejado con el esquema usado en el paso S17a se usa en este proceso. En la primera realización del segundo aspecto, la segunda información de atributo y la segunda información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes (ver las Figura 11 a 13). El esquema se usa para extraer y disponer los valores de atributos necesarios a partir de la información de entrada.

A continuación, una unidad de generación de clave 25 del aparato de generación de clave 20 genera un número aleatorio α que es un elemento del campo finito F_q, en base al parámetro público q según el algoritmo de cifrado de predicado, y usa el número aleatorio α , la segunda información de atributo $v'_{(p)} = (v'_{(p)1}, \ldots, v'_{(p)n})$ o la segunda información de predicado $w'_{(p)} = (w'_{(p)1}, \ldots, w'_{(p)n})$ leída de la memoria 21, y una clave privada B* del aparato de generación de clave para obtener una clave de descifrado R' según la Expresión (14) (paso S36d). La segunda

información de predicado $w'_{(p)}$ se usa en este ejemplo debido a que la información de entrada usada en el proceso de cifrado es la información de designación de atributo. Cuando la información de entrada es la información de designación de predicado, se usa la segunda información de atributo $v'_{(p)}$. Por lo tanto, $w'_{(p)}$ necesita ser sustituido con $v'_{(p)}$ en la Expresión (14).

$$R' = \varepsilon \sum_{i=1}^{n} w'_{(p)i} b_i^* + b_{n+1}^* \qquad (14)$$

A continuación, bajo el control de la unidad de controlador, la unidad de transmisor 24 del aparato de generación de clave 20 envía la clave de descifrado R' al segundo aparato de descifrado 30-2, y la unidad de receptor del segundo aparato de descifrado 30-2 recibe la clave de descifrado R' (paso S28). La clave de descifrado recibida R' se almacena en la memoria 31 del segundo aparato de descifrado 30-2.

La descripción del <<proceso de generación de clave>> finaliza aquí, y se resumirá la descripción del <<proceso de descifrado>>.

Cuando el segundo aparato de descifrado 30-2 ya tiene la clave de descifrado o recibe la clave de descifrado a través del proceso de generación de clave (paso S40), una unidad de descifrado 33 del segundo aparato de descifrado 30-2 lee el parámetro público, la clave de descifrado R', la información de cifrado C_1, y el texto de cifrado C_2 (si es necesario) de la memoria 31, y obtiene la clave común K y el texto plano M (si es necesario) (paso S41).

Los detalles del proceso en el paso S41 se describirán más abajo. La primera unidad de descifrado 33a lee el parámetro público, la clave de descifrado R', y la información de cifrado C_1 de la memoria 31, y obtiene $e(C_1, R)$ según el algoritmo de cifrado de predicado. Como se muestra la Expresión (15), el resultado del cálculo depende del resultado del producto interior canónico de la primera información de atributo v y la segunda información de predicado $w'_{(p)}$ sacadas de la información de cifrado C_1 y la clave de descifrado R' según una bilinealidad cuando la información de entrada es la información de designación de atributo. Cuando la información de entrada es la información de designación de predicado, v necesita ser sustituido con $v'_{(p)}$ y $w'_{(p)}$ necesita ser sustituido con w en la Expresión (15). El resultado del cálculo depende del resultado del producto interior canónico de la primera información de predicado w y la segunda información de atributo $v'_{(p)}$ sacadas de la información de cifrado C_1 y la clave de descifrado R' según una bilinealidad. En la Expresión (15), $e(b_i, b_i^*)$ se define como se muestra en la Expresión (12) descrita anteriormente.

$$\begin{aligned} e(C_1, R') &= e(r\sum_{i=1}^{n} v_i b_i, R') \cdot e(\rho b_{n+1}, R') \\ &= \prod_{i=1}^{n} e(b_i, b_i^*)^{r\alpha v_i w'_{(p)i}} \cdot e(b_{n+1}, b_{n+1}^*)^{\rho} \\ &= g_T{}^{r\alpha \sum_{i=1}^{n} v_i w'_{(p)i}} \cdot g_T{}^{\rho} \\ &= g_T{}^{r\alpha v \cdot w'_{(p)}} \cdot g_T{}^{\rho} \end{aligned} \qquad (15)$$

Por lo tanto, cuando el producto interior canónico de la primera información de atributo v y la segunda información de predicado $w'_{(p)}$ es cero (o cuando el producto interior canónico de la primera información de predicado w en la segunda información de atributo $v'_{(p)}$ es cero), se obtiene el resultado del cálculo en la Expresión (15), $g_T{}^{\rho}$. Cuando se obtiene el resultado del cálculo, $g_T{}^{\rho}$, la primera unidad de descifrado 33a del segundo aparato de descifrado 30-2 obtiene la clave común K, la cual es correcta, según la Expresión (7), descrita anteriormente (paso S34c). Cuando el producto interior canónico de la primera información de atributo v y la segunda información de predicado $w'_{(p)}$ no es cero (o cuando el producto interior canónico de la primera información de predicado w y la segunda información de atributo $v'_{(p)}$ no es cero), la primera unidad de descifrado 33a obtiene un valor incorrecto según la Expresión (7), descrita anteriormente. En este ejemplo, se supone que la función de cálculo de claves H es común al sistema o está incluida en el parámetro público. La información de cifrado C_1 corresponde a la información ρ usada para generar la clave común K en este ejemplo. Cuando la información de cifrado C_1 corresponde a la clave común K, el resultado del cálculo en la Expresión (15) es la clave común K (o un valor incorrecto). En otras palabras, un usuario autorizado del segundo aparato de descifrado 30-2 tiene una información de designación de predicado que da la segunda información de predicado $w'_{(p)}$ que hace el producto interior canónico con la primera información de atributo v cero, o una información de designación de atributo que da la segunda información de atributo $v'_{(p)}$ que hace el

producto interior canónico con la primera información de predicado w cero.

Entonces, la segunda unidad de descifrado 33b usa la clave común K y el texto cifrado C_2 para calcular un texto plano M según la Expresión (13), descrita anteriormente (paso S34d). Un método de descifrado Dec_k que usa la clave privada corresponde al método de cifrado Enc_K. Como se describió anteriormente, cuando la primera realización del segundo aspecto se dedica a la entrega de la clave común K, se omite el proceso del paso S34d. Más específicamente, incluso si el segundo aparato de descifrado 30-2 tiene la función de la segunda unidad de descifrado 33b, no realiza el proceso del paso S34d.

Si el resultado del cálculo en la Expresión (15) es un valor incorrecto, el texto plano M correcto no se puede obtener por la Expresión (13), descrita anteriormente.

El segundo aparato de descifrado 30-2 puede almacenar la clave de descifrado R' en la tabla de claves de descifrado. Además, el segundo aparato de descifrado 30-2 puede almacenar la clave común K en la tabla de claves de descifrado.

La descripción del <<segundo proceso de descifrado>> finaliza aquí.

Cuando el segundo aparato de descifrado 30-2 tiene una unidad de transferencia 37, el segundo aparato de descifrado 30-2 puede transferir el mensaje cifrado recibido desde el primer aparato de descifrado 30-1, a otro segundo aparato de descifrado (aparato de descifrado que no intercambia un mensaje cifrado con el aparato de cifrado) o al primer aparato de descifrado (aparato de descifrado que intercambia un mensaje cifrado con el aparato de cifrado). Este proceso de transferencia se puede realizar en cualquier momento después de que el segundo aparato de descifrado 30-2 reciba el mensaje cifrado desde el primer aparato de descifrado 30-1.

(Segunda realización según el segundo aspecto)
Una segunda realización del segundo aspecto difiere de la primera realización del segundo aspecto en que el primer aparato de descifrado 30-1 y el segundo aparato de descifrado 30-2 generan la segunda información de atributo o la segunda información de predicado. Debido a esta diferencia, la segunda realización del segundo aspecto difiere en varios puntos de la primera realización del segundo aspecto. Una descripción de las partes en común entre la primera y segunda realizaciones del segundo aspecto se omite (los mismos números de referencia se asignan a los mismos componentes), y una descripción de las diferencias a partir de la primera realización del segundo aspecto se hará con referencia a las Figura 42 a 48.

Los procesos de los pasos S1 a S22 son los mismos que aquéllos en la primera realización del segundo aspecto.

Cuando la clave de descifrado no se posee en el proceso del paso S22b, una segunda unidad de adquisición de información de lógica de predicado 35 del primer aparato de descifrado 30-1 lee la política, el par de esquemas, el parámetro público, y la información de usuario de la memoria 31 y obtiene una información de atributo (llamada segunda información de atributo) o una información de predicado (llamada segunda información de predicado) a partir de la información de usuario (paso S23g). En este proceso, el esquema emparejado con el esquema identificado por la política se aplica a la información de usuario. Cuando la política es Cipher_Text_Policy, el esquema (esquema de atributo) emparejado con el esquema (esquema de predicado) identificado por Cipher_Text_Policy se usa para obtener la segunda información de atributo a partir de la información de usuario (información de designación de atributo). Cuando la política es Key_Policy, el esquema (esquema de predicado) emparejado con el esquema (esquema de atributo) identificado por Key_Policy se usa para obtener la segunda información de predicado a partir de la información usuario (información de designación de predicado). Se debería señalar que el esquema emparejado con el esquema usado en el paso S17a se usa en este proceso. En la segunda realización del segundo aspecto, la segunda información de atributo y la segunda información de predicado son un información de vector que tiene elementos del campo finito F_q como componentes (ver las Figura 11 a 13).

Después del proceso del paso S23g, se realiza el proceso del paso 23. En este proceso, la unidad de trasmisor 34 del primer aparato de descifrado 30-1 genera un mensaje de petición de clave que incluye el parámetro público, la política, el par de esquemas, y la información de autenticación leídos de la memoria 31, y la segunda información de atributo o la segunda información de predicado, bajo el control de la unidad de controlador. La unidad de trasmisor 34 del primer aparato de descifrado 30-1 envía el mensaje de petición de clave al aparato de generación de clave que ha leído la dirección de la memoria 31, y una unidad de receptor del aparato de generación de clave 20 recibe el mensaje de petición de clave.

Cuando la verificación tiene éxito en el proceso del paso S24a, se realiza el proceso del paso S24d. Dado que el aparato de generación de clave 20 ha recibido la segunda información de atributo o la segunda información de predicado desde el primer aparato de descifrado 30-1, la función y el proceso de generar la información son innecesarios, a diferencia de la primera realización del segundo aspecto.

Los procesos de los pasos S28 a S34a, a ser realizados después del proceso del paso S24d, son los mismos que

aquéllos en la primera realización del segundo aspecto.

Cuando la clave de descifrado no se posee en el proceso del paso S34b, una segunda unidad de adquisición de información de lógica de predicado 35 del segundo aparato de descifrado 30-2 lee la política, el par de esquemas, el parámetro público, y la información de usuario de la memoria 31 y obtiene una información de atributo (llamada segunda información de atributo) o una información de predicado (llamada segunda información de predicado) a partir de la información de usuario (paso S35g). En este proceso, el esquema emparejado con el esquema identificado por la política se aplica a la información de usuario. Cuando la política es Cipher_Text_Policy, el esquema (esquema de atributo) emparejado con el esquema (esquema de predicado) identificado por Cipher_Text_Policy se usa para obtener la segunda información de atributo a partir de la información de usuario (información de designación de atributo). Cuando la política es Key_Policy, el esquema (esquema de predicado) emparejado con el esquema (esquema de atributo) identificado por Key_Policy se usa para obtener la segunda información de predicado a partir de la información de usuario (información de designación de predicado). Se debería señalar que el esquema emparejado con el esquema usado en el paso S17a se usa en este proceso. En la segunda realización del segundo aspecto, la segunda información de atributo y la segunda información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes (ver las Figura 11 a 13).

Después del proceso del paso S35g, se realiza el proceso del paso 35. En este proceso la unidad de trasmisor 34 del segundo aparato de descifrado 30-2 genera un mensaje de petición de clave que incluye el parámetro público, la política, el par de esquemas, y la información de autenticación leídos de la memoria 31, y la segunda información de atributo o la segunda información de predicado, bajo el control de la unidad de controlador. La unidad de trasmisor 34 del segundo aparato de descifrado 30-2 envía el mensaje de petición de clave al aparato de generación de clave que ha leído la dirección de la memoria 31, y la unidad de receptor del aparato de generación de clave 20 recibe el mensaje de petición de clave.

Cuando la verificación tiene éxito en el proceso del paso S36a, se realiza el proceso del paso S36d. Dado que el aparato de generación de clave 20 ha recibido la segunda información de atributo o la segunda información de predicado desde el segundo aparato de descifrado 30-2, la función y el proceso para generar la información son innecesarios, a diferencia de la primera realización del segundo aspecto.

Los procesos de los pasos S40 y S41, que siguen al proceso del paso S36d, son los mismos que aquéllos en la primera realización del segundo aspecto.

(Tercera realización según el segundo aspecto)

Una tercera realización del segundo aspecto difiere de la primera realización del segundo aspecto en que la unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, junto con la clave pública incluida en el parámetro público y el texto plano M leído de la memoria 11 para obtener una información de cifrado C_1. En otras palabras, el algoritmo de cifrado de predicado descrito en la Bibliografía que no es de patente 3, por ejemplo, se usa en la tercera realización del segundo aspecto. Debido a esta diferencia, la tercera realización del segundo aspecto difiere en varios puntos de la primera realización del segundo aspecto. Una descripción de las partes en común entre la primera y tercera realizaciones del segundo aspecto se omite (los mismos números de referencia se asignan a los mismos componentes), y una descripción de las diferencias a partir de la primera realización del segundo aspecto se hará con referencia a las Figura 49 a 54.

Los procesos de los pasos S1 a S17a son los mismos que aquéllos en la primera realización del segundo aspecto. El parámetro público y alguna otra información se requieren por el algoritmo de cifrado de predicado de la tercera realización del segundo aspecto. Para información específica requerida, ver la Bibliografía que no es de patente 3, descrita anteriormente, por ejemplo.

En el proceso del paso S17b1, que sigue al proceso del paso S17a, la unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, junto con la clave pública incluida en el parámetro público y el texto plano M leído de la memoria 11, para obtener una información de cifrado C_1 según el algoritmo de cifrado de predicado (paso S17b1).

Después del proceso del paso S17b1, se realiza el proceso del paso 17d. En este proceso, la unidad de trasmisor 14 del aparato de cifrado 10 genera un mensaje cifrado que incluye la información de cifrado C_1, y el par de esquemas, la política, el parámetro público, y la dirección del aparato de generación de clave leídos de la memoria 31, bajo el control de la unidad de controlador (paso S17d).

Los procesos de los pasos S18 a S28, que siguen al proceso del paso S17d, son los mismos que aquéllos en la primera realización del segundo aspecto.

En el proceso del paso S22c1, que sigue al proceso del paso S28, la unidad de descifrado 33 del primer aparato de descifrado 30-1 lee el parámetro público, la clave de descifrado R, y la información de cifrado C_1 de la memoria 31 para calcular el texto plano M según el algoritmo de cifrado de predicado (paso S22c1).

Los procesos de los pasos S30 a S40, que siguen al proceso del paso S22c1, son los mismos que aquéllos en la primera realización del segundo aspecto.

En el proceso del paso S34c1, que sigue al proceso del paso S40, la unidad de descifrado 33 del segundo aparato de descifrado 30-2 lee el parámetro público, la clave de descifrado R, y la información de cifrado C_1 de la memoria 31 para calcular el texto plano M según el algoritmo de cifrado de predicado (paso S34c1).

(Cuarta realización según el segundo aspecto)

Una cuarta realización del segundo aspecto corresponde a una combinación de la segunda realización del segundo aspecto y la tercera realización del segundo aspecto. La cuarta realización del segundo aspecto difiere de la primera realización del segundo aspecto en que (1) el primer aparato de descifrado 30-1 y el segundo aparato de descifrado 30-2 generan la segunda información de atributo o la segunda información de predicado, y (2) la unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, junto con la clave pública incluida en el parámetro público y el texto plano M leído de la memoria 11, para obtener una información de cifrado C_1. Debido a estas diferencias, la cuarta realización del segundo aspecto difiere en varios puntos de la primera realización el segundo aspecto. Una descripción de las partes en común entre la primera y cuarta realizaciones del segundo aspecto se omite (los mismos números de referencia se asignan a los mismos componentes), y una descripción de las diferencias a partir de la primera realización del segundo aspecto se hará con referencia a las Figura 55 a 58.

Los procesos de los pasos S1 a S17a son los mismos que aquéllos en la primera realización del segundo aspecto. El parámetro público y alguna otra información se requieren por el algoritmo de cifrado de predicado de la cuarta realización del segundo aspecto. Para una información específica requerida, ver la Bibliografía que no es de patente 3, descrita anteriormente, por ejemplo.

En el proceso del paso S17b1, que sigue al proceso del paso S17a, la unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, junto con la clave pública incluida en el parámetro público y el texto plano M leído de la memoria 11, para obtener una información de cifrado C_1 según el algoritmo de cifrado de predicado (paso S17b1).

Después del proceso del paso S17b1, se realiza el proceso del paso 17d. En este proceso, la unidad de trasmisor 14 del aparato de cifrado 10 genera un mensaje cifrado que incluye la información de cifrado C_1, y el par de esquemas, la política, el parámetro público, y la dirección del aparato de generación de clave leídos de la memoria 31, bajo el control de la unidad de controlador (paso S17d).

Los procesos de los pasos S18 a S22b, que siguen al proceso del paso S17d, son los mismos que aquéllos en la primera realización del segundo aspecto.

Cuando la clave de descifrado no se posee en el proceso del paso S22b, la segunda unidad de adquisición de información de lógica de predicado 35 del primer aparato de descifrado 30-1 lee la política, el par de esquemas, el parámetro público, y la información de usuario de la memoria 31 y obtiene una información de atributo (llamada segunda información de atributo) o una información de predicado (llamada segunda información de predicado) a partir de la información de usuario (paso S23g). En este proceso, el esquema emparejado con el esquema identificado por la política se aplica a la información de usuario. Cuando la política es Cipher_Text_Policy, el esquema (esquema de atributo) emparejado con el esquema (esquema de predicado) identificado por Cipher_Text_Policy se usa a obtener la segunda información de atributo a partir de la información de usuario (información de designación de atributo). Cuando la política es Key_Policy, el esquema (esquema de predicado) emparejado con el esquema (esquema de atributo) identificado por Key_Policy se usa para obtener la segunda información de predicado a partir de la información de usuario (información de designación de predicado). Se debería señalar que el esquema emparejado con el esquema usado en el paso S17a se usa en este proceso. En la cuarta realización del segundo aspecto, la segunda información de atributo y la segunda información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes (ver las Figura 11 a 13).

Después del proceso del paso S23g, se realiza el proceso del paso 23. En este proceso, la unidad de trasmisor 34 del primer aparato de descifrado 30-1 genera un mensaje de petición de clave que incluye el parámetro público, la política, el par de esquemas, y la información de autenticación leídos de la memoria 31, y la segunda información de atributo o la segunda información de predicado, bajo el control de la unidad de controlador. La unidad de trasmisor 34 del primer aparato de descifrado 30-1 envía el mensaje de petición de clave al aparato de generación de clave que ha leído la dirección de la memoria 31, y la unidad de receptor del aparato de generación de clave 20 recibe el mensaje de petición de clave.

Cuando la verificación tiene éxito en el proceso del paso S24a, se realiza el proceso del paso S24d. Dado que el aparato de generación de clave 20 ha recibido la segunda información de atributo o la segunda información de predicado desde el primer aparato de descifrado 30-1, la función y el proceso para generar la información son

innecesarios.

El proceso del paso S28, que sigue al proceso del paso S24d, es el mismo que aquél en la primera realización del segundo aspecto.

En el proceso del paso S22c1, que sigue al proceso del paso S28, la unidad de descifrado 33 del primer aparato de descifrado 30-1 lee el parámetro público, la clave de descifrado R, y la información de cifrado C_1 de la memoria 31 para calcular el texto plano M según el algoritmo de cifrado de predicado (paso S22c1).

Los procesos de los pasos S30 a S34, que siguen al proceso del paso S22c1, son los mismos que aquéllos en la primera realización del segundo aspecto.

Cuando la clave de descifrado no se posee en el proceso del paso S34b, la segunda unidad de adquisición de información de lógica de predicado 35 del segundo aparato de descifrado 30-2 lee la política, el par de esquemas, el parámetro público, y la información de usuario de la memoria 31 y obtiene una información de atributo (llamada segunda información de atributo) o una información de predicado (llamada segunda información de predicado) a partir de la información de usuario (paso S35g). En este proceso, el esquema emparejado con el esquema identificado por la política se aplica a la información de usuario. Cuando la política es Cipher_Text_Policy, el esquema (esquema de atributo) emparejado con el esquema (esquema de predicado) identificado por Cipher_Text_Policy se usa para obtener la segunda información de atributo a partir de la información de usuario (información de designación de atributo). Cuando la política es Key_Policy, el esquema (esquema de predicado) emparejado con el esquema (esquema de atributo) identificado por Key_Policy se usa para obtener la segunda información de predicado a partir de la información de usuario (información de designación de predicado). Se debería señalar que el esquema emparejado con el esquema usado en el paso S17a se usa en este proceso. En la cuarta realización del segundo aspecto, la segunda información de atributo y la segunda información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes (ver las Figura 11 a 13).

Después del proceso del paso S35g, se realiza el proceso del paso 35. En este proceso, la unidad de trasmisor 34 del segundo aparato de descifrado 30-2 genera un mensaje de petición de clave que incluye el parámetro público, la política, el par de esquemas, y la información de autenticación leídos de la memoria 31, y la segunda información de atributo y la segunda información de predicado, bajo el control de la unidad de controlador. La unidad de trasmisor 34 del segundo aparato de descifrado 30-2 envía el mensaje de petición de clave al aparato de generación de clave que ha leído la dirección de la memoria 31, y la unidad de receptor del aparato de generación de clave 20 recibe el mensaje de petición de clave.

Cuando la verificación tiene éxito en el proceso del paso S36a, se realiza el proceso del paso S36d. Dado que el aparato de generación de clave 20 ha recibido la segunda información de atributo o la segunda información de predicado desde el segundo aparato de descifrado 30-2, la función y el proceso para generar la información son innecesarios, a diferencia de la primera realización del segundo aspecto.

El proceso del paso S40, que sigue al proceso del paso S36d, es el mismo que aquél en la primera realización del segundo aspecto.

En el proceso del paso S34c1, que sigue al proceso del paso S40, la unidad de descifrado 33 del segundo aparato de descifrado 30-2 lee el parámetro público, la clave de descifrado R, y la información de cifrado C_1 de la memoria 31 para calcular el texto plano M según el algoritmo de cifrado de predicado (paso S34c1).

Las realizaciones descritas anteriormente del segundo aspecto se implementan, por ejemplo, como sistemas de correo electrónico o sistemas de mensajes instantáneos. La Figura 59 muestra la estructura de datos intercambiados. El formato básico del mensaje entero es conforme, por ejemplo, a S/MIME (Extensiones de Correo de Internet Multipropósito Seguras). Se da una estructura de datos adecuada para los datos desde el marcador de posición de inicio de un mensaje de cifrado al marcador de posición final del mensaje cifrado en XML (el Lenguaje de Marcas Extensible) o algún otro lenguaje.

Una serie de datos que conciernen al cifrado de predicado se disponen desde el marcador de posición de inicio de un mensaje cifrado al marcador de posición final del mensaje cifrado.

Un bloque identificador de algoritmo especifica una información que identifica el algoritmo de cifrado de predicado usado para cifrar la clave privada y el algoritmo de cifrado de clave privada usado para cifrar la carga útil del mensaje. Se puede especificar un identificador que indica el algoritmo o la versión de un algoritmo (por ejemplo, PE/Versión X + Camellia (Camellia es una marca comercial registrada).

Un bloque de firma digital especifica la firma digital. Se puede usar un algoritmo de firma conocido. Este elemento se puede omitir dependiendo de la aplicación.

Un bloque de información de parámetro público especifica una información que identifica el parámetro público usado. Se puede especificar un identificador que identifica el parámetro público o los datos del parámetro público.

Un campo de política específica un identificador que identifica la política usada.

Un campo de esquema especifica un identificador que identifica el esquema usado o los datos del esquema.

Un campo de información de cifrado especifica los datos (información de cifrado) obtenidos cifrando, con el cifrado de predicado, la clave privada usada para cifrar la carga útil del mensaje (texto plano).

Un campo de texto cifrado especifica los datos (texto cifrado) obtenidos cifrando la carga útil del mensaje (texto plano).

Un campo de atributo y un campo de predicado especifican las representaciones de cadenas de letras que indican el atributo y el predicado usados para el cifrado, que corresponden al campo de política, respectivamente. Estos elementos se pueden omitir según la aplicación.

Un campo de adjunto puede incluir un fichero de adjunto cifrado con RSA, por ejemplo. Este elemento se puede omitir según la aplicación.

En una comunicación segura para mensajería instantánea, por ejemplo, no es necesario reenviar la información de cifrado obtenida cifrando la clave privada. En una mensajería instantánea habitual, cuando se obtiene una clave privada adecuada en el primer mensaje instantáneo, el receptor puede almacenar la clave privada para descifrar mensajes instantáneos posteriores. En ese caso, el remitente sólo envía texto cifrado al receptor pero puede no enviar el parámetro público, la política, el esquema, o la información de cifrado en los mensajes instantáneos posteriores. De la misma forma, cuando no se cambia el algoritmo de cifrado usado, el identificador de algoritmo de cifrado se puede omitir en los mensajes instantáneos posteriores.

El cifrado de predicado no depende de una información basada en el receptor, en el cifrado. Por lo tanto, el remitente (aparato que envía) puede enviar un mensaje cifrado a un receptor desconocido (aparato que recibe). En otras palabras, el remitente realiza un cifrado sólo una vez incluso si hay una pluralidad de receptores (aparatos que reciben) (en el sistema criptográfico de clave pública, el cifrado necesita ser realizado N veces). Por lo tanto, el remitente (aparato que envía) puede enviar un mensaje cifrado a una pluralidad de receptores a un coste bajo.

El receptor (aparato que recibe) puede transferir el mensaje cifrado recibido desde el aparato de cifrado a una tercera parte (aparato). En el sistema criptográfico de clave pública, el receptor (aparato que recibe) necesita descifrar el mensaje cifrado, cifrar el mensaje original con la clave pública de la tercera parte (aparato), y enviar el mensaje cifrado, causando un coste de procesamiento alto. En las realizaciones anteriormente descritas, dado que el mensaje cifrado recibido desde el aparato de cifrado se puede transferir a la tercera parte (aparato) sin ningún procesamiento, el mensaje cifrado se transfiere a un coste de procesamiento bajo.

Ejemplos según un tercer aspecto relativo a la presente invención, que se refieren a una tecnología de comunicación criptográfica que puede operar flexiblemente, que se basa en cifrado de predicado, y que permite un contenido (contenido cifrado) cifrado con el cifrado de predicado a ser distribuido se describirán a continuación mientras que se pone atención a la tecnología de comunicación criptográfica del primer aspecto, descrito anteriormente. En la tecnología de comunicación criptográfica del tercer aspecto, un contenido (contenido cifrado) cifrado con un cifrado de predicado se almacena en un servidor de contenido, y el contenido cifrado se distribuye a un aparato de descifrado tras una petición.

La descripción de la tecnología de comunicación criptográfica del tercer aspecto y la descripción de la tecnología de comunicación criptográfica del primer aspecto tienen muchas partes en común sustanciales, pero, para evitar referirse a descripción de la tecnología de comunicación criptográfica del primer aspecto, la tecnología de comunicación criptográfica del tercer aspecto se describirá más abajo con explicaciones que se superponen y figuras que se incluyen tanto como sea posible. Por lo tanto, en ambas descripciones, se usan números de expresión idénticos, números de referencia idénticos asignados a bloques de función, y números de referencia idénticos asignados a pasos. Debido a que los contextos son diferentes, no debería haber de riesgo de confusión.

(Primer ejemplo según el tercer aspecto)
Un primer ejemplo según el tercer aspecto se describirá más abajo con referencia a las Figura 60 a 71.

Como se muestra en la Figura 60, un sistema criptográfico 1 según el tercer aspecto incluye una pluralidad de aparatos cliente 10 y 30, uno o una pluralidad de aparatos de generación de clave 20, uno o una pluralidad de servidores de contenido 60, uno o una pluralidad de aparatos de gestión de información de usuario 40 (en lo sucesivo cada uno llamado aparato de gestión), aparatos de gestión de par de información de regla de conversión 50 (en lo sucesivo cada uno llamado aparato de registro), uno o una pluralidad de aparatos el mantenimiento 80, y

uno o una pluralidad de aparatos de autenticación 90. Estos aparatos pueden comunicar unos con otros a través de una red de comunicación 5, tal como Internet.

Los aparatos cliente funcionan como aparatos de cifrado para cifrar contenido para generar contenido cifrado o aparatos de descifrado para descifrar el contenido cifrado, en base a sus funciones de procesamiento. Dependiendo de sus funciones, los aparatos cliente se llaman aparatos de cifrado 10 o aparatos de descifrado 30. El sistema criptográfico 1 del tercer aspecto puede incluir aparatos cliente que funcionan solamente como aparatos de cifrado y/o aparatos cliente que funcionan solamente como aparatos de descifrado.

En el sistema criptográfico 1 del tercer aspecto, el cifrado y el descifrado se realizan usando cifrado de predicado. En el tercer aspecto, el algoritmo de cifrado de predicado a ser usado no está limitado, y se puede usar el algoritmo de cifrado de predicado descrito en la Bibliografía que no es de patente 3, por ejemplo. En el primer ejemplo del tercer aspecto, se usará un algoritmo de cifrado de predicado de tipo KEM (el mecanismo de encapsulación de clave).

Un método de comunicación criptográfico usado en el sistema criptográfico 1 se describirá con referencia a las Figura 61, 62, 63, 64, 66, 69, y 71. Ver las Figura 65, 67, 68, y 70 para la estructura funcional de cada aparato.

<<Proceso de preparación>>
La descripción entera del <<proceso de preparación>> en el primer ejemplo del primer aspecto se incorpora aquí y se omite una descripción del <<proceso de preparación>>. Ver la Figura 61 para el proceso de preparación, las Figura 11 a 13 para los pares de esquemas, y la Figura 14 para las listas de políticas. La descripción del proceso de preparación finaliza aquí.

<<Proceso de cifrado>>
Bajo el control de una unidad de controlador, no mostrada, una unidad de trasmisor 14 del aparato de cifrado 10 envía una consulta de búsqueda al aparato de registro 50, y la unidad de recepción del aparato de registro 50 recibe la consulta de búsqueda (paso S14). La unidad de búsqueda del aparato de registro 50 busca algunas o todas las entradas registradas en la unidad de almacenamiento del aparato de registro 50 y elige una entrada (paso S15). La unidad de trasmisor del aparato de registro 50 envía la entrada al aparato de cifrado 10, y una unidad de receptor del aparato de cifrado 10 recibe la entrada (paso S16). Esta entrada incluye la dirección del aparato de generación de clave, el parámetro público del aparato de generación de clave, la lista de políticas que se puede usar por el aparato de generación de clave, y la lista de esquemas que se puede usar por el aparato de generación de clave. Esta entrada recibida se almacena en una memoria 11 del aparato de cifrado 10.

Cuando el aparato de cifrado 10 tiene el parámetro público, la lista de esquemas, la lista de políticas, y la dirección de cada aparato de generación de clave 20 por adelantado, se omiten los procesos de los pasos S14 a S16. Se debería señalar que el sistema criptográfico 1 puede no tener el aparato de registro 50.

Una primera unidad de adquisición de información de lógica de predicado 12 del aparato de cifrado 10 lee la información de entrada, la política, y los esquemas desde la memoria 11 y obtiene una información de atributo (en lo sucesivo llamada primera información de atributo) y una información de predicado (en lo sucesivo llamada primera información de predicado) (paso S17a). Los detalles de este proceso se describirán más abajo con referencia a las Figura 12 y 13.

Cuando la lista de esquemas tiene una pluralidad de pares de esquemas, se selecciona un par de esquema en base al uso o similar. El usuario del aparato de cifrado 10 puede seleccionar un par de esquemas y una información de designación de entrada del mismo. Alternativamente, la primera unidad de adquisición de información de lógica de predicado 12 puede seleccionar un par de esquemas según una regla predeterminada.

Según si la información de entrada es una información de designación de atributo o una información de designación de predicado, se selecciona uno de los esquemas junto con la política. El usuario del aparato de cifrado 10 puede seleccionar la política y uno de los esquemas y una información de designación de entrada del mismo. Alternativamente, la primera unidad de adquisición de información de lógica de predicado 12 puede seleccionar la política y uno de los esquemas según una regla predeterminada. Cuando solamente se prepara un tipo de política en el aparato de generación de clave 20, se selecciona un esquema del par de esquemas según la política. Si el esquema seleccionado no corresponde al tipo de la información de entrada, un par de esquemas necesita ser seleccionado de nuevo de la lista de esquemas o una entrada necesita ser proporcionada por el aparato de registro 50 de nuevo.

La información de entrada puede ser una información introducida por el usuario del aparato de cifrado 10 o una información adquirida por una unidad de adquisición (no mostrada) del aparato de cifrado 10 desde un medio de almacenamiento tal como una tarjeta IC 39.

Entonces, la primera unidad de adquisición de información de lógica de predicado 12 usa el esquema seleccionado a partir del par de esquemas según la política para obtener la primera información de atributo o la primera

información de predicado a partir de la información de entrada. Cuando la política es Key_Policy y el esquema seleccionado es un esquema de atributo, se obtiene la primera información de atributo. Cuando la política es Cipher_Text_Policy y el esquema seleccionado es un esquema de predicado, se obtiene la primera información de predicado. La primera información de atributo y la primera información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes en el primer ejemplo según el tercer aspecto (ver las Figura 11 a 13). El esquema se usa para extraer o disponer valores de atributos necesarios a partir de la información de entrada.

A continuación, una unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, una base ortogonal B (clave pública sustancial) incluida en el parámetro público leído de la memoria 11, y un contenido M para obtener una clave común K, una información de cifrado C_1, y un texto cifrado C_2 (pasos S17b y S17c). Los detalles de estos procesos se describirán más abajo.

Una primera unidad de cifrado 13a genera los números aleatorios r y ρ que son elementos del campo finito F_q según el algoritmo de cifrado de predicado, especifica la clave común K como se muestra por la Expresión (7), descrita anteriormente, y obtiene la información de cifrado C_1 según la Expresión (8) (paso S17b), donde H indica, por ejemplo, una función de cálculo de claves. En este ejemplo, se usa la primera información de atributo v. Para usar la primera información de predicado, v necesita ser sustituido con w en la Expresión (8), descrita anteriormente. En este ejemplo, la información de cifrado C_1 corresponde a ρ usada para generar la clave común K. La información de cifrado C_1 puede corresponder a la clave común K.

A continuación, la segunda unidad de cifrado 13b usa la clave común K y el contenido M para obtener el texto cifrado C_2 según la Expresión (9), descrita anteriormente (paso S17c). Un método de cifrado Enc_k que usa la clave privada puede ser un método conocido. Por ejemplo, puede ser el método descrito en la Bibliografía que no es de patente 1.

A continuación, bajo el control de la unidad de controlador, la unidad de transmisor 14 del aparato de cifrado 10 genera un mensaje de cifrado que incluye la información de cifrado C_1 y el contenido cifrado C_2, junto con el par de esquemas, la política, el parámetro público, y la dirección del aparato de generación de clave leídos de la memoria 11 (paso S17d). La unidad de transmisor 14 del aparato de cifrado 10 entonces envía el mensaje cifrado al servidor de contenido 60, y una unidad de receptor del servidor de contenido 60 recibe el mensaje cifrado (paso S18). El contenido cifrado se carga mediante un método conocido tal como FTP (protocolo de transferencia de ficheros) o WebDAV (protocolo de creación y control de versiones distribuido para la WWW).

La descripción del <<proceso de cifrado>> finaliza aquí.

<<Proceso de entrega de contenido>>
Bajo el control de una unidad de controlador, el servidor de contenido 60 almacena, en una memoria 61 del mismo, el mensaje cifrado enviado desde cada aparato de cifrado 10. Con esto, la información de cifrado y el contenido cifrado incluidos en el mensaje cifrado se registran en el servidor de contenido 60. El contenido cifrado registrado en el servidor de contenido 60 se hace público, por ejemplo, en una página web.

La página web se visualiza en una unidad de visualización, no mostrada, del aparato de descifrado 30 mediante una unidad de navegador 38 del aparato de descifrado 30 según el protocolo de Internet. El usuario del aparato de descifrado 30 realiza una operación de entrada para seleccionar un contenido cifrado deseado. En base a la información de entrada de usuario, la unidad de navegador 38 del aparato de descifrado 30 envía una petición de adquisición para adquirir el contenido cifrado seleccionado desde el servidor de contenido 60, a una unidad de descifrado 33 (en lo sucesivo llamada unidad de retransmisión) del aparato de descifrado 30 (paso S19). Entonces, la unidad de retransmisión 33 del aparato de descifrado 30 envía esta petición de adquisición al servidor de contenido 60, y una unidad de receptor del servidor de contenido 60 recibe la petición de adquisición (paso S20). En este sentido, la unidad de navegador 38 y el servidor de contenido 60 realizan intercambios a través de la unidad de retransmisión 33 según, por ejemplo, HTTP (protocolo de transferencia de hipertexto) (se puede usar el ajuste de intermediario de un navegador WWW). Una unidad de búsqueda 62 del servidor de contenido 60 busca el mensaje cifrado que incluye el contenido cifrado especificado en la petición de adquisición y lo selecciona (paso S21). Una unidad de transmisor 64 del servidor de contenido 60 envía el mensaje cifrado al aparato de descifrado 30 bajo el control de la unidad de búsqueda 62, y una unidad de receptor del aparato de descifrado recibe el mensaje cifrado (paso S22).

La descripción del <<proceso de entrega de contenido>> finaliza aquí.

<<Proceso de descifrado>>
Bajo el control de una unidad de controlador, no mostrada, una unidad de transmisor 34 del aparato de descifrado 30 envía una consulta de búsqueda que incluye la dirección del aparato de generación de clave, la dirección que se incluye en el mensaje cifrado, al aparato de registro 50, y la unidad de recepción del aparato de registro 50 recibe la consulta de búsqueda (paso S23). La unidad de búsqueda del aparato de registro 50 busca la entrada del aparato

de generación de clave especificada por la dirección y la selecciona (paso S24). La unidad de transmisor del aparato de registro 50 envía la entrada del resultado de búsqueda al aparato de descifrado 30, y la unidad de receptor del aparato de descifrado 30 recibe la entrada (paso S25). Esta entrada incluye la dirección del aparato de generación de clave, el parámetro público del aparato de generación de clave, la lista de políticas que se puede usar por el aparato de generación de clave, y la lista de esquemas que se puede usar por el aparato de generación de clave. La entrada recibida se almacena en una memoria 31 del aparato de descifrado 30.

Cuando el aparato de descifrado 30 tiene el parámetro público, la lista de esquemas, la lista de políticas, y la dirección de cada aparato de generación de clave 20 por adelantado, se omiten los procesos de los pasos S19 a S21. En ese caso, el aparato de descifrado 30 busca en la memoria 31 la entrada del aparato de generación de clave que corresponde a la dirección incluida en el mensaje cifrado y la recupera.

Bajo el control de la unidad de controlador, una unidad de verificación (no mostrada) del aparato de descifrado 30 verifica que el par de esquemas y la política incluida en el mensaje cifrado están incluidos en la lista de esquemas y la lista de políticas incluidas en la entrada obtenida desde el aparato de registro 50 (paso S26a). Si esta verificación falla, el proceso finaliza con un fallo de procesamiento de descifrado (paso S26g).

Cuando la verificación tiene éxito, una unidad de adquisición 32 del aparato de descifrado 30 lee la información de designación de atributo o la información de designación de predicado que corresponde al usuario del aparato de descifrado 30 desde un medio de almacenamiento tal como la tarjeta IC 39 (paso S26f). Si se lee la información de designación de atributo o la información de designación de predicado depende de la política incluida en el mensaje cifrado. Más específicamente, la información de designación leída corresponde al contenido de la política que identifica un esquema emparejado con el otro esquema identificado por la política incluida en el mensaje cifrado. Cuando la política es Cipher_Text_Policy, la unidad de adquisición 32 lee la información de designación de atributo desde el medio de almacenamiento. Cuando la política es Key_Policy, la unidad de adquisición 32 lee la información de designación de predicado desde el medio de almacenamiento. La información de designación leída en lo sucesivo se llama información de usuario. La unidad de adquisición 32 del aparato de descifrado 30 puede leer desde el aparato de gestión 40 la información de designación de atributo o la información de designación de predicado que corresponde al usuario del aparato de descifrado 30, de la misma forma que en <<un proceso de adquisición de información de usuario>> en el aparato de generación de clave 20, descrito más tarde. En el primer ejemplo del tercer aspecto, se puede omitir el proceso del paso S26f. Cuando el aparato de descifrado 30 tiene la información de designación de atributo y la información de designación de predicado que corresponde al usuario por adelantado, o bien la información de designación de atributo o bien la información de designación de predicado sirve como una información de usuario, según la política.

A continuación, la unidad de verificación del aparato del descifrado 30 verifica que el aparato de descifrado 30 tiene la clave de descifrado a ser usada para descifrar la información de cifrado incluida en el mensaje de cifrado (paso S26b).

El aparato de descifrado 30 almacena una tabla de claves de descifrado en la memoria 31. En la tabla de claves de descifrado, como se muestra en la Figura 15, por ejemplo, el identificador de cada aparato de generación de clave está asociado con el parámetro público, el par de esquemas, el objetivo de clave de descifrado, la información de designación de predicado, y la clave de descifrado. La unidad de verificación verifica que el aparato de descifrado 30 tiene la clave de descifrado que corresponde al identificador del aparato de generación de clave determinado desde la dirección incluida en el mensaje cifrado, al parámetro público, al par de esquemas, y al objetivo de clave de descifrado (que corresponde al contenido de la política que identifica un esquema emparejado con el otro esquema identificado por la política incluida en el mensaje cifrado). Cuando el aparato de descifrado 30 tienen la clave de descifrado, se realiza el proceso del paso S33. Si el aparato de descifrado 30 no tiene la clave de descifrado, se realiza el proceso del paso S27.

La descripción del <<proceso de descifrado>> se detiene temporalmente aquí y se describirá más abajo <<un proceso de generación de clave>>.

Si el aparato de descifrado 30 no tiene la clave de descifrado, la unidad de trasmisor 34 del aparato de descifrado 30 genera, bajo el control de la unidad de controlador, un mensaje de petición de clave que incluye el parámetro público, la política, el par de esquemas, la información de usuario (en su caso), y la información de autenticación, todos estos elementos que se leen de la memoria 31. La información de autenticación incluye, por ejemplo, el ID del usuario y una contraseña. La unidad de trasmisor 34 del aparato de descifrado 30 envía el mensaje de petición de clave al aparato de generación de clave que ha leído la dirección de la memoria 31, y la unidad de receptor del aparato de generación de clave 20 recibe el mensaje de petición de clave (paso S27). El mensaje de petición de clave recibido se almacena en una memoria 21 del aparato de generación de clave 20.

Bajo el control de una unidad de controlador, una unidad de verificación (no mostrada) del aparato de generación de clave 20 verifica que el par de esquemas y la política incluida en el mensaje de petición de clave se incluyen en la lista de esquemas y la lista de políticas incluidas en la entrada propiedad del aparato de generación de clave 20 (por

ejemplo, la entrada generada en el paso S1) y que el parámetro público incluido en el mensaje de petición de clave es idéntico al parámetro público del aparato de generación de clave 20 (paso S28a). Si esta verificación falla, el proceso finaliza con un fallo del proceso de generación de clave (paso S28g). Cuando la información de autenticación se incluye en el mensaje de petición de clave, la información de autenticación también se verifica en el proceso del paso S28a. El aparato de generación de clave 20 almacena una tabla de autenticación en la memoria 21. En la tabla de autenticación, como se muestra la Figura 16, por ejemplo, cada ID de usuario se asocia con una contraseña. La unidad de verificación verifica que el ID de usuario y la contraseña incluidos en el mensaje de petición de clave son idénticos al ID de usuario y la contraseña incluidos en la tabla de autenticación. Si la verificación falla, se realiza el proceso del paso S28g.

Cuando esta verificación tiene éxito, la unidad de verificación del aparato de generación de clave 20 verifica que el mensaje de petición de clave incluye la información de usuario (paso S28b). Cuando el mensaje de petición de clave incluye la información de usuario, se realiza el proceso del paso S28c. Si el mensaje de petición de clave no incluye la información de usuario, se realiza el proceso del paso S29. Cuando se emplea un método en el cual un mensaje de petición de clave siempre incluye información de usuario, el proceso del paso S28b y <<un proceso de adquisición de información de usuario>>, descrito más tarde, son innecesarios.

La descripción del <<proceso de generación de clave>> se detiene temporalmente aquí y se describirá más abajo <<el proceso de adquisición de información de usuario>>.

La unidad de transmisor 24 del aparato de generación de clave 20 envía una petición que incluye la política y la información de autenticación (en su caso) incluidas en el mensaje de petición de clave al aparato de gestión 40, y el aparato de gestión 40 recibe la petición (paso S29). La petición recibida se almacena en una memoria del aparato de gestión 40.

El aparato de gestión 40 almacena una tabla de autenticación en la memoria. De la misma forma que en la tabla de autenticación descrita anteriormente, el ID de usuario está asociado con la contraseña en esta tabla de autenticación (ver la Figura 16). Una unidad de verificación (no mostrada) del aparato de gestión 40 verifica que el ID de usuario y la contraseña incluidos en la petición son idénticos al ID de usuario y la contraseña incluidos en la tabla de autenticación.

Cuando esta verificación tiene éxito, una unidad de búsqueda (no mostrada) del aparato de gestión 40 busca una tabla de información de usuario almacenada en la memoria para la información de designación de atributo o la información de designación de predicado según la política incluida en la petición (paso S30). La tabla de información de usuario incluye, por ejemplo, una primera tabla formada de cada ID de usuario, y un nombre de atributo y una información de designación de atributo asociados con el ID de usuario, y una segunda tabla formada del ID de usuario y una información de designación de predicado asociada con el ID de usuario (ver la Figura 17). Si se lee la información de designación de atributo o la información de designación de predicado se determina por la política incluida en la petición. Más específicamente, la información leída corresponde al contenido de la política que identifica un esquema emparejado con el otro esquema identificado por la política incluida en la petición. Cuando la política es Cipher_Text_Policy, la unidad de búsqueda lee la información de designación de atributo que corresponde al ID de usuario incluido en la petición a partir de la primera tabla. Cuando la política es Key_Policy, la unidad de búsqueda lee la información de designación de predicado que corresponde al ID de usuario incluido en la petición a partir de la segunda tabla. La información de designación leída en lo sucesivo se llama información de usuario.

Bajo el control de una unidad de controlador, una unidad de transmisor del aparato de gestión 40 envía la información de usuario al aparato de generación de clave 20, y la unidad de receptor del aparato de generación de clave 20 recibe la información de usuario (paso S31). La información de usuario recibida se almacena en la memoria 21 del aparato de generación de clave 20.

La descripción del <<proceso de adquisición de información de usuario>> finaliza aquí, y se resumirá la descripción del <<proceso de generación de clave>>.

Cuando el aparato de generación de clave 20 ya tiene la información de usuario o recibe la información de usuario a través del proceso de adquisición de información de usuario (paso S31), una segunda unidad de adquisición de información de lógica de predicado 23 del aparato de generación de clave 20 lee la política, el par de esquemas, el parámetro público, y la información de usuario de la memoria 21, y obtiene una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (segunda información de predicado) a partir de la información de usuario (paso S28c). En este proceso, el esquema emparejado con el esquema identificado por la política se aplica a la información de usuario. Cuando la política es Cipher_Text_Policy, el esquema (esquema de atributo) emparejado con el esquema (esquema de predicado) identificado por Cipher_Text_Policy se usa para obtener la segunda información de atributo a partir de la información de usuario (información de designación de atributo). Cuando la política es Key_Policy, el esquema (esquema de predicado) emparejado con el esquema (esquema de atributo) identificado por Key_Policy se usa para obtener la segunda

información de predicado a partir de la información de usuario (información de designación de predicado). Se debería señalar que el esquema emparejado con el esquema usado en el paso S17a se usa en este proceso. En el primer ejemplo del tercer aspecto, la segunda información de atributo y la segunda información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes (ver las Figura 11 a 13). El esquema se usa para extraer y disponer los valores de atributos necesarios a partir de la información de entrada.

A continuación, una unidad de generación de clave 25 del aparato de generación de clave 20 genera un número aleatorio α que es un elemento del campo finito F_q, en base al parámetro público q según el algoritmo de cifrado de predicado, y usa el número aleatorio α, la segunda información de atributo $v_{(p)} = (v_{(p)1}, \ldots, v_{(p)n})$ o la segunda información de predicado $w_{(p)} = (w_{(p)1}, \ldots, w_{(p)n})$ leídos de la memoria 21, y una clave privada B* del aparato de generación de clave para obtener una clave de descifrado R según la Expresión (10), descrita anteriormente (paso S28d). La segunda información de predicado $w_{(p)}$ se usa en este ejemplo debido a que la información de entrada usada en el proceso de cifrado es la información de designación de atributo. Cuando la información de entrada es la información de designación de predicado, se usa la segunda información de atributo $v_{(p)}$. Por lo tanto, $w_{(p)}$ necesita ser sustituida con $v_{(p)}$ en la Expresión (10), descrita anteriormente.

A continuación, bajo el control de la unidad de controlador, la unidad de transmisor 24 del aparato de generación de clave 20 envía la clave de descifrado R al aparato de descifrado 30, y la unidad de receptor del aparato de descifrado 30 recibe la clave de descifrado R (paso S32). La clave de descifrado recibida R se almacena en la memoria 31 del aparato de descifrado 30.

La descripción del <<proceso de generación de clave>> finaliza aquí, y se resumirá la descripción del <<proceso de descifrado>>.

Cuando el aparato de descifrado 30 ya tiene la clave de descifrado o recibe la clave de descifrado a través del proceso de generación de clave (paso S32), la unidad de retransmisión 33 del aparato de descifrado 30 lee el parámetro público, la clave de descifrado R, la información de cifrado C_1, y el contenido cifrado C_2 (si es necesario) de la memoria 31, y obtiene la clave común K y el contenido M (si es necesario) (paso S33).

Los detalles del proceso en el paso 33 se describirán más abajo. La unidad de retransmisión 33 incluye una primera unidad de descifrado 33a y una segunda unidad de descifrado 33b para el descifrado.

La primera unidad de descifrado 33a lee el parámetro público, la clave de descifrado R, y la información de cifrado C_1 de la memoria 31, y obtiene $e(C_1, R)$ según el algoritmo de cifrado de predicado. Como se muestra en la Expresión (11), descrita anteriormente, el resultado del cálculo depende del resultado del producto interior canónico de la primera información de atributo v y la segunda información de predicado $w_{(p)}$ sacadas de la información de cifrado C_1 y la clave de descifrado R según una bilinealidad cuando la información de entrada es la información de designación de atributo. Cuando la información de entrada es la información de designación de predicado, v necesita ser sustituida con $v_{(p)}$ y $w_{(p)}$ necesita ser sustituida con w en la Expresión (11), descrita anteriormente. El resultado del cálculo depende del resultado del producto interior canónico de la primera información de predicado w y la segunda información de atributo $v_{(p)}$ sacadas de la información de cifrado C_1 y la clave de descifrado R según una bilinealidad. En la Expresión (11), $e(b_i, b_i^*)$ se define como se muestra en la Expresión (12), descrita anteriormente, donde δ_{ij} es el símbolo de la delta de Kronecker.

Por lo tanto, cuando el producto interior canónico de la primera información de atributo v y la segunda información de predicado $w_{(p)}$ es cero (o cuando el producto interior canónico de la primera información de predicado w y la segunda información de atributo $v_{(p)}$ es cero), se obtiene el resultado del cálculo en la Expresión (11), g_T^{ρ}. Cuando se obtiene el resultado del cálculo, g_T^{ρ}, la primera unidad de descifrado 33a del aparato de descifrado 30 obtiene la clave común K, que es correcta, según la Expresión (7), descrita anteriormente (paso S26c). Cuando el producto interior canónico de la primera información de atributo v y la segunda información de predicado $w_{(p)}$ no es cero (o cuando el producto interior canónico de la primera información de predicado w y la segunda información de atributo $v_{(p)}$ no es cero), la primera unidad de descifrado 33a obtiene un valor incorrecto según la Expresión (7), descrita anteriormente. En este ejemplo, se supone que la función de cálculo de claves H es común al sistema o está incluida en el parámetro público. La información de cifrado C_1 corresponde a la información ρ usada para generar la clave común K en este ejemplo. Cuando una información de cifrado C_1 corresponde a la clave común K, el resultado del cálculo en la Expresión (11), descrita anteriormente, es la clave común K (o valor incorrecto). En otras palabras, un usuario autorizado del aparato de descifrado 30 tiene una información de designación de predicado que da la segunda información de predicado $w_{(p)}$ que hace el producto interior canónico con la primera información de atributo v cero, o una información de designación de atributo que da la segunda información de atributo $v_{(p)}$ que hace el producto interior canónico con la primera información de predicado w cero.

Entonces, una segunda unidad de descifrado 33b usa la clave común K y el contenido cifrado C_2 para calcular el contenido M según la Expresión (13), descrita anteriormente (paso S26d). Un método de descifrado Dec_k que usa la clave privada corresponde al método de cifrado Enc_k.

Si el resultado del cálculo en la Expresión (11), descrita anteriormente, es un valor incorrecto, el texto plano M correcto no se puede obtener por la Expresión (13), descrita anteriormente.

El aparato de descifrado 30 puede almacenar la clave de descifrado R en la tabla de claves de descifrado. Además, el aparato de descifrado 30 puede almacenar la clave común K en la tabla de claves de descifrado.

El contenido M, obtenido descifrando el contenido cifrado, se envía desde la unidad de retransmisión 33 a la unidad de navegador 38 (paso S34), y la unidad de navegador 38 visualiza el contenido M en una unidad de visualización del aparato de descifrado 30 (paso S35).

La descripción del <<proceso de descifrado>> finaliza aquí.

(Segundo ejemplo según el tercer aspecto)
Un segundo ejemplo del tercer aspecto difiere del primer ejemplo del tercer aspecto en que el aparato de descifrado 30 genera la segunda información de atributo o la segunda información de predicado. Debido esta diferencia, el segundo ejemplo del tercer aspecto difiere en varios puntos del primer ejemplo del tercer aspecto. Una descripción de las partes en común entre el primer y segundo ejemplos del tercer aspecto se omite (los mismos números de referencia se asignan a los mismos componentes), y se hará una descripción de las diferencias a partir del primer ejemplo del tercer aspecto con referencia a las Figura 72 a 75.

Los procesos de los pasos S1 a S26b son los mismos que aquéllos en el primer ejemplo del tercer aspecto.

Cuando la clave de descifrado no se posee en el proceso del paso S26b, una segunda unidad de adquisición de información de lógica de predicado 35 del aparato de descifrado 30 lee la política, el par de esquemas, el parámetro público, y la información de usuario de la memoria 31 y obtiene una información de atributo (llamada segunda información de atributo) o una información de predicado (llamada segunda información de predicado) a partir de la información de usuario (paso S27g). En este proceso, el esquema emparejado con el esquema identificado por la política se aplica a la información de usuario. Cuando la política es Cipher_Text_Policy, el esquema (esquema de atributo) emparejado con el esquema (esquema de predicado) identificado mediante Cipher_Text_Policy se usa para obtener la segunda información de atributo a partir de la información de usuario (información de designación de atributo). Cuando la política es Key_Policy, el esquema (esquema de predicado) emparejado con el esquema (esquema de atributo) identificado por Key_Policy se usa para obtener la segunda información de predicado a partir de la información de usuario (información de designación de predicado). Se debería señalar que el esquema emparejado con el esquema usado en el paso S17a se usa en este proceso. En el segundo ejemplo del tercer aspecto, la segunda información de atributo y la segunda información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes (ver las Figura 11 a 13).

Después del proceso del paso S27g, se realiza el proceso del paso 27. En este proceso, la unidad de trasmisor 34 del aparato de descifrado 30 genera un mensaje de petición de clave que incluye el parámetro público, la política, el par de esquemas, y la información de autenticación leídos de la memoria 31, y la segunda información de atributo o la segunda información de predicado, bajo el control de la unidad de controlador. La unidad de trasmisor 34 del aparato de descifrado 30 envía el mensaje de petición de clave al aparato de generación de clave que ha leído la dirección de la memoria 31, y la unidad de receptor del aparato de generación de clave 20 recibe el mensaje de petición de clave.

Cuando la verificación tiene éxito en el proceso del paso S28a, se realiza el proceso del paso S28d. Dado que el aparato de generación de clave 20 ha recibido la segunda información de atributo o la segunda información de predicado desde el aparato de descifrado 30, la función y el proceso para generar la información son innecesarios, a diferencia del primer ejemplo del tercer aspecto.

Los procesos de los pasos S32 a S35, a ser realizados después del proceso del paso S28d, son los mismos que aquéllos en el primer ejemplo del tercer aspecto.

(Tercer ejemplo según el tercer aspecto)
Un tercer ejemplo del tercer aspecto difiere del primer ejemplo del tercer aspecto en que la unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, junto con la clave pública incluida en el parámetro público y el contenido M leídos de la memoria 11, para obtener un contenido de cifrado C_1. En otras palabras, el algoritmo de cifrado de predicado descrito en la Bibliografía que no es de patente 3, por ejemplo, se usa en el tercer ejemplo del tercer aspecto. Debido a esta diferencia, el tercer ejemplo del tercer aspecto difiere en varios puntos del primer ejemplo del tercer aspecto. Una descripción de las partes en común entre el primer y tercer ejemplos del tercer aspecto se omite (los mismos números de referencia se asignan a los mismos componentes), y se hará una descripción de las diferencias a partir del primer ejemplo del tercer aspecto con referencia a las Figura 76 a 79.

Los procesos de los pasos S1 a S17a son los mismos que aquéllos en el primer ejemplo del tercer aspecto. El parámetro público y alguna otra información se requieren por el algoritmo de cifrado de predicado del tercer ejemplo del tercer aspecto. Para información específica requerida, ver la Bibliografía que no es de patente 3, descrita anteriormente, por ejemplo.

En el proceso del paso S17b1, que sigue al proceso del paso S17a, la unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, junto con la clave pública incluida en el parámetro público y el contenido M leídos de la memoria 11, para obtener el contenido cifrado C_1 según el algoritmo de cifrado de predicado (paso S17b1).

Después del proceso del paso S17b1, se realiza el proceso del paso 17d. En este proceso, la unidad de transmisor 14 del aparato de cifrado 10 genera un mensaje cifrado que incluyen el contenido cifrado C_1, y el par de esquemas, la política, el parámetro público, y la dirección del aparato de generación de clave leídos de la memoria 31, bajo el control de la unidad de controlador (paso S17d).

Los procesos de los pasos S18 a S32, que siguen al proceso del paso S17d, son los mismos que aquéllos en el primer ejemplo del tercer aspecto.

En el proceso del paso S26c1, que sigue al proceso del paso S32, una unidad de descifrado 33c incluida en la unidad de retransmisión 33 del aparato de descifrado 30 lee el parámetro público, la clave de descifrado R, y el contenido cifrado C_1 de la memoria 31 para calcular el contenido M según el algoritmo de cifrado de predicado (paso S26c1).

Los procesos de los pasos S34 y S35, que siguen al proceso del paso S26c1, son los mismos que aquéllos en el primer ejemplo del tercer aspecto.

(Cuarto ejemplo según el tercer aspecto)
Un cuarto ejemplo del tercer aspecto corresponde a una combinación del segundo ejemplo del tercer aspecto y el tercer ejemplo del tercer aspecto. El cuarto ejemplo del tercer aspecto difiere del primer ejemplo del tercer aspecto en que (1) el aparato de descifrado 30 genera la segunda información de atributo o la segunda información de predicado, y (2) la unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, junto con la clave pública incluida en el parámetro público y el contenido M leídos de la memoria 11, para obtener el contenido cifrado C_1. Debido a estas diferencias, el cuarto ejemplo del tercer aspecto difiere en varios puntos del primer ejemplo del tercer aspecto. Una descripción de las partes en común entre el primer y cuarto ejemplos del tercer aspecto se omite (los mismos números de referencia se asignan a los mismos componentes), y se hará una descripción de las diferencias del primer ejemplo del tercer aspecto con referencia a las Figura 80 y 81.

Los procesos de los pasos S1 a S17a son los mismos que aquéllos en el primer ejemplo del tercer aspecto. El parámetro público y alguna otra información se requieren por el algoritmo de cifrado de predicado del cuarto ejemplo del tercer aspecto. Para información específica requerida, ver la Bibliografía que no es de patente 3, descrita anteriormente, por ejemplo.

En el proceso del paso S17b1, que sigue al proceso del paso S17a, una unidad de cifrado 13 del aparato de cifrado 10 usa la primera información de atributo $v = (v_1, \ldots, v_n)$ o la primera información de predicado $w = (w_1, \ldots, w_n)$, junto con la clave pública incluida en el parámetro público y el contenido M leídos de la memoria 11, para obtener el contenido cifrado C_1 según el algoritmo de cifrado de predicado (paso S17b1).

Después del proceso del paso S17b1, se realiza el proceso del paso 17d. En este proceso, la unidad de transmisor 14 del aparato de cifrado 10 genera un mensaje cifrado que incluye el contenido cifrado C_1, y el par de esquemas, la política, el parámetro público, y la dirección del aparato de generación de clave leídos de la memoria 31, bajo el control de la unidad de controlador (paso S17d).

Los procesos de los pasos S18 a S26b, que siguen al proceso del paso S17d, son los mismos que aquéllos en el primer ejemplo del tercer aspecto.

Cuando la clave de descifrado no se posee en el proceso del paso S26b, la segunda unidad de adquisición de información de lógica de predicado 35 del aparato de descifrado 30 lee la política, el par de esquemas, el parámetro público, y la información de usuario de la memoria 31 y obtiene una información de atributo (llamada segunda información de atributo) o una información de predicado (llamada segunda información de predicado) a partir de la información de usuario (paso S27g). En este proceso, se aplica el esquema emparejado con el esquema identificado por la política a la información de usuario. Cuando la política es Cipher_Text_Policy, el esquema (esquema de atributo) emparejado con el esquema (esquema de predicado) identificado por Cipher_Text_Policy se usa para obtener la segunda información de atributo a partir de la información de usuario (información de designación de atributo). Cuando la política es Key_Policy, el esquema (esquema de predicado) emparejado con el esquema

(esquema de atributo) identificado por Key_Policy se usa para obtener la segunda información de predicado a partir de la información de usuario (información de designación de predicado). Se debería señalar que el esquema emparejado con el esquema usado en el paso S17a se usa en este proceso. En el cuarto ejemplo del tercer aspecto, la segunda información de atributo y la segunda información de predicado son una información de vector que tiene elementos del campo finito F_q como componentes (ver las Figura 11 a 13).

Después del proceso del paso S27g, se realiza el proceso del paso 27. En este proceso, la unidad de transmisor 34 del aparato de descifrado 30 genera un mensaje de petición de clave que incluye el parámetro público, la política, el par de esquemas, y la información de autenticación leídos de la memoria 31, y la segunda información de atributo o la segunda información de predicado, bajo el control de la unidad de controlador. La unidad de transmisor 34 del aparato de descifrado 30 envía el mensaje de petición de clave al aparato de generación de clave que ha leído la dirección de la memoria 31, y la unidad de receptor del aparato de generación de clave 20 recibe el mensaje de petición de clave.

Cuando la verificación tiene éxito en el proceso del paso S28a, se realiza el proceso del paso S28d. Dado que el aparato de generación de clave 20 ha recibido la segunda información de atributo o la segunda información de predicado desde el aparato de descifrado 30, la función y el proceso para generar la información son innecesarios.

El proceso del paso S32, que sigue al proceso del paso S28d, es el mismo que aquél en el primer ejemplo del tercer aspecto.

En el proceso del paso S26c1, que sigue al proceso del paso S32, la unidad de descifrado 33 del aparato de descifrado 30 lee el parámetro público, la clave de descifrado R, y el contenido cifrado C_1 de la memoria 31 para calcular el contenido M según el algoritmo de cifrado de predicado (paso S26c1).

Los procesos de los pasos S34 y S35, a ser realizados después del proceso del paso S26c1, son los mismos que aquéllos en el primer ejemplo del tercer aspecto.

La unidad de retransmisión descifra el contenido cifrado como se entiende claramente a partir de los ejemplos descritos anteriormente del tercer aspecto. Por lo tanto, el descifrado se puede realizar separadamente del protocolo habitual de, por ejemplo, un servidor WWW o un navegador WWW, y se puede usar fácilmente un sistema WWW conocido. Dado que la unidad de retransmisión realiza el descifrado incluso cuando el usuario no realiza ninguna operación para descifrar el contenido cifrado, se proporciona al usuario una gran comodidad.

En los ejemplos descritos anteriormente del tercer aspecto, se puede proporcionar un servidor caché en el camino de comunicación entre el servidor de contenido 60 y el aparato de descifrado 30 (en ese caso, el contenido cifrado se almacena en caché).

La unidad de retransmisión puede almacenar en caché el contenido cifrado antes de que se descifre, a fin de proporcionar comodidad cuando un terminal cliente no está siempre conectado a la red de comunicación 5.

Para evitar la operación de caché de un navegador WWW para el contenido descifrado, se puede añadir una cabecera de control de caché HTTP que deshabilita el almacenamiento en caché a una respuesta al navegador WWW.

Cuando una pluralidad de usuarios usa el mismo terminal cliente, la unidad de retransmisión puede tener una función de autenticación. En ese caso, se pueden usar una autenticación básica y una autenticación implícita en HTTP para un navegador WWW, y una tabla de información de autenticación (ID de usuario y contraseñas) y una función de gestión para añadir, cambiar, y borrar información de autenticación se puede añadir a la unidad de retransmisión.

Se prefiere que los ejemplos descritos anteriormente del tercer aspecto sean aplicados a sistemas de entrega de contenidos. Dado que el cifrado de predicado no está basado en una información que dependa del receptor, se prefiere que el cifrado de predicado sea aplicado a un control de acceso del contenido que se puede navegar por personas sin especificar.

La Figura 82 muestra la estructura de datos intercambiados. El formato básico del mensaje entero es conforme, por ejemplo, a S/MIME (Extensiones de Correo de Internet Multipropósito Seguras). Una estructura de datos adecuada se da a los datos desde el marcador de posición de inicio de un mensaje cifrado hasta el marcador de posición final del mensaje cifrado en XML (el Lenguaje de Marcas Extensible) o algún otro lenguaje.

Los datos relacionados con el contenido cifrado se llaman bloque de cifrado. Los componentes del bloque de cifrado se describirán más abajo.

Un bloque de identificador de algoritmo especifica una información que identifica el algoritmo de cifrado de predicado

usado para cifrar la clave privada y el algoritmo de cifrado de clave privada usado para cifrar el contenido. Se puede especificar un identificador que indica el algoritmo o la versión de un algoritmo (por ejemplo, PE/Versión X + Camellia (Camellia es una marca comercial registrada).

Un bloque de firma digital especifica la firma digital. Se puede usar un algoritmo de firma conocido. Este elemento se puede omitir dependiendo de la aplicación.

Un bloque de información de parámetro público especifica una información que identifica el parámetro público usado. Se puede especificar un identificador que identifica el parámetro público o los datos del parámetro público.

Un campo de política especifica un identificador que identifica la política usada.

Un campo de esquema especifica un identificador que identifica el esquema usado o los datos del esquema.

Un campo de información de cifrado especifica los datos (información de cifrado) obtenidos cifrando, con el cifrado de predicado, la clave privada usada para cifrar el contenido.

Un nombre de fichero de contenido, un tipo de contenido, y un tamaño de fichero de contenido especifican el nombre de fichero del contenido, el tipo de datos (tal como texto o html) del contenido, y el tamaño de fichero del contenido, respectivamente.

Un campo de atributo y un campo de predicado especifican representaciones de cadenas de letras que indican el atributo y el predicado usados para el cifrado, que corresponden al campo de política, respectivamente. Estos elementos se pueden omitir según la aplicación.

El contenido cifrado generado cifrando el contenido se describe en los datos de cifrado.

La estructura de datos básica del contenido se describe con HTML (Lenguaje de Marcas de Hipertexto), y el bloque de cifrado se especifica mediante una sentencia de comentario en HTML.

El bloque de cifrado se da en una estructura de datos adecuada con XML (el Lenguaje de Marcas Extensible) u otros lenguajes.

Cuando el contenido cifrado se navega directamente con un navegador, no se visualizan sentencias de comentario, y se visualizan otras sentencias HTML. Por lo tanto, un mensaje que indica que los datos incluyen contenido cifrado o un mensaje de error para un fallo de descifrado se puede describir en las otras sentencias HTML.

En la descripción anterior, la estructura algebraica S es un campo finito. La estructura algebraica puede ser un anillo finito (anillo de restos enteros). Cuando un algoritmo de cifrado de predicado usa un producto interior, por ejemplo, la primera y segunda información de atributo y la primera y segunda información de predicado son vectores que tienen elementos de S como componentes.

Según el esquema de la estructura algebraica S, la clave pública B es un conjunto de elementos de un módulo V en S, la clave privada B* es un conjunto de elementos de un módulo V* dual del módulo V, y la clave de descifrado R es un elemento del módulo dual V*. Cuando la estructura algebraica S es un campo finito, el módulo V en el campo finito es un denominado espacio de vector en el campo finito. En ese caso, la unidad de cifrado realiza cálculos que incluyen una multiplicación escalar en la que los elementos de la clave pública B se multiplican por los componentes, usados como coeficientes, de la primera información de atributo o una multiplicación escalar en la que los elementos de la clave pública B se multiplican por los componentes, usados como coeficientes, de la primera información de predicado, para obtener una información de cifrado. La unidad de generación de clave realiza cálculos que incluyen una multiplicación escalar en la que los elementos de la clave privada B* se multiplican por los componentes, usados como coeficientes, de la segunda información de predicado o una multiplicación escalar en la que los elementos de la clave privada B* se multiplican por los componentes, usados como coeficientes, de la segunda información de atributo, para obtener la clave de descifrado R.

Las entidades hardware (el aparato cliente, el aparato de generación de clave, el aparato de registro, el aparato de gestión, el aparato de mantenimiento, el aparato de autenticación, y el servidor de contenido) incluidas en el sistema criptográfico incluyen una unidad de entrada conectable a un teclado o similar, una unidad de salida conectable a una unidad de visualización de cristal líquido o similar, una unidad de comunicación conectable a un aparato de comunicación (tal como un cable de comunicación) con el cual se permiten comunicaciones fuera de las entidades, una CPU (unidad de procesamiento central) (la cual se puede dotar con una memoria caché y un registro), memorias tales como una RAM y una ROM, un dispositivo almacenamiento externo (disco duro), y un canal principal que se conecta de manera que se pueden intercambiar datos entre la unidad de entrada, la unidad de salida, la unidad de comunicación, la CPU, la RAM, la ROM, y la unidad del almacenamiento externo. Si es necesario, las entidades hardware se pueden dotar con un aparato (unidad) que puede leer y escribir datos a y desde un medio de

almacenamiento tal como un CD ROM. Las entidades físicas dotadas con tales recursos hardware incluyen un ordenador de propósito general.

El dispositivo de almacenamiento externo de cada entidad hardware almacena un programa requerido para implementar las funciones precedentes y los datos requeridos en el procesamiento del programa (en lugar del dispositivo de almacenamiento externo, un dispositivo de almacenamiento solamente de lectura, es decir, una ROM, puede almacenar el programa, por ejemplo). Los datos obtenidos mediante el procesamiento del programa y similares se almacenan en una RAM o el dispositivo de almacenamiento externo, si es necesario. En las descripciones anteriores, los dispositivos de almacenamiento, tales como RAM y registros, que almacenan resultados de cálculos y las direcciones de las áreas de almacenamiento de los resultados se llaman sólo memorias.

En cada entidad hardware, el programa almacenado en el dispositivo de almacenamiento externo (o la ROM) y los datos requeridos para el procesamiento del programa se leen en una memoria, cuando se necesita, y se interpretan, ejecutan, o procesan por la CPU, según se requiera. Como resultado, la CPU implementa las funciones predeterminadas (tales como aquéllas de la unidad de cifrado, la unidad de descifrado, la unidad de generación de clave, la primera unidad de adquisición de información de lógica de predicado, la segunda unidad de adquisición de información de lógica de predicado, y la unidad de control).

Se requieren cálculos numéricos en teoría de números en algunos casos en operaciones detalladas de las entidades hardware descritas en cada realización. Dado que los cálculos numéricos en teoría de números se realizan de la misma forma que con una tecnología conocida, se omite una descripción detallada de los mismos, incluyendo un método de cálculo de los mismos. (Un software que es capaz de cálculos numéricos en teoría de números e indica el nivel técnico actual de los mismos incluye PARI/GP y KANT/KASH. Para PARI/GP, ver http://pari.math.u-bourdeaux.fr/, recuperado el 14 de abril de 2009. Para KANT/KASH, ver http://www.math.tu-berlin.de/algebra/, recuperado el 14 de abril de 2009). La siguiente referencia A describe los cálculos numéricos en teoría de números. Referencia A: H. Cohen, “A Course in Computational Algebraic Number Theory”, GTM 138, Springer-Verlag, 1993.

La presente invención no está limitada a las realizaciones descritas anteriormente, y se pueden hacer modificaciones adecuadas sin apartarse del alcance de la presente invención. Los procesos descritos en las realizaciones anteriores se pueden ejecutar no solamente secuencialmente en el tiempo según el orden de descripción sino también en paralelo o individualmente cuando sea necesario o según las capacidades de procesamiento de los aparatos que ejecutan los procesos.

Cuando las funciones de procesamiento de las entidades hardware descritas en las realizaciones anteriores se implementan por un ordenador, los detalles de procesamiento de las funciones que se deberían proporcionar por las entidades hardware se describen en un programa. Cuando el programa se ejecuta por un ordenador, las funciones de procesamiento de las entidades hardware se implementan en el ordenador.

El programa que contiene los detalles de procesamiento se puede grabar en un medio de almacenamiento legible por ordenador. El medio de almacenamiento legible por ordenador puede ser cualquier tipo de medio, tal como un dispositivo de almacenamiento magnético, un disco óptico, un medio de almacenamiento magneto óptico, y una memoria de semiconductores. Por ejemplo, un dispositivo de disco duro, un disco flexible, una cinta magnética, o similares se pueden usar como dispositivo de grabación magnética; un disco versátil digital (DVD), una memoria de acceso aleatorio de DVD (DVD-RAM), una memoria solamente de lectura de disco compacto (CD-ROM), un CD grabable o regrabable (CD-R/RW), o similares se pueden usar como disco óptico; un disco magneto óptico o similar se puede usar como un medio de almacenamiento magneto óptico; y una memoria solamente de lectura borrable y programable electrónicamente (EEPROM) o similar se puede usar como memoria de semiconductores.

El programa se distribuye mediante venta, transferencia, o préstamo de un medio de grabación portátil tal como un DVD o un CD ROM con el programa grabado en él, por ejemplo. El programa también puede ser distribuido almacenando el programa en una unidad de almacenamiento de un ordenador servidor y transfiriendo el programa desde el ordenador servidor a otro ordenador a través de la red.

Un ordenador que ejecuta este tipo de programa primero almacena el programa grabado en el medio de grabación portátil o el programa transferido desde el ordenador servidor en su unidad de almacenamiento. Entonces, el ordenador lee el programa almacenado en su unidad de almacenamiento y ejecuta el procesamiento según el programa leído. De una forma de ejecución del programa diferente, el ordenador puede leer el programa directamente del medio de grabación portátil y ejecutar el procesamiento según el programa, o el ordenador puede ejecutar el procesamiento según el programa cada vez que el ordenador recibe el programa transferido desde el ordenador servidor. Alternativamente, el procesamiento se puede ejecutar mediante un denominado servicio de proveedor de servicios de aplicaciones (ASP), en el cual se implementa la función de procesamientos sólo dando una instrucción de ejecución de programa y obteniendo resultados sin transferir el programa desde el ordenador servidor al ordenador. El programa de esta forma incluye una información que se proporciona para uso en el procesamiento por un ordenador y se trata en consecuencia como un programa (algo que no es una instrucción directa al ordenador sino que son datos o similares que tienen características que determinan el procesamiento

ejecutado por el ordenador).

En la descripción dada anteriormente, las entidades hardware se implementan ejecutando el programa predeterminado en el ordenador, pero al menos una parte del procesamiento se puede implementar mediante hardware.

<<Suplemento>>
Un cifrado de predicado que usa productos internos se describirá más abajo en detalle, el cual es un ejemplo de cifrado de predicado que se puede usar en la presente invención. Los números de expresión se asignan nuevamente más abajo. Se debería señalar que la misma redacción y símbolos que aquéllos usados en las descripciones anteriores pueden tener diferentes significados en la siguiente descripción por el bien de la explicación.

[Definiciones]
Se definirán primero los términos y símbolos a ser usados en la siguiente descripción.

Matriz: una disposición rectangular de elementos de un conjunto en el cual se define un cálculo. No solamente los elementos de un anillo sino también los elementos de un grupo pueden formar una matriz.
$(\cdot)^T$: Matriz traspuesta de $\cdot$
$(\cdot)^{-1}$: Matriz inversa de $\cdot$
$\wedge$: AND Lógica
$\vee$: OR Lógica
Z: Conjunto de enteros
k: Parámetro de seguridad ($k \in Z, k > 0$)
{0, 1}*: Secuencia binaria que tiene una longitud de bit deseada. Un ejemplo es una secuencia formada por los enteros 0 y 1. No obstante, {0, 1}* no está limitada a secuencias formadas por los enteros 0 y 1. {0, 1}* es un campo finito de orden 2 o su campo extendido.
$\{0, 1\}^{\xi}$: Secuencia binaria que tiene una longitud de bit ξ ($\xi \in Z$, $\xi > 0$). Un ejemplo es una secuencia formada por los enteros 0 y 1. No obstante, $\{0, 1\}^{\xi}$ no está limitada a secuencias formadas por los enteros 0 y 1. $\{0, 1\}^{\xi}$ es un campo finito de orden 2 (cuando $\xi = 1$) o su campo extendido (cuando $\xi > 1$).
(+): Operador OR exclusivo entre secuencias binarias. Por ejemplo, se satisface lo siguiente: 10110011 (+) 11100001 = 01010010.
F_q: campo finito de orden q, donde q es un entero igual o mayor que 1. Por ejemplo, el orden q es un número primo de una potencia de un número primo. En otras palabras, el campo finito F_q es un campo primo o un campo extendido del campo primo, por ejemplo. Cuando el campo finito F_q es un campo primo, se pueden realizar fácilmente los cálculos restantes para el módulo q, por ejemplo. Cuando el campo finito F_q es un campo extendido, se pueden realizar fácilmente los cálculos restantes para el modulo de un polinomio irreducible, por ejemplo. Un método específico para configurar un campo finito F_q se describe, por ejemplo, en la bibliografía de referencia 1, “ISO/IEC 18033-2: Information technology-Security techniques-Encryption algorithms-Part 2: Asymmetric ciphers”.
0_F: Elemento unidad aditivo del campo finito F_q
1_F: Elemento unidad multiplicativo del campo finito F_q
δ (i,j): Función delta de Kronecker. Cuando i = j, δ (i,j) = 1_F. Cuando $i \neq j$, δ (i,j) = 0_F.
E: Curva elíptica definida en el campo finito F_q. Se define como un punto especial O llamado el punto de infinito más un conjunto de puntos (x, y) que satisface x, y, $\in F_q$ y la ecuación de Weierstrass en un sistema de coordenadas afín

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

donde $a_1, a_2, a_3, a_4, a_6 \in F_q$. Se puede definir una operación binaria + llamada de adición elíptica para cualesquiera dos puntos en la curva elíptica E, y se puede definir una operación unaria - llamada inversa elíptica para cualquier punto en la curva elíptica E. Es bien conocido que un conjunto finito de puntos racionales en la curva elíptica E forma un grupo con respecto a la adición elíptica. También es bien conocido que una operación llamada multiplicación escalar elíptica se puede definir con la adición elíptica. Un método de operación específico de operaciones elípticas tal como la adición elíptica en un ordenador es bien conocido también. (Por ejemplo, ver la bibliografía de referencia 2, “RFC 5091: Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems”, y la bibliografía de referencia 3, Ian F. Blake, Gadiel Seroussi, y Nigel P. Smart, “Elliptic Curves in Cryptography”, Pearson Education, ISBN 4-89471-431-0).

Un conjunto finito de puntos racionales en la curva elíptica E tiene un subgrupo de orden p ($p \geq 1$). Cuando el número de elementos en un conjunto finito de puntos racionales en la curva elíptica E es #E y p es un número primo grande que puede dividir #E sin un resto, por ejemplo, un conjunto finito E[p] de p puntos divididos por igual en la curva elíptica E forma un subgrupo de un conjunto finito de puntos racionales en la curva elíptica E. Los p puntos divididos por igual en la curva elíptica E son puntos A en la curva elíptica E que satisfacen la multiplicación escalar elíptica pA

= 0.

G_1, G_2, G_T: Grupos cíclicos de orden q. Ejemplos de los grupos cíclicos G_1 y G_2 incluyen el conjunto finito E[p] de p puntos divididos por igual en la curva elíptica E y subgrupos de los mismos. G_1 puede ser igual a G_2, o G_1 puede no ser igual a G_2. Ejemplos del grupo cíclico G_T incluyen un conjunto finito que constituye un campo extendido del campo finito F_q. Un ejemplo específico del mismo es un conjunto finito de la raíz de orden p de 1 en el cierre algebraico del campo finito F_q.

Operaciones definidas en los grupos cíclicos G_1 y G_2 se expresan como sumas, y una operación definida en el grupo cíclico G_T se expresa como una multiplicación. Más específicamente, $\chi \cdot \Omega \in G_1$ para $\chi \in F_q$ y $\Omega \in G_1$ significa que la operación definida en el grupo cíclico G_1 se aplica a $\Omega \in G_1$ χ veces, y $\Omega_1 + \Omega_2 \in G_1$ para $\Omega_1, \Omega_2 \in G_1$ significa que la operación definida en el grupo cíclico G_1 se aplica a $\Omega_1 \in G_1$ y $\Omega_2 \in G_1$. De la misma forma, $\chi \cdot \Omega \in G_2$ para $\chi \in F_q$ y $\Omega \in G_2$ significa que la operación definida en el grupo cíclico G_2 se aplica a $\Omega \in G_2$ χ veces, y $\Omega_1 + \Omega_2 \in G_2$ para $\Omega_1, \Omega_2 \in G_2$ significa que la operación definida en el grupo cíclico G_2 se aplica a $\Omega_1 \in G_2$ y $\Omega_2 \in G_2$. Al contrario, Ω $\chi \in G_T$ para $\chi \in F_q$ y $\Omega \in G_T$ significa que la operación definida en el grupo cíclico G_T se aplica a $\Omega \in G_T$ χ veces, y $\Omega_1 \cdot \Omega_2 \in G_T$ para $\Omega_1, \Omega_2 \in G_T$ significa que la operación definida en el grupo cíclico G_T se aplica a $\Omega_1 \in G_T$ y $\Omega_2 \in G_T$.
G_1^{n+1}: Producto directo de (n +1) grupos críticos G_1 ($n \geq 1$)
G_2^{n+1}: Producto directo de (n +1) grupos críticos G_2
g_1, g_2, g_T: Elementos de generación de los grupos cíclicos G_1, G_2, G_T
V: Espacio de vector (n + 1) dimensional formado del producto directo de los (n + 1) grupos cíclicos G_1
V*: Espacio de vector (n + 1) dimensional formado del producto directo de los (n + 1) grupos cíclicos G_2
e: Función (función bilineal) para calcular un mapa bilineal no degenerado que correlaciona el producto directo G_1^{n+1} x G_2^{n+1} del producto directo G_1^{n+1} y el producto directo G_2^{n+1} al grupo cíclico G_T. La función bilineal e recibe (n + 1) elementos γ_L (L = 1, …, n + 1) ($n \geq 1$) del grupo cíclico G_1 y (n + 1) elementos γ_L^* (L = 1, …, n + 1) del grupo cíclico G_2 y saca un elemento del grupo cíclico G_T.

$$e: G_1^{n+1} \times G_2^{n+1} \rightarrow G_T \qquad (2)$$

La función bilineal e satisface las siguientes características:

- Bilinealidad: Las siguiente relación se satisface para todo $\Gamma_1 \in G_1^{n+1}$, $\Gamma_2 \in G_2^{n+1}$, y ν y $\kappa \in F_q$

$$e(\nu \cdot \Gamma_1, \kappa \cdot \Gamma_2) = e(\Gamma_1, \Gamma_2)^{\nu \cdot \kappa} \qquad (3)$$

- No degeneración: Esta función no correlaciona todo

$$\Gamma_1 \in G_1^{n+1}, \Gamma_2 \in G_2^{n+1} \qquad (4)$$

sobre el elemento unidad del grupo cíclico G_T.

- Computabilidad: Existe un algoritmo para calcular eficientemente e(Γ_1, Γ_2) para todo $\Gamma_1 \in G_1^{n+1}$, $\Gamma_2 \in G_2^{n+1}$.

La siguiente función para calcular un mapa bilineal no degenerado que correlaciona el producto directo G_1 x G_2 del grupo cíclico G_1 y el grupo cíclico G_2 al grupo cíclico G_T constituye la función bilineal e.

$$\text{Par:} \quad G_1 \times G_2 \rightarrow G_T \qquad (5)$$

La función bilineal e recibe un vector (n + 1) dimensional (γ_1, …, γ_{n+1}) formado de (n + 1) elementos γ_L (L = 1, …, n + 1) del grupo cíclico G_1 y un vector (n + 1) dimensional (γ_1^*, …, γ_{n+1}^*) formado de (n + 1) elementos γ_L^* (L = 1, …, n + 1) del grupo cíclico G_2 y saca un elemento del grupo cíclico G_T.

$$e = \prod_{L-1}^{n+1} \text{Par}(\gamma_L, \gamma_L^*) \qquad (6)$$

La función bilineal Par recibe un elemento del grupo cíclico G_1 y un elemento del grupo cíclico G_2 y saca un elemento del grupo cíclico G_T, y satisface las siguientes características:

- Bilinealidad: La siguiente relación se satisface para todo $\Omega_1 \in G_1$, $\Omega_2 \in G_2$, y ν , $\kappa \in F_q$

$$\text{Par}(\nu \cdot \Omega_1, \kappa\ \Omega_2) = \text{Par}(\Omega_1, \Omega_2)^{\nu \cdot \kappa} \quad (7)$$

- No degeneración: Esta función no correlaciona todo

$$\Omega_1 \in G_1 \text{ y } \Omega_2 \in G_2 \quad (8)$$

sobre el elemento unidad del grupo cíclico G_T.

- Computabilidad: Existe un algoritmo para calcular eficientemente Par(Ω_1, Ω_2) para todo $\Omega_1 \in G_1$, $\Omega_2 \in G_2$.

Un ejemplo específico de la función bilineal Par es una función para realizar una operación de emparejamiento tal como un emparejamiento de Weil o un emparejamiento de Tate. (Ver la bibliografía de referencia 4, Alfred. J. Menezes, "Elliptic Curve Public Key Cryptosystems", Kluwer Academic Publishers, ISBN 0-7923-9368-6, páginas 61-81, por ejemplo). Una función de emparejamiento modificada e(Ω_1 , phi(Ω_2)) ($\Omega_1 \in G_1$, $\Omega_2 \in G_2$) obtenida combinando una función para realizar una operación de emparejamiento, tal como un emparejamiento de Tate, y una función predeterminada phi según el tipo de la curva elíptica E se pueden usar como la función bilineal Par (ver la bibliografía de referencia 2, por ejemplo). Como el algoritmo para realizar una operación de emparejamiento en un ordenador, se puede usar el algoritmo de Miller (ver la bibliografía de referencia 5, V. S. Miller, "Short Programs for Functions on Curves", 1986, http://crypto.stanford.edu/miller/miller.pdf) o algún otro algoritmo conocido. Los métodos para configurar un grupo cíclico y una curva elíptica usados para realizar eficientemente una operación de emparejamiento han sido conocidos. (Por ejemplo, ver la bibliografía de referencia 2, descrita anteriormente, la bibliografía referencia 6, A. Miyaji, M. Nakabayashi, y S. Takano, "New Explicit Conditions of Elliptic Curve Traces for FR Reduction", IEICE Trans. Fundamentals, Vol. E84-A, Nº 5, páginas 1234-1243, mayo de 2001, la bibliografía referencia 7, P. S. L. M. Barreto, B. Lynn, M. Scott, "Constructing Elliptic Curves with Prescribed Embedding Degrees", Actas SCN '2002, LNCS 2576, páginas 257-267, Springer-Verlag. 2003, y la bibliografía referencia 8, R. Dupont, A. Enge, F. Morain, "Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields", http//eprint.iacr.org/2002/094/.

a_i (i = 1, …, n + 1): vector de base (n + 1) dimensional que tiene (n + 1) elementos del grupo cíclico G_1 como elementos. Un ejemplo del vector de base a_i es un vector de base (n + 1) dimensional que tiene $\kappa_1 \cdot g_1 \in G_1$ como un elemento i-dimensional y el elemento unidad (expresado como "0" en la expresión aditiva) del grupo cíclico G_1 como los n elementos restantes. En ese caso, cada elemento del vector de base (n + 1) dimensional a_i (i = 1, …, n + 1) se pueden enumerar como sigue:

$$a_1 = (\kappa_1 \cdot g_1, 0, 0, \ldots, 0)$$

$$a_2 = (0, \kappa_1 \cdot g_1, 0, \ldots, 0) \quad (9)$$

……

$$a_{n+1} = (0, 0, 0, \ldots, \kappa_1 \cdot g_1)$$

Aquí, κ_1 es una constante formada de los elementos del campo finito F_q distintos del elemento unidad aditivo 0_F. Un ejemplo de $\kappa_1 \in F_q$ es $\kappa_1 = 1_F$. El vector de base a_i es una base ortogonal. Cada vector (n + 1) dimensional que tiene (n + 1) elementos del grupo cíclico G_1 como elementos se expresa por una suma lineal de vectores de base (n + 1) dimensionales a_i (i = 1, …, n + 1). Por lo tanto, los vectores de base (n + 1) dimensionales a_i extienden el espacio de vector V, descrito anteriormente.

a_i^* (i = 1, …, n + 1): vector de base (n + 1) dimensional que tiene (n + 1) elementos del grupo cíclico G_2 como elementos. Un ejemplo del vector de base a_i^* es un vector de base (n + 1) dimensional que tiene $\kappa_2 \cdot g_2 \in G_2$ como un elemento i-dimensional y el elemento unidad (expresado como "0" en la expresión aditiva) del grupo cíclico G_2 como los n elementos restantes. En ese caso, cada elemento del vector de base (n + 1) dimensional a_i^* (i = 1, …, n + 1) se pueden enumerar como sigue:

$$a_1^* = (\kappa_2 \cdot g_2, 0, 0, \ldots, 0)$$

$$a_2^* = (0, \kappa_2 \cdot g_2, 0, \ldots, 0) \quad (10)$$

……

$$a_{n+1}^* = (0, 0, 0, \ldots, \kappa_2 \cdot g_2)$$

Aquí, κ_2 es una constante formada de los elementos del campo finito F_q distintos del elemento unidad aditivo 0_F. Un ejemplo de $\kappa_2 \in F_q$ es $\kappa_2 = 1_F$. El vector de base a_i^* es una base ortogonal. Cada vector (n + 1) dimensional que tiene (n + 1) elementos del grupo cíclico G_2 como elementos se expresa por una suma lineal de vectores de base (n + 1) dimensionales a_i^* (i = 1, …, n + 1). Por lo tanto, los vectores de base (n + 1) dimensionales a_i^* extienden el espacio de vector V*, descrito anteriormente.

El vector de base a_i y el vector de base a_i^* satisfacen la siguiente expresión para los elementos $\tau = \kappa_1 \cdot \kappa_2$ del campo finito F_q distinto de 0_F.

$$e(a_i, a_j^*) = g_T^{\tau\delta_{(i,j)}} \quad (11)$$

Cuando i = j, se satisface la siguiente expresión a partir de las Expresiones (6) y (7).

$$\begin{aligned} e(a_i, a_j^*) &= Par(\kappa_1 \cdot g_1, \kappa_2 \cdot g_2) \cdot Par(0, 0) \cdot \ldots \cdot Par(0, 0) \\ &= Par(g_1, g_2)^{\kappa_1 \kappa_2} \cdot Par(g_1, g_2)^{0'0} \cdot \ldots \cdot Par(g_1, g_2)^{0'0} \\ &= Par(g_1, g_2)^{\kappa_1 \kappa_2} = g_T^{\tau} \end{aligned}$$

Cuando $i \neq j$, $e(a_i, a_j^*)$ no incluye $Par(\kappa_1 \cdot g_1, \kappa_2 \cdot g_2)$ y es el producto de $Par(\kappa_1 \cdot g_1, 0)$, $Par(0, \kappa_2 \cdot g_2)$ y $Par(0, 0)$. Además, se satisface la siguiente expresión a partir de la Expresión (7).

$$Par(g_1, 0) = Par(0, g_2) = Par(g_1, g_2)^{0'0}$$

Por lo tanto, cuando $i \neq j$, se satisface la siguiente expresión.

$$e(a_i, a_j^*) = e(g_1, g_2)^0 = g_T^0$$

Especialmente cuando $\tau = \kappa_1 \cdot \kappa_2 = 1_F$ (por ejemplo, $\kappa_1 = \kappa_2 = 1_F$), se satisface la siguiente expresión.

$$e(a_i, a_j^*) = g_T^{\delta_{(i,j)}} \quad (12)$$

Aquí, g_T^0 es el elemento unidad del grupo cíclico G_T, y $g_T^1 = g_T$ es un elemento de generación del grupo cíclico G_T. En ese caso, el vector de base a_i y el vector de base a_i^* son una base ortogonal normal dual, y el espacio de vector V y el espacio de vector V* son un espacio de vector dual que constituye una correspondencia bilineal (espacio de vector de emparejamiento dual (DPVS)).

A: Una matriz de (n + 1) filas por (n + 1) columnas que tiene el vector de base a_i (i = 1, …, n + 1) como elementos. Cuando el vector de base a_i (i = 1, …, n + 1) se expresa por la Expresión (9), por ejemplo, la matriz A es como sigue:

$$A = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} \kappa_1 \cdot g_1 & 0 & \cdots & 0 \\ 0 & \kappa_1 \cdot g_1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_1 \cdot g_1 \end{pmatrix} \quad \ldots(13)$$

A*: Una matriz de (n + 1) filas por (n + 1) columnas que tiene el vector de base a_i^* (i = 1, …, n + 1) como elementos. Cuando el vector de base a_i^* (i = 1, …, n + 1) se expresa por la Expresión (10), por ejemplo, la matriz A* es como sigue:

$$A^* = \begin{pmatrix} a_1^* \\ a_2^* \\ \vdots \\ a_{n+1}^* \end{pmatrix} = \begin{pmatrix} \kappa_2 \cdot g_2 & 0 & \cdots & 0 \\ 0 & \kappa_2 \cdot g_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_2 \cdot g_2 \end{pmatrix} \quad \ldots(14)$$

X: Una matriz de (n + 1) filas por (n + 1) columnas que tiene elementos del campo finito F_q como elementos. La matriz X se usa para aplicar una conversión de coordenadas al vector de base a_i. Cuando el elemento situado en la fila de orden i y la columna de orden j en la matriz X, $\chi_{i,j} \in F_q$, la matriz X es como sigue:

$$X = \begin{pmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,n+1} \\ \chi_{2,1} & \chi_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1} & \chi_{n+1,2} & \cdots & \chi_{n+1,n+1} \end{pmatrix} \quad \text{...(15)}$$

Aquí, cada elemento $\chi_{i,j}$ de la matriz X se llama coeficiente de conversión.

X*: La matriz traspuesta de la matriz inversa de la matriz X. $X^* = (X^{-1})^T$. La matriz X* se usa para aplicar una conversión de coordenadas al vector de base a_i^*. Cuando el elemento situado en la fila de orden i y la columna de orden j en la matriz X*, $\chi_{i,j}^*$, $\in F_q$, la matriz X* es como sigue:

$$X^* = \begin{pmatrix} \chi_{1,1}^* & \chi_{1,2}^* & \cdots & \chi_{1,n+1}^* \\ \chi_{2,1}^* & \chi_{2,2}^* & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1}^* & \chi_{n+1,2}^* & \cdots & \chi_{n+1,n+1}^* \end{pmatrix} \quad \text{...(16)}$$

Aquí, cada elemento $\chi_{i,j}^*$ de la matriz X* se llama coeficiente de conversión.

En ese caso, cuando una matriz unidad de (n + 1) filas por (n + 1) columnas se llama I, $X \cdot (X^*)^T = I$. En otras palabras, para la matriz unidad mostrada más abajo,

$$I = \begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix} \quad \text{...(17)}$$

se satisface la siguiente expresión.

$$\begin{pmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,n+1} \\ \chi_{2,1} & \chi_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1} & \chi_{n+1,2} & \cdots & \chi_{n+1,n+1} \end{pmatrix} \cdot \begin{pmatrix} \chi_{1,1}^* & \chi_{2,1}^* & \cdots & \chi_{n+1,1}^* \\ \chi_{1,2}^* & \chi_{2,2}^* & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{1,n+1}^* & \chi_{2,n+1}^* & \cdots & \chi_{n+1,n+1}^* \end{pmatrix} \quad \text{...(18)}$$

$$= \begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix}$$

Aquí, los vectores (n + 1) dimensionales se definirán más abajo.

$$\vec{\chi_i} = (\chi_{i,1}, \ldots, \chi_{i,n+1}) \quad \text{(19)}$$

$$\vec{\chi_j} = (\chi_{j,1}^*, \ldots, \chi_{j,n+1}^*) \quad \text{(20)}$$

El producto interior de los vectores (n + 1) dimensionales $\vec{\chi_i}$ y $\vec{\chi_j}^*$ satisface la siguiente expresión a partir de la Expresión (18).

$$\vec{\chi_i} \cdot \vec{\chi_j}^{*} = \delta(i, j) \qquad (21)$$

b_i: vector de base (n + 1) dimensional que tiene (n + 1) elementos del grupo cíclico G_1 como elementos. El vector de base b_i se obtiene aplicando conversión de coordenadas a a_i (i = 1, …, n + 1) usando la matriz X. Específicamente, el vector de base b_i se obtiene por el siguiente cálculo

$$b_i = \sum_{j=1}^{n+1} \chi_{i,j} \cdot a_j \qquad (22)$$

Cuando el vector de base a_j (j = 1, …, n + 1) se expresa por la Expresión (9), cada elemento del vector de base b_i se muestra más abajo.

$$b_i = (\chi_{i,1} \cdot \kappa_1 \cdot g_1, \chi_{i,2} \cdot \kappa_1 \cdot g_1, \ldots, \chi_{i,n+1} \cdot \kappa_1 \cdot g_1) \qquad (23)$$

Cada vector (n + 1) dimensional que tiene (n + 1) elementos del grupo cíclico G_1 como elementos se expresa por una suma lineal de los vectores de base (n + 1) dimensionales b_i (i = 1, …, n + 1). Por lo tanto, los vectores de base (n + 1) dimensionales b_i expanden el espacio de vector V, descrito anteriormente.

b_i^*: vector de base (n + 1) dimensional que tiene (n + 1) elementos del grupo cíclico G_2 como elementos. El vector de base b_i^* se obtiene aplicando conversión de coordenadas a a_i^* (i = 1, …, n + 1) usando la matriz X*. Específicamente, el vector de base b_i^* se obtiene por el siguiente cálculo

$$b_i^* = \sum_{j=1}^{n+1} \chi_{i,j}^* \cdot a_j^* \qquad (24)$$

Cuando el vector de base a_j (j = 1, …, n + 1) se expresa por la Expresión (10), cada elemento del vector de base b_i^* se muestra más abajo.

$$b_i^* = (\chi_{i,1}^* \cdot \kappa_2 \cdot g_2, \chi_{i,2} \cdot \kappa_2 \cdot g_2, \ldots, \chi_{i,n+1}^* \cdot \kappa_2 \cdot g_2) \qquad (25)$$

Cada vector (n + 1) dimensional que tiene (n + 1) elementos del grupo cíclico G_2 como elementos se expresa por una suma lineal de los vectores de base (n + 1) dimensionales b_i^* (i = 1, …, n + 1). Por lo tanto, los vectores de base (n + 1) dimensionales b_i^* expanden el espacio de vector V*, descrito anteriormente.

El vector de base b_i y el vector de base b_i^* satisfacen la siguiente expresión para los elementos $\tau = \kappa_1 \cdot \kappa_2$ del campo finito F_q distinto de 0_F:

$$e(b_i, b_j^*) = g_T^{\tau\delta_{(i,j)}} \qquad (26)$$

La siguiente expresión se satisface a partir de las Expresiones (6), (21), (23), y (25).

$$\begin{aligned} e(b_i, b_j^*) &= \prod_{L=1}^{n+1} \mathbf{Par}(\chi_{i,L} \cdot \kappa_1 \cdot g_1, \chi_{j,L}^* \cdot \kappa_2 \cdot g_2) \\ &= \mathbf{Par}(\chi_{i,1} \cdot \kappa_1 \cdot g_1, \chi_{j,1}^* \cdot \kappa_2 \cdot g_2) \cdot \ldots \cdot (\chi_{i,n} \cdot \kappa_1 \cdot g_1, \chi_{j,n}^* \cdot \kappa_2 \cdot g_2) \\ &\quad \times \mathbf{Par}(\chi_{j,n+1} \cdot \kappa_1 \cdot g_1, \chi_{j,n+1}^* \cdot \kappa_2 \cdot g_2) \\ &= \mathbf{Par}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,1} \cdot \chi_{j,1}^*} \cdot \ldots \cdot \mathbf{Par}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,2} \cdot \chi_{j,2}^*} \\ &\quad \times \mathbf{Par}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,n+1} \cdot \chi_{j,n+1}^*} \\ &= \mathbf{Par}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 (\chi_{i,1} \cdot \chi_{j,1}^* + \chi_{i,2} \cdot \chi_{j,2}^* + \ldots + \chi_{i,n+1} \cdot \chi_{j,n+1}^*)} \\ &= \mathbf{Par}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \vec{\chi_i} \cdot \vec{\chi_j}^*} \\ &= \mathbf{Par}(g_1, g_2)^{\tau \cdot \delta(i,j)} = g_T^{\tau \cdot \delta(i,j)} \end{aligned}$$

Especialmente cuando $\tau = \kappa_1 \cdot \kappa_2 = 1_F$ (por ejemplo, $\kappa_1 = \kappa_2 = 1_F$), se satisface la siguiente expresión.

$$e(b_i, b_j^*) = g_T^{\delta_{(i,j)}} \qquad (27)$$

En ese caso, el vector de base b_i y el vector de base b_i^* son la base ortogonal normal dual de un espacio de vector de emparejamiento dual (el espacio de vector V y el espacio de vector V*).

Siempre que se satisface la Expresión (26), se pueden usar los vectores de base a_i y a_i^* distintos de aquéllos mostrados en las Expresiones (9) y (10) como ejemplos, y los vectores de base b_i y b_i^* distintos de aquéllos mostrados en las Expresiones (22) y (24) como ejemplos.

B: Una matriz de (n + 1) filas por (n + 1) columnas que tiene el vector de base b_i (i = 1, …, n + 1) como elementos. Se satisface B = X·A. Cuando el vector de base b_i se expresa por la Expresión (23), por ejemplo, la matriz B es como sigue:

$$B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} \chi_{1,1} \cdot \kappa_1 \cdot g_1 & \chi_{1,2} \cdot \kappa_1 \cdot g_1 & \cdots & \chi_{1,n+1} \cdot \kappa_1 \cdot g_1 \\ \chi_{2,1} \cdot \kappa_1 \cdot g_1 & \chi_{2,2} \cdot \kappa_1 \cdot g_1 & & \vdots \\ \vdots & & \ddots & \chi_{n,n+1} \cdot \kappa_1 \cdot g_1 \\ \chi_{n+1,1} \cdot \kappa_1 \cdot g_1 & \cdots & \chi_{n+1,n} \cdot \kappa_1 \cdot g_1 & \chi_{n+1,n+1} \cdot \kappa_1 \cdot g_1 \end{pmatrix} \qquad \text{...(28)}$$

B*: Una matriz de (n + 1) filas por (n + 1) columnas que tiene el vector de base b_i^* (i = 1, …, n + 1) como elementos. Se satisface B* = X*·A*. Cuando el vector de base b_i^* (i = 1, …, n + 1) se expresa por la Expresión (25), por ejemplo, la matriz B* es como sigue:

$$B^* = \begin{pmatrix} b_1^* \\ b_2^* \\ \vdots \\ b_{n+1}^* \end{pmatrix} = \begin{pmatrix} \chi_{1,1}^* \cdot \kappa_2 \cdot g_2 & \chi_{1,2}^* \cdot \kappa_2 \cdot g_2 & \cdots & \chi_{1,n+1}^* \cdot \kappa_2 \cdot g_2 \\ \chi_{2,1}^* \cdot \kappa_2 \cdot g_2 & \chi_{2,2}^* \cdot \kappa_2 \cdot g_2 & & \vdots \\ \vdots & & \ddots & \chi_{n,n+1}^* \cdot \kappa_2 \cdot g_2 \\ \chi_{n+1,1}^* \cdot \kappa_2 \cdot g_2 & \cdots & \chi_{n+1,n}^* \cdot \kappa_2 \cdot g_2 & \chi_{n+1,n+1}^* \cdot \kappa_2 \cdot g_2 \end{pmatrix} \qquad (29)$$

$\vec{w}$: Un vector n dimensional que tiene elementos del campo finito F_q como elementos.

$$\vec{w} = (w_1, \ldots, w_n) \in F_q^n \qquad (30)$$

w_μ: El elemento de orden μ (μ = 1, …, n) del vector n dimensional.

$\vec{v}$: Un vector n dimensional que tiene elementos del campo finito F_q como elementos.

$$\vec{v} = (v_1, \ldots, v_n) \in F_q^n \qquad (31)$$

v_μ: El elemento de orden μ (μ = 1, …, n) del vector n dimensional.

Función sin colisiones: Una función h que satisface la siguiente condición con respecto a un parámetro de seguridad suficientemente grande k, o una función considerada como que sirve como tal.

$$\Pr[A(h) = (x, y) \mid h(x) = h(y) \wedge x \neq y] < \varepsilon(k) \qquad (32)$$

Aquí Pr[·] es la probabilidad del evento [·]; A(h) es un algoritmo de tiempo de polinomio de probabilidad para calcular x e y ($x \neq y$) que satisface h(x) = h(y) para una función h; y ε (k) es un polinomio para el parámetro de seguridad k. Una función sin colisiones ejemplo es una función de cálculo de claves tal como la función de cálculo de claves

criptográficas descrita en la bibliografía de referencia 1.

Función de inyección: Una función por la cual cada elemento que pertenece a una gama de valores se expresa como la imagen de un elemento solamente en la gama de definición, o una función considerada como tal. Una función de inyección ejemplo es una función de cálculo de claves tal como la función de derivación de claves (KDF) descrita en la bibliografía de referencia 1.

Función pseudo aleatoria: Una función que pertenece a un subconjunto ϕ_ζ cuando un algoritmo de tiempo de polinomio de probabilidad no puede distinguir entre el subconjunto ϕ_χ y su conjunto entero Φ_ζ, o una función considerada como tal. El conjunto Φ_ζ es un conjunto de todas las funciones que correlacionan un elemento de un conjunto $\{0, 1\}^\xi$ a un elemento del conjunto $\{0, 1\}^\xi$. Un ejemplo de función pseudo aleatoria es una función de cálculo de claves tal como aquélla descrita anteriormente.

H_1: Una función sin colisión que recibe dos secuencias binarias $(\omega_1, \omega_2) \in \{0, 1\}^k$ x $\{0, 1\}^*$ y saca dos elementos $(\psi_1, \psi_2) \in F_q$ x F_q del campo finito F_q.

$$H_1: \quad \{0, 1\}^k \text{ x } \{0, 1\}^* \rightarrow F_q \text{ x } F_q \qquad (33)$$

Un ejemplo de la función H_1 es una función que recibe los bits conectados $\omega_1 \| \omega_2$ de ω_1 y ω_2, realiza cálculos con una función de cálculo de claves tal como la función de cálculo de claves criptográfica descrita en la bibliografía de referencia 1, una función de conversión de secuencia binaria a entero (conversión de cadena de octetos/entero), y una función de conversión de secuencia binaria a elemento de campo finito (conversión de cadena de octetos y entero/campo finito), y saca dos elementos $(\psi_1, \psi_2) \in F_q$ x F_q del campo finito F_q. Se prefiere que la función H_1 sea una función pseudo aleatoria.

H_2: Una función sin colisión que recibe un elemento del grupo cíclico G_T y una secuencia binaria $(\xi, \omega_2) \in G_T$ x $\{0, 1\}^*$ y saca un elemento $\psi \in F_q$ del campo finito F_q.

$$H_2: \quad G_T \text{ x } \{0, 1\}^* \rightarrow F_q \qquad (34)$$

Un ejemplo de la función H_2 es una función que recibe un elemento $\xi \in G_T$ del grupo cíclico G_T y una secuencia binaria $\omega_2 \in \{0, 1\}^*$, introduce el elemento $\xi \in G_T$ del grupo cíclico G_T a la función de conversión de elemento de campo finito a secuencia binaria (conversión de cadena de octetos y entero/campo finito) descrita en la bibliografía de referencia 1 para obtener una secuencia binaria, aplica una función de cálculo de claves tal como la función de cálculo de claves criptográficas descrita en la bibliografía de referencia 1 a los bits conectados de la secuencia binaria y la secuencia binaria $\omega_2 \in \{0, 1\}^*$, realiza una función de conversión de secuencia binaria a elemento de campo finito (conversión de cadena de octetos y entero/campo finito), y saca un elemento $\psi \in F_q$ del campo finito F_q. Se prefiere desde un punto de vista de seguridad que la función H_2 sea una función pseudo aleatoria.

R: Una función de inyección que recibe un elemento $\xi \in G_T$ del grupo cíclico G_T y saca una secuencia binaria $\omega \in \{0, 1\}^k$.

$$R: \quad G_T \rightarrow \{0, 1\}^* \qquad (35)$$

Un ejemplo de la función de inyección R es una función que recibe un elemento $\xi \in G_T$ del grupo cíclico G_T, realiza cálculos con la función de conversión de elemento de campo finito a secuencia binaria (conversión de cadena de octetos y entero/campo finito) y entonces con una función de cálculo de claves tal como la KDF (función de derivación de clave) descrita en la bibliografía de referencia 1, y saca una secuencia binaria $\omega \in \{0, 1\}^k$. Desde un punto de vista de seguridad, se prefiere que la función R sea una función sin colisión, y es más preferido que la función R sea una función pseudo aleatoria.

Enc: Una función de cifrado de clave privada que indica un proceso de cifrado de un sistema criptográfico de clave privada. Sistemas criptográficos de clave privada ejemplo son Camellia y AES.

$Enc_k(M)$: Texto cifrado obtenido cifrando un texto plano M mediante la función de cifrado de clave privada Enc con el uso de una clave común K.

Dec: Una función de descifrado de clave privada que indica un proceso de descifrado del sistema criptográfico de clave privada.

$Dec_k(C)$: Un resultado de descifrado obtenido descifrando un texto cifrado C mediante la función de descifrado de clave privada Dec con el uso de la clave común K.

[Cifrado de predicado del producto interior]

La configuración básica del cifrado de predicado del producto interior se describirá más abajo.

<Cifrado de predicado>
El cifrado de predicado (algunas veces llamado cifrado de función) supone que un texto cifrado se puede descifrar cuando una combinación de una información de atributo y una información de predicado hace verdadera una expresión lógica predeterminada. Una de la información de atributo y la información de predicado se incorpora en el texto cifrado y la otra se incorpora en la información de clave. La configuración de cifrado de predicado convencional se describe, por ejemplo, en la bibliografía de referencia 9, Jonathan Katz, Amit Sahai y Brent Waters, "Predicate Encryption supporting Disjunctions, Polynomial Equations, and Inner Products", uno de los cuatro documentos de Eurocrypt 2008 invitados por la Journal of Cryptology.

<Cifrado de predicado del producto interior>
El cifrado de predicado del producto interior supone que un texto cifrado se puede descifrar cuando el producto interior de una información de atributo y una información de predicado manejadas como vectores es cero. En el cifrado de predicado del producto interior, un producto interior de cero es equivalente a una expresión lógica de verdadero.

[Relación entre expresión lógica y polinomio]
En un cifrado de predicado del producto interior, una expresión lógica formada de una(s) OR lógica(s) y/o una(s) AND lógica(s) se expresa por un polinomio.

La OR lógica $(x = \eta_1) \vee (x = \eta_2)$ de la sentencia 1 que indica que x es η_1 y la sentencia 2 que indica que x es η_2 se expresa por el siguiente polinomio.

$$(x - \eta_1)\cdot(x - \eta_2) \qquad (36)$$

Entonces, las relaciones entre valores verdaderos y los valores de función de la Expresión (36) se muestran en la siguiente tabla.

Tabla 1

Sentencia 1 ($x = \eta_1$)	Sentencia 2 ($x = \eta_2$)	OR lógica $(x = \eta_1) \vee (x = \eta_2)$	Valor de función $(x = \eta_1)\cdot(x = \eta_2)$
Verdadera	Verdadera	Verdadera	0
Verdadera	Falsa	Verdadera	0
Falsa	Verdadera	Verdadera	0
Falsa	Falsa	Falsa	Distinto de 0

Como se entiende a partir de la Tabla 1, cuando la OR lógica $(x = \eta_1) \vee (x = \eta_2)$ es verdadera, el valor de función de la Expresión (36) es cero; y cuando la OR lógica $(x = \eta_1) \vee (x = \eta_2)$ es falsa, el valor de función de la Expresión (36) es un valor distinto de cero. En otras palabras, una OR lógica $(x = \eta_1) \vee (x = \eta_2)$ verdadera es equivalente a un valor de función de cero en la Expresión (36). Por lo tanto, la OR lógica se puede expresar por la Expresión (36).

La AND lógica $(x = \eta_1) \wedge (x = \eta_2)$ de la sentencia 1 que indica que x es η_1 y la sentencia 2 que indica que x es η_2 se expresa por el siguiente polinomio.

$$\iota_1\cdot(x - \eta_1) + \iota_2\cdot(x - \eta_2) \qquad (37)$$

donde ι_1 y ι_2 son números aleatorios. Entonces, las relaciones entre valores verdaderos y los valores de función de la Expresión (37) se muestran en la siguiente tabla.

Tabla 2

Sentencia 1 ($x = \eta_1$)	Sentencia 2 ($x = \eta_2$)	AND lógica $(x = \eta_1) \wedge (x = \eta_2)$	Valor de función $\iota_1\cdot(x - \eta_1) + \iota_2\cdot(x - \eta_2)$
Verdadera	Verdadera	Verdadera	0
Verdadera	Falsa	Falsa	Distinto de 0

Falsa	Verdadera	Falsa	Distinto de 0
Falsa	Falsa	Falsa	Distinto de 0

Como se entiende a partir de la Tabla 2, cuando la AND lógica $(x = \eta_1) \wedge (x = \eta_2)$ es verdadera, el valor de función de la Expresión (37) es cero; y cuando la AND lógica $(x = \eta_1) \wedge (x = \eta_2)$ es falsa, el valor de función de la Expresión (37) es un valor distinto de cero. En otras palabras, una AND lógica $(x = \eta_1) \wedge (x = \eta_2)$ verdadera es equivalente a un valor de función de cero en la Expresión (37). Por lo tanto, la AND lógica se puede expresar mediante la Expresión (37).

Como se describió anteriormente, usando las Expresiones (36) y (37), una expresión lógica formada por una(s) OR lógica(s) y/o una(s) AND lógica(s) se puede expresar por el polinomio f(x). Un ejemplo se mostrará más abajo.

Expresión lógica: $\{(x = \eta_1) \vee (x = \eta_2) \vee (x = \eta_3)\} \wedge (x = \eta_4) \wedge (x = \eta_5)$

Polinomio: $f(x) = \iota_1 \cdot \{(x - \eta_1) \cdot (x - \eta_2) \cdot (x - \eta_3)\} + \iota_2 \cdot (x - \eta_4) + \iota_3 \cdot (x - \eta_5)$

(38)

En la Expresión (36), se usa un elemento indeterminado x para expresar la OR lógica. También se puede usar una pluralidad de elementos indeterminados para expresar una OR lógica. Por ejemplo, se usan dos elementos indeterminados x_0 y x_1 para expresar la OR lógica $(x_0 = \eta_0) \vee (x_1 = \eta_1)$ de la sentencia 1 que indica que x_0 es η_0 y la sentencia 2 que indica que x_1 es η_1 mediante el siguiente polinomio.

$$(x_0 - \eta_0) \cdot (x_1 - \eta_1)$$

También se pueden usar tres o más elementos indeterminados para expresar una OR lógica por un polinomio.

En la Expresión (37), se usa un elemento indeterminado x para expresar la AND lógica. También se puede usar una pluralidad de elementos indeterminados para expresar una AND lógica. Por ejemplo, la AND lógica $(x_0 = \eta_0) \wedge (x_1 = \eta_1)$ de la sentencia 1 que indica que x_0 es η_0 y la sentencia 2 que indica que x_1 es η_1 se puede expresar por el siguiente polinomio.

$$\iota_0 \cdot (x_0 - \eta_0) + \iota_1 \cdot (x_1 - \eta_1)$$

También se pueden usar tres o más elementos indeterminados para expresar una AND lógica por un polinomio.

Una expresión lógica que incluye una(s) OR lógica(s) y/o una(s) AND lógica(s) se expresa con H (H $\geq$ 1) tipos de elementos indeterminados $x_0, \ldots, x_{H-1}$ según el polinomio $f(x_0, \ldots, x_{H-1})$. Se supone que una sentencia para cada uno de los elementos indeterminados $x_0, \ldots, x_{H-1}$ es "x_h es η_h", donde η_h (h = 0, …, H-1) es una constante determinada para cada sentencia. Entonces, en el polinomio $f(x_0, \ldots, x_{H-1})$ que indica la expresión lógica, la sentencia que indica que un elemento indeterminado x_h es una constante η_h se expresa por el polinomio que indica la diferencia entre el elemento indeterminado x_h y la constante η_h; cada OR lógica de sentencias se expresa por el producto de los polinomios que indican las sentencias; y la AND lógica de las sentencias y las OR lógicas de las sentencias se expresa por una OR lineal de los polinomios que indican las sentencias o las OR lógicas de las sentencias. Por ejemplo, se usan cinco elementos indeterminados $x_0, \ldots, x_4$ para expresar una expresión lógica

$$\{(x_0 = \eta_0) \vee (x_1 = \eta_1) \vee (x_2 = \eta_2)\} \wedge (x_3 = \eta_3) \wedge (x_4 = \eta_4)$$

por el siguiente polinomio

$$f(x0, \ldots, x4) = \iota_0 \cdot \{(x_0 - \eta_0) \cdot (x_1 - \eta_1) \cdot (x_2 - \eta_2)\} + \iota_1 \cdot (x_3 - \eta_3) + \iota_2 \cdot (x_4 - \eta_4)$$

[Relación entre polinomio y producto interior]

El polinomio $f(x_0, \ldots, x_{H-1})$ que indica una expresión lógica se puede expresar por el producto interior de dos vectores n dimensionales. Más específicamente, un vector que tiene los elementos indeterminados de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos,

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

y un vector que tiene los coeficientes de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos,

$$\vec{w} = (w_1, \ldots, w_n)$$

se usan para generar el producto interior de los mismos,

$$f(x_0, \ldots, x_{H-1}) = \vec{w} \cdot \vec{v}$$

que es igual al polinomio $f(x_0, \ldots, x_{H-1})$. En otras palabras, si el polinomio $f(x_0, \ldots, x_{H-1})$ que indica una expresión lógica es cero es equivalente a si el producto interior del vector $\vec{v}$ que tiene los elementos indeterminados de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos y el vector $\vec{w}$ que tiene los coeficientes de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos es cero.

$$f(x_0, \ldots, x_{H-1}) = 0 \leftrightarrow \vec{w} \cdot \vec{v} = 0$$

Por ejemplo, un polinomio $f(x) = \theta_0 \cdot x^0 + \theta_1 \cdot x + \ldots + \theta_{n-1} \cdot x^{n-1}$ se puede expresar con dos vectores n dimensionales

$$\vec{w} = (w_1, \ldots, w_n) = (\theta_0, \ldots, \theta_{n-1}) \quad (39)$$

$$\vec{v} = (v_1, \ldots, v_n) = (x^0, \ldots, x^{n-1}) \quad (40)$$

por el producto interior de los mismos.

$$f(x) = \vec{w} \cdot \vec{v} \quad (41)$$

En otras palabras, si el polinomio f(x) que indica una expresión lógica es cero es equivalente a si el producto interior en la Expresión (41) es cero.

$$f(x) = 0 \leftrightarrow \vec{w} \cdot \vec{v} = 0 \quad (42)$$

Cuando un vector que tiene los elementos indeterminados de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos se expresa por

$$\vec{w} = (w_1, \ldots, w_n)$$

y el vector que tiene los coeficientes de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos se expresa por

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

si el polinomio $f(x_0, \ldots, x_{H-1})$ que indica una expresión lógica es cero es equivalente a si el producto interior del vector $\vec{w}$ y el vector $\vec{v}$ es cero.

Por ejemplo, cuando se usan las siguientes expresiones en lugar de las expresiones (39) y (40),

$$\vec{w} = (w_1, \ldots, w_n) = (x^0, \ldots, x^{n-1}) \quad (43)$$

$$\vec{v} = (v_1, \ldots, v_n) = (\theta_0, \ldots, \theta_{n-1}) \quad (44)$$

si el polinomio f(x) que indica una expresión lógica es cero es equivalente a si el producto interior en la Expresión (41) es cero.

En el cifrado de predicado del producto interior, se usa uno de los vectores $\vec{v} = (v_1, \ldots, v_n)$ y $\vec{w} = (w_1, \ldots, w_n)$ como información de atributo y el otro se usa como información de predicado. Una de la información de atributo y la información de predicado se incorpora en el texto cifrado y la otra se incorpora en la información de clave. Por ejemplo, se usa un vector n dimensional $(\theta_0, \ldots, \theta_{n-1})$ como información de predicado, otro vector n dimensional $(x^0, \ldots, x^{n-1})$ se usa como información de atributo, una de la información de atributo y la información de predicado se incorpora en el texto cifrado, y la otra se incorpora en la información de clave. Se supone en la siguiente descripción que un vector n dimensional incorporado en la información de clave es $\vec{w} = (w_1, \ldots, w_n)$ y otro vector n dimensional incorporado en el texto cifrado es $\vec{v} = (v_1, \ldots, v_n)$. Por ejemplo,

Información de predicado: $\vec{w} = (w_1, \ldots, w_n) = (\theta_0, \ldots, \theta_{n-1})$

Información de atributo: $\vec{v} = (v_1, \ldots, v_n) = (x^0, \ldots, x^{n-1})$

Alternativamente,

Información de predicado: $\vec{v} = (v_1, \ldots, v_n) = (\theta_0, \ldots, \theta_{n-1})$

Información de atributo: $\vec{w} = (w_1, \ldots, w_n) = (x^0, \ldots, x^{n-1})$

[Configuración básica del cifrado de predicado del producto interior]
La configuración básica de un mecanismo de encapsulación de claves (KEM) que usa cifrado de predicado del producto interior se describirá más abajo. Esta configuración incluye Setup(1^k), GenKey(MSK, $\vec{w}$), Enc(PA, $\vec{v}$), y Dec(SKw, C_2).

<<Configuración de Setup(1^k)>>
Entrada: Parámetro de seguridad k

Salida: Información de clave maestra MSK, parámetro público PK

En un ejemplo de Setup(1^k), se usa un parámetro de seguridad k como n, se seleccionan una matriz de (n + 1) filas por (n + 1) columnas A que tiene un vector de base (n + 1) dimensional a_i (i = 1, …, n + 1) como elementos, una matriz de (n + 1) filas por (n + 1) columnas A* que tiene un vector de base a_i^* (i = 1, …, n + 1) como elementos, y unas matrices de (n + 1) filas por (n + 1) columnas X y X* usadas para conversión de coordenadas. Entonces, un vector de base (n + 1) dimensional b_i (i = 1, …, n + 1) se calcula a través de conversión de coordenadas por la Expresión (22) y un vector de base (n + 1) dimensional b_i^* (i = 1, …, n + 1) se calcula a través de conversión de coordenadas por la Expresión (24). Una matriz de (n + 1) filas por (n + 1) columnas B* que tiene el vector de base b_i^* (i = 1, …, n + 1) como elementos se saca como información de clave maestra MSK; y unos espacios de vector V y V*, una matriz de (n + 1) filas por (n + 1) columnas B que tiene el vector de base b_i (i = 1, …, n + 1) como elementos, el parámetro de seguridad k, el campo finito F_q, la curva elíptica E, los grupos cíclicos G_1, G_2, y G_T, los elementos de generación g_1, g_2, y g_T, la función bilineal e, y otros se sacan como un parámetro público PK.

<<Generación de información de clave GenKey(MSK, $\vec{w}$)>>
Entrada: Información de clave maestra MSK, vector $\vec{w}$

Salida: Información de clave D* que corresponde al vector $\vec{w}$

En un ejemplo de GenKey(MSK, $\vec{w}$), $\alpha \in F_q$ se selecciona a partir del campo finito F_q. Entonces, la matriz B*, la cual es la información de clave maestra MSK, se usa para generar y sacar una información de clave D* que corresponde al vector $\vec{w}$ de la siguiente manera.

$$\mathbf{D^* = \alpha \cdot (\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + b_{n+1}^* \in G_2^{n+1}} \qquad (45)$$

Es difícil resolver un problema logarítmico discreto en el grupo cíclico G_2, es difícil separar y extraer los componentes de $w_\mu \cdot b_\mu^*$ y b_{n+1}^*.

<<Cifrado Enc(PA, $\vec{v}$)>>
Entrada: Parámetro público PK, vector $\vec{v}$

Salida: Texto cifrado C_2, clave común K

En un ejemplo de Enc(PA, $\vec{v}$), se generan una clave común K y un número aleatorio υ_1, que es un elemento del campo finito F_q. Entonces, el parámetro público PK, tal como la matriz B, un elemento υ_2 que corresponde a un valor que incluye la clave común K, en el campo finito F_q, el vector $\vec{v}$, y el número aleatorio υ_1 se usan para generar el texto cifrado C_2 de la siguiente forma.

$$\mathbf{C_2 = \upsilon_1 \cdot (\sum_{\mu=1}^{n} v_\mu \cdot b_\mu) + \upsilon_2 \cdot b_{n+1} \in G_1^{n+1}} \qquad (46)$$

Se sacan el texto cifrado C_2 y la clave común K. Un ejemplo de la clave común K es $g_T^{\tau \upsilon_2} \in G_T$, donde $\upsilon 2$ significa υ_2. Un ejemplo de τ es 1_F, como se describió anteriormente. Es difícil resolver un problema logarítmico discreto en el grupo cíclico G_1, es difícil separar y extraer los componentes de $v_\mu \cdot b_\mu$ y $\upsilon_2 \cdot b_{n+1}$.

<<Descifrado y compartición de clave Dec(SKw, C_2)>>
Entrada: Información de clave D_1^* que corresponde al vector $\vec{w}$, texto cifrado C_2

Salida: Clave común K

En un ejemplo de Dec(SKw, C_2), el texto cifrado C_2 y la información de clave D_1* se introducen a la función bilineal e de la Expresión (2). Entonces, a partir de las características de las Expresiones (3) y (26), se satisface lo siguiente.

$$\begin{aligned} e(C_2, D^*) &= e(\upsilon_1 \cdot (\textstyle\sum_{\mu=1}^{n} v_\mu \cdot b_\mu) + \upsilon_2 \cdot b_{n+1}, \alpha \cdot (\textstyle\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + b_{n+1}^*) \\ &= e(\upsilon_1 \cdot v_1 \cdot b_1, \alpha \cdot w_1 \cdot b_1^*) \cdot \ldots \cdot e(\upsilon_1 \cdot v_n \cdot b_n, \alpha \cdot w_n \cdot b_n^*) \\ &\quad \times e(\upsilon_2 \cdot b_{n+1}, b_{n+1}^*) \\ &= e(b_1, b_1^*)^{\upsilon_1 \cdot v_1 \cdot \alpha \cdot w_1} \cdot \ldots \cdot e(b_n, b_n^*)^{\upsilon_1 \cdot v_n \cdot \alpha \cdot w_n} \cdot e(b_{n+1}, b_{n+1}^*)^{\upsilon_2} \\ &= g_T^{\tau \cdot \upsilon_1 \cdot v_1 \cdot \alpha \cdot w_1} \cdot \ldots \cdot g_T^{\tau \cdot \upsilon_1 \cdot v_n \cdot \alpha \cdot w_n} \cdot g_T^{\tau \cdot \upsilon_2} \\ &= g_T^{\tau \cdot \upsilon_1 \cdot \alpha \cdot \vec{v} \cdot \vec{w}} \cdot g_T^{\tau \cdot \upsilon_2} \end{aligned} \quad \ldots(47)$$

Cuando el producto interior $\vec{w} \cdot \vec{v}$ es cero, la Expresión (47) se puede cambiar a la siguiente.

$$\begin{aligned} e(C_2, D^*) &= g_T^{\tau \cdot \upsilon_1 \cdot \alpha \cdot 0} \cdot g_T^{\tau \cdot \upsilon_2} \\ &= g_T^{\tau \cdot \upsilon_2} \end{aligned} \quad \ldots(48)$$

A partir de este resultado, se genera y se saca la clave común K. Un ejemplo de la clave común K es $g_T^{\tau\upsilon_2} \in G_T$.

Los vectores de base (n + 1) dimensional se usan para configurar el algoritmo. La dimensión no está limitada a (n + 1). Un vector de base $(n + \Xi)$ dimensional b_i* (i = 1, …, $n + \Xi$) se puede usar para configurar el algoritmo, donde Ξ es un entero predeterminado igual a dos o más. En ese caso, la Expresión (49) se puede usar en lugar de la Expresión (45), y la Expresión (50) se puede usar en lugar de la Expresión (46), donde υ_1 es una constante o una variable (tal como un número aleatorio).

$$\mathbf{D^* = \alpha \cdot (\textstyle\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + \sum_{\iota=n+1}^{n+\Xi} \upsilon_\iota \cdot b_\iota^* \in G_2^{n+\Xi}} \quad (49)$$

$$\mathbf{C_2 = \upsilon_1 \cdot (\textstyle\sum_{\mu=1}^{n} v_\mu \cdot b_\mu) + \sum_{\iota=2}^{\Xi+1} \upsilon_\iota \cdot b_{\iota+n+1} \in G_1^{n+\Xi}} \quad (50)$$

La siguiente expresión se puede usar como la Expresión (45).

$$\mathbf{D^* = \alpha \cdot (\textstyle\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + \upsilon_{n+1} \cdot b_{n+1}^* \in G_2^{n+1}}$$

Además, se puede conmutar la información de entrada. Específicamente, w se sustituye con v en la Expresión (45) y v se sustituye con w en la Expresión (46). La descripción del <<suplemento>> finaliza aquí.

Información descrita en las figuras, tal como nombres, es imaginaria y no tiene relación con personas reales.

<Resumen>
Mientras que la presente invención se define enteramente por las reivindicaciones adjuntas, la descripción anterior del segundo aspecto se puede resumir en referencia a los siguientes elementos, que son útiles para comprender la invención. En la siguiente descripción, los números de elementos comenzarán de nuevo en uno.

Según un Elemento 1, se proporciona un método de comunicación criptográfico que es para un sistema criptográfico que usa cifrado de predicado e incluye al menos uno o una pluralidad de aparatos de cifrado; uno o una pluralidad de aparatos de generación de clave; y una pluralidad de aparatos de descifrado; en donde una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en lo sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo

de cifrado de predicado; y una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado se determina por adelantado. El método de comunicación criptográfico comprende: un primer paso de adquisición de información de lógica de predicado de uso de un tipo de información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, el un tipo de información de regla de conversión que se selecciona junto con la información de política según si una información de entrada introducida al aparato de cifrado es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo (en lo sucesivo llamada primera información de atributo) o una información de predicado (en lo sucesivo llamada primera información de predicado) a partir de la información de entrada, en una primera unidad de adquisición de información de lógica de predicado de cada uno del uno o la pluralidad de aparatos de cifrado; un paso de cifrado de uso de la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave, para obtener una clave común y una información de cifrado que corresponde a la clave común o que corresponde a una información usada para generar la clave común, según el algoritmo de cifrado de predicado en una unidad de cifrado del aparato de cifrado; un paso de transmisión de información de cifrado de transmisión de la información de cifrado a un primer aparato de descifrado, en una unidad de transmisor del aparato de cifrado; un paso de recepción de información de cifrado de recepción de la información de cifrado a partir del aparato de cifrado, en una unidad de recepción del primer aparato de descifrado; un segundo paso de adquisición de información de lógica de predicado de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (en lo sucesivo llamada según información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del aparato de descifrado, en una segunda unidad de adquisición de información de lógica de predicado de cada uno del uno o la pluralidad de aparatos de generación de clave; un paso de generación de clave de uso de la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave, para generar una primera clave de descifrado usada para descifrar la información de cifrado, en una unidad de generación de clave del aparato de generación de clave; y un paso de transmisión de clave de descifrado de transmisión de la primera clave de descifrado al primer aparato de descifrado, en una unidad de transmisor del aparato de generación de clave; un paso de recepción de clave de descifrado de recepción de la primera clave de descifrado desde el aparato de generación de clave, en la unidad de recepción del primer aparato de descifrado; un paso de descifrado de uso de la primera clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado del primer aparato de descifrado; un paso de transferencia de transferencia de la información de cifrado a un segundo aparato de descifrado, distinto del primer aparato de descifrado, en una unidad de transferencia del primer aparato de descifrado; un paso de recepción de recepción de la información de cifrado del primer aparato de descifrado, en una unidad de recepción del segundo aparato de descifrado; un tercer paso de adquisición de información de lógica de predicado de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada tercera información de atributo) o una información de predicado (en lo sucesivo llamada tercera información de predicado) a partir de la información de designación de atributo o la información de designación de predicado que corresponde a un usuario del segundo aparato de descifrado, en la segunda unidad de adquisición de información de lógica de predicado del aparato de generación de clave; un paso de generación de clave de uso de la tercera información de atributo o la tercera información de predicado, junto con la clave privada del aparato de generación de clave, para generar una segunda clave de descifrado usada para descifrar la información de cifrado, en la unidad de generación de clave del aparato de generación de clave; y un paso de transmisión de clave de descifrado de transmisión de la segunda clave de descifrado al segundo aparato de descifrado, en la unidad de transmisor del aparato de generación de clave; un paso de recepción de clave de descifrado de recepción de la segunda clave de descifrado desde el aparato de generación de clave, en la unidad de recepción del segundo aparato de descifrado; y un paso de descifrado de uso de la segunda clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado del segundo aparato de descifrado.

Según un Elemento 2, se proporciona un método de comunicación criptográfico que es para un sistema criptográfico que usa cifrado de predicado e incluye al menos uno o una pluralidad de aparatos de cifrado; uno o una pluralidad de aparatos de generación de clave; y uno o una pluralidad de aparatos de descifrado; en donde una clave privada y una clave publica que corresponde a la clave privada se determinan por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en lo sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo de cifrado de predicado; y se determina por adelantado una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado. El método de

comunicación criptográfico comprende: un primer paso de adquisición de información de lógica de predicado de uso de un tipo de información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, el un tipo de información de regla de conversión que se selecciona junto con la información de política según si una información de entrada introducida al aparato de cifrado es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo (en lo sucesivo llamada primera información de atributo) o una información de predicado (en lo sucesivo llamada primera información de predicado) a partir de la información de entrada, en una primera unidad de adquisición de información de lógica de predicado de cada uno del uno o la pluralidad de aparatos de cifrado; un paso de cifrado de uso de la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave, para obtener una clave común y una información de cifrado que corresponde a la clave común o que corresponde a una información usada para generar la clave común, según el algoritmo de cifrado de predicado en una unidad de cifrado del aparato de cifrado; un paso de transmisión de información de cifrado de transmisión de la información de cifrado a un primer aparato de descifrado, en una unidad de transmisor del aparato de cifrado; un paso de recepción de información de cifrado de recepción de información de cifrado desde el aparato de cifrado, en una unidad de recepción del primer aparato de descifrado; un segundo paso de adquisición de información de lógica de predicado de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (en lo sucesivo llamada segunda información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del primer aparato de descifrado, en una segunda unidad de adquisición de información de lógica de predicado del primer aparato de descifrado; un paso de transmisión de información de lógica de transmisión de la segunda información de atributo o la segunda información de predicado al aparato de generación de clave, en una unidad de transmisor del primer aparato de descifrado; un paso de recepción de información de lógica de recepción de la segunda información de atributo o la segunda información de predicado desde el primer aparato de descifrado, en una unidad de receptor del aparato de generación de clave; un paso de generación de clave de uso de la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave, para generar una primera clave de descifrado usada para descifrar la información de cifrado, en una unidad de generación de clave del aparato de generación de clave; y un paso de transmisión de clave de descifrado de transmisión de la primera clave de descifrado al primer aparato de descifrado, en una unidad de transmisor del aparato de generación de clave; un paso de recepción de clave de descifrado de recepción de la primera clave de descifrado desde el aparato de generación de clave, en una unidad de recepción del primer aparato de descifrado; un paso de descifrado de uso de la primera clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado del primer aparato de descifrado; un paso de transferencia de transferencia de la información de cifrado a un segundo aparato de descifrado, distinto del primer aparato de descifrado, en una unidad de transferencia del primer aparato de descifrado; un paso de recepción de recepción de la información de cifrado desde el primer aparato de descifrado, en una unidad de recepción del segundo aparato de descifrado; un tercer paso de adquisición de información de lógica de predicado de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada tercera información de atributo) o una información de predicado (en lo sucesivo llamada tercera información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del segundo aparato de descifrado, en la segunda unidad de adquisición de información de lógica de predicado del segundo aparato de descifrado; un paso de transmisión de información de lógica de transmisión de la tercera información de atributo o la tercera información de predicado al aparato de generación de clave, en una unidad de transmisor del segundo aparato de descifrado; un paso de recepción de información de lógica de recepción de la tercera información de atributo o la tercera información de predicado desde el segundo aparato de descifrado, en una unidad de receptor del aparato de generación de clave; un paso de generación de clave de uso de la tercera información de atributo o la tercera información de predicado, junto con la clave privada del aparato de generación de clave, para generar una segunda clave de descifrado usada para descifrar la información de cifrado, en la unidad de generación de clave del aparato de generación de clave; y un paso de transmisión de clave de descifrado de transmisión de la segunda clave de descifrado al segundo aparato de descifrado, en la unidad de transmisor del aparato de generación de clave; un paso de recepción de clave de descifrado de recepción de la segunda clave de descifrado desde el aparato de generación de clave, en una unidad de recepción del segundo aparato de descifrado; y un paso de descifrado de uso de la segunda clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado del segundo aparato de descifrado.

Según un Elemento 3, se proporciona un método de comunicación criptográfico que es para un sistema criptográfico que usa cifrado de predicado e incluye al menos uno o una pluralidad de aparatos de cifrado; uno o una pluralidad de aparatos de generación de clave; y uno o una pluralidad de aparatos de descifrado; en donde una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información (en lo sucesivo llamada información de

regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en lo sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo de cifrado de predicado; una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado se determina por adelantado. El método de comunicación criptográfico comprende: un primer paso de adquisición de información de lógica de predicado de uso de un tipo de información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, el un tipo de información de regla de conversión que se selecciona junto con la información de política según si una información de entrada introducida al aparato de cifrado es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo (en lo sucesivo llamada primera información de atributo) o una información de predicado (en lo sucesivo llamada primera información de predicado) a partir de la información de entrada, en una primera unidad de adquisición de información de lógica de predicado de cada uno del uno o la pluralidad de aparatos de cifrado; un paso de cifrado de uso de la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave y texto plano, para obtener una información de cifrado que corresponde al texto plano, según el algoritmo de cifrado de predicado en una unidad de cifrado del aparato de cifrado; un paso de transmisión de información de cifrado de transmisión de la información de cifrado a un primer aparato de descifrado, en una unidad de transmisor del aparato de cifrado; un paso de recepción de información de cifrado de recepción de la información de cifrado desde el aparato de cifrado, en una unidad de recepción del primer aparato de descifrado; un segundo paso de adquisición de información de lógica de predicado de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (en lo sucesivo llamada segunda información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del primer aparato de descifrado, en una segunda unidad de adquisición de información de lógica de predicado de cada uno del uno o la pluralidad de aparatos de generación de clave; un paso de generación de clave de uso de la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave, para generar una primera clave de descifrado usada para descifrar la información de cifrado, en una unidad de generación de clave del aparato de generación de clave; y un paso de transmisión de clave de descifrado de transmisión de la primera clave de descifrado al primer aparato de descifrado, en una unidad de transmisor del aparato de generación de clave; un paso de recepción de clave de descifrado de recepción de la primera clave de descifrado desde el aparato de generación de clave, en la unidad de recepción del primer aparato de descifrado; un paso de descifrado de uso de la primera clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado del primer aparato de descifrado; un paso de transferencia de transferencia de la información de cifrado a un segundo aparato de descifrado, distinto del primer aparato de descifrado, en una unidad de transferencia del primer aparato de descifrado; un paso de recepción de recepción de la información de cifrado desde el primer aparato de descifrado, en una unidad de recepción del segundo aparato de descifrado; un tercer paso de adquisición de información de lógica de predicado de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada tercera información de atributo) o una información de predicado (en lo sucesivo llamada tercera información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del segundo aparato de descifrado, en la segunda unidad de adquisición de información de lógica de predicado del segundo aparato de descifrado; un paso de generación de clave de uso de la tercera información de atributo o la tercera información de predicado, junto con la clave privada del aparato de generación de clave, para generar una segunda clave de descifrado usada para descifrar la información de cifrado, en la unidad de generación de clave del aparato de generación de clave; y un paso de transmisión de clave de descifrado de transmisión de la segunda clave de descifrado al segundo aparato de descifrado, en la unidad de transmisor del aparato de generación de clave; un paso de recepción de clave de descifrado de recepción de la segunda clave de descifrado desde el aparato de generación de clave, en la unidad de recepción del segundo aparato de descifrado; y un paso de descifrado de uso de la segunda clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado del segundo aparato de descifrado.

Según un Elemento 4, se proporciona un método de comunicación criptográfico que es para un sistema criptográfico que usa cifrado de predicado e incluye al menos uno o una pluralidad de aparatos de cifrado; uno o una pluralidad de aparatos de generación de clave; y uno o una pluralidad de aparatos de descifrado; en donde una clave privada y una clave publica que corresponde a la clave privada se determinan por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en

un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en lo sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo de cifrado de predicado; y se determina por adelantado una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado. El método de comunicación criptográfico comprende: un primer paso de adquisición de información de lógica de predicado de uso de un tipo de información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, el un tipo de información de regla de conversión que se selecciona junto con la información de política según si una información de entrada introducida al aparato de cifrado es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo (en lo sucesivo llamada primera información de atributo) o una información de predicado (en lo sucesivo llamada primera información de predicado) a partir de la información de entrada, en una primera unidad de adquisición de información de lógica de predicado de cada uno del uno o la pluralidad de aparatos de cifrado; un paso de cifrado de uso de la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave y texto plano, para obtener una información de cifrado que corresponde al texto plano según el algoritmo de cifrado de predicado en una unidad de cifrado del aparato de cifrado; un paso de transmisión de información de cifrado de transmisión de la información de cifrado a un primer aparato de descifrado, en una unidad de transmisor del aparato de cifrado; un paso de recepción de información de cifrado de recepción de la información de cifrado desde el aparato de cifrado, en una unidad de recepción del primer aparato de descifrado; un segundo paso de adquisición de información de lógica de predicado de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (en lo sucesivo llamada segunda información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del primer aparato de descifrado, en una segunda unidad de adquisición de información de lógica de predicado del primer aparato de descifrado; un paso de transmisión de información de lógica de transmisión de la segunda información de atributo o la segunda información de predicado al aparato de generación de clave, en una unidad de transmisor del primer aparato de descifrado; un paso de recepción de información de lógica de recepción de la segunda información de atributo o la segunda información de predicado desde el primer aparato de descifrado, en una unidad de receptor del aparato de generación de clave; un paso de generación de clave de uso de la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave, para generar una primera clave de descifrado usada para descifrar la información de cifrado, en una unidad de generación de clave del aparato de generación de clave; y un paso de transmisión de clave de descifrado de transmisión de la primera clave de descifrado al primer aparato de descifrado, en una unidad de transmisor del aparato de generación de clave; un paso de recepción de clave de descifrado de recepción de la primera clave de descifrado desde el aparato de generación de clave, en una unidad de recepción del primer aparato de descifrado; un paso de descifrado de uso de la primera clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado del primer aparato de descifrado; un paso de transferencia de transferencia de la información de cifrado a un segundo aparato de descifrado, distinto del primer aparato de descifrado, en una unidad de transferencia del primer aparato de descifrado; un paso de recepción de recepción de la información de cifrado desde el primer aparato de descifrado, en una unidad de recepción del segundo aparato de descifrado; un tercer paso de adquisición de información de lógica de predicado de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada tercera información de atributo) o una información de predicado (en lo sucesivo llamada tercera información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del segundo aparato de descifrado, en la segunda unidad de adquisición de información de lógica de predicado del segundo aparato de descifrado; un paso de transmisión de información de lógica de transmisión de la tercera información de atributo o la tercera información de predicado al aparato de generación de clave, en una unidad de transmisor del segundo aparato de descifrado; un paso de recepción de información de lógica de recepción de la tercera información de atributo o la tercera información de predicado desde el segundo aparato de descifrado, en la unidad de receptor del aparato de generación de clave; un paso de generación de clave de uso de la tercera información de atributo o la tercera información de predicado, junto con la clave privada del aparato de generación de clave, para generar una segunda clave de descifrado usada para descifrar la información de cifrado, en la unidad de generación de clave del aparato de generación de clave; y un paso de transmisión de clave de descifrado de transmisión de la segunda clave de descifrado al segundo aparato de descifrado, en la unidad de transmisor del aparato de generación de clave; un paso de recepción de clave de descifrado de recepción de la segunda clave de descifrado desde el aparato de generación de clave, en la unidad de recepción del segundo aparato de descifrado; y un paso de descifrado de uso de la segunda clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado del segundo aparato de descifrado.

Según un Elemento 5, se proporciona un método de comunicación criptográfico según uno de los Elementos 1 y 2, en donde el paso de cifrado comprende un paso de generación de texto cifrado de cifrado también de texto plano

con la clave común para obtener un texto cifrado, en la unidad de cifrado; y un paso de descifrado comprende un segundo paso de descifrado de realización de un segundo proceso de descifrado del texto cifrado con la clave común obtenida en el proceso de descifrado o un segundo proceso de descifrado del texto cifrado con una clave común generada a partir de la información usada para generar la clave común y obtenida en el proceso de descifrado, en la unidad de descifrado.

Según un Elemento 6, se proporciona un método de comunicación criptográfico según uno de los Elementos 1 a 5, que comprende un paso de adquisición de adquisición de la información de designación de atributo o la información de designación de predicado que corresponde al usuario del aparato de descifrado desde un medio de almacenamiento que almacena la información de designación de atributo y/o la información de designación de predicado que corresponde al usuario, en una unidad de adquisición del aparato de descifrado.

Según un Elemento 7, se proporciona un método de comunicación criptográfico según uno de los Elementos 1 y 3, que comprende un paso de transmisión de información de transmisión de la información de designación de atributo o la información de designación de predicado que corresponde al usuario del aparato de descifrado, al aparato de generación de clave, en una unidad de transmisor del aparato de descifrado; y un paso de recepción de información de usuario de recepción de la información de designación de atributo o la información de designación de predicado que corresponde al usuario desde el aparato de descifrado, en una unidad de receptor del aparato de generación de clave.

Según un Elemento 8, se proporciona un método de comunicación criptográfico según uno de los Elementos 1 a 6, en donde el sistema criptográfico además comprende uno o una pluralidad de aparatos de gestión de información con una unidad de almacenamiento adaptada para almacenar la información de designación de atributo y/o la información de designación de predicado que corresponde al usuario; y el método de comunicación criptográfico comprende un paso de adquisición de información de usuario de adquisición de la información de designación de atributo o la información de designación de predicado que corresponde al usuario del aparato de descifrado desde el aparato de gestión de información de usuario, en una unidad de adquisición de información de usuario del aparato de generación de clave.

Según un Elemento 9, se proporciona un método de comunicación criptográfico según uno de los Elementos 1 a 8, en donde el uno o la pluralidad de pares de información de regla de conversión se determinan por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; el sistema criptográfico comprende uno o una pluralidad de aparatos de gestión de par de información de regla de conversión dotados con una unidad de almacenamiento adaptada para almacenar el par de información de regla de conversión que corresponde a cada uno del uno o la pluralidad de aparatos de generación de clave; y el método de comunicación criptográfico comprende: un paso de adquisición de par de información de regla de conversión para adquirir el par de información de regla de conversión desde el aparato de gestión de par de información de regla de conversión, en una unidad de adquisición de par de información de regla de conversión del aparato de cifrado; y un paso de adquisición del par de información de regla de conversión de adquisición del par de información de regla de conversión desde el aparato de gestión de par de información de regla de conversión, en una unidad de adquisición de par de información de regla de conversión del aparato de descifrado.

Según un Elemento 10, se proporciona un método de comunicación criptográfico según uno de los Elementos 1 a 9, en donde si la información de política identifica solamente la información de regla de conversión de atributo, solamente la información de regla de conversión de predicado, o la información de regla de conversión de atributo y la información de regla de conversión de predicado se determina por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave.

Según un Elemento 11, se proporciona un método de comunicación criptográfico según uno de los Elementos 1 a 10, en donde una estructura algebraica K es un anillo finito o un campo finito; la primera y segunda información de atributo y la primera y segunda información de predicado son vectores que tienen elementos de K como componentes; y en el paso de descifrado, la información de cifrado y la clave de descifrado sirven como entradas y se realiza un cálculo que depende del resultado del producto interior canónico de la primera información de predicado y la segunda información de atributo, o del producto interior canónico de la primera información de atributo y la segunda información de predicado, en la unidad de descifrado.

Según un Elemento 12, se proporciona un método de comunicación criptográfico según el Elemento 11, en donde la clave pública es un conjunto de elementos de un módulo V en K; la clave privada es un conjunto de elementos de un módulo V* dual del módulo V; la clave de descifrado es un elemento del módulo dual V*; en el paso de cifrado, se realizan cálculos que incluyen una multiplicación escalar en la cual los elementos de la clave pública se multiplican por los componentes, usados como coeficientes, de la primera información de atributo o una multiplicación escalar en la que los elementos de la clave pública se multiplican por los componentes, usados como coeficientes, de la primera información de predicado, para obtener la información de cifrado, en la unidad de cifrado; en el paso de generación de clave, se realizan cálculos que incluyen una multiplicación escalar en la cual los elementos de la clave privada se multiplican por los componentes, usados como coeficientes, de la segunda información de predicado o

una multiplicación escalar en la cual los elementos de la clave privada se multiplican por los componentes, usados como coeficientes, de la segunda información de atributo, para obtener la clave de descifrado, en la unidad de generación de clave; y el cálculo usado en el proceso de descifrado de la unidad de descifrado tiene bilinealidad y el resultado de cálculo depende del resultado del producto interior canónico de la primera información de predicado y la segunda información de atributo, o de la primera información de atributo y la segunda información de predicado, todas las partes de la información que se sacan a partir de la información de cifrado y la clave de descifrado según una bilinealidad.

Según un Elemento 13, un sistema criptográfico que usa cifrado de predicado comprende al menos: uno o una pluralidad de aparatos de cifrado; uno o una pluralidad de aparatos de generación de clave; y una pluralidad de aparatos de descifrado; en donde una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en lo sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo de cifrado de predicado; una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado se determina por adelantado; cada uno del uno o la pluralidad de aparatos de cifrado comprende una primera unidad de adquisición de información de lógica de predicado adaptada para usar un tipo de información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, el un tipo de información de regla de conversión que se selecciona junto con la información de política según si una información de entrada introducida al aparato de cifrado es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo (en lo sucesivo llamada primera información de atributo) o una información de predicado (en lo sucesivo llamada primera información de predicado) a partir de la información de entrada; y una unidad de cifrado adaptada para usar la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave, para obtener una clave común, y una información de cifrado que corresponde a la clave común o que corresponde a una información usada para generar la clave común, según el algoritmo de cifrado de predicado; cada uno del uno o la pluralidad de aparatos de generación de clave comprende una segunda unidad de adquisición de información de lógica de predicado adaptada para usar la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (en lo sucesivo llamada segunda información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del aparato de descifrado; y una unidad de generación de clave adaptada para usar la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave, para generar una clave de descifrado usada para descifrar la información de cifrado; y el aparato de descifrado comprende una unidad de descifrado adaptada para usar la clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado; y una unidad de transferencia adaptada para transferir la información de cifrado a al menos un aparato de descifrado distinto del aparato de descifrado.

Según un Elemento 14, un sistema criptográfico que usa cifrado de predicado comprende al menos: uno o una pluralidad de aparatos de cifrado; uno o una pluralidad de aparatos de generación de clave; y una pluralidad de aparatos de descifrado; en donde una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en lo sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo de cifrado de predicado; una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado se determina por adelantado; cada uno del uno o la pluralidad de aparatos de cifrado comprende una primera unidad de adquisición de información de lógica de predicado adaptada para usar un tipo de información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, el un tipo de información de regla de conversión que se selecciona junto con la información de política según si una información de entrada introducida al aparato de cifrado es o bien una información de designación de atributo o bien una información de designación de predicado, para

obtener una información de atributo (en lo sucesivo llamada primera información de atributo) o una información de predicado (en lo sucesivo llamada primera información de predicado) a partir de la información de entrada; y una unidad de cifrado adaptada para usar la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave, para obtener una clave común, y una información de cifrado que corresponde a la clave común o que corresponde a una información usada para generar la clave común, según el algoritmo de cifrado de predicado; el aparato de descifrado comprende una segunda unidad de adquisición de información de lógica de predicado adaptada para usar la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (en lo sucesivo llamada segunda información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del aparato de descifrado; una unidad de descifrado adaptada para usar una clave de descifrado enviada desde el aparato de generación de clave para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado; y una unidad de transferencia adaptada para transferir la información de cifrado a al menos un aparato de descifrado distinto del aparato de descifrado; y cada uno del uno o la pluralidad de aparatos de generación de clave comprende una unidad de generación de clave adaptada para usar la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave, para generar la clave de descifrado usada para descifrar la información de cifrado.

Según un Elemento 15, un sistema criptográfico que usa cifrado de predicado comprende al menos: uno o una pluralidad de aparatos de cifrado; uno o una pluralidad de aparatos de generación de clave; y una pluralidad de aparatos de descifrado; en donde una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo de cifrado de predicado; una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado se determina por adelantado; cada uno del uno o la pluralidad de aparatos de cifrado comprende una primera unidad de adquisición de información de lógica de predicado adaptada para usar un tipo de información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, el un tipo de información de regla de conversión que se selecciona junto con la información de política según si una información de entrada introducida al aparato de cifrado es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo (en lo sucesivo llamada primera información de atributo) o una información de predicado (en lo sucesivo llamada primera información de predicado) a partir de la información de entrada; y una unidad de cifrado adaptada para usar la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave y texto plano, para obtener una información de cifrado que corresponde al texto plano según el algoritmo de cifrado de predicado; cada uno del uno o la pluralidad de aparatos de generación de clave comprende una segunda unidad de adquisición de información de lógica de predicado adaptada para usar la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (en lo sucesivo llamada segunda información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde un usuario del aparato de descifrado; y una unidad de generación de clave adaptada para usar la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave, para generar una clave de descifrado usada para descifrar la información de cifrado; y el aparato de descifrado comprende una unidad de descifrado adaptada para usar la clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado; y una unidad de transferencia adaptada para transferir la información de cifrado a al menos un aparato de descifrado distinto del aparato de descifrado.

Según un Elemento 16, un sistema criptográfico que usa cifrado de predicado comprende al menos: uno o una pluralidad de aparatos de cifrado; uno o una pluralidad de aparatos de generación de clave; y una pluralidad de aparatos de descifrado; en donde una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión

para convertir una información que designa un predicado (en sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo de cifrado de predicado; una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado se determina por adelantado; cada uno del uno o la pluralidad de aparatos de cifrado comprende una primera unidad de adquisición de información de lógica de predicado adaptada para usar un tipo de información de regla de conversión de la información de regla de conversión de atributo y la información de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, el un tipo de información de regla de conversión que se selecciona junto con la información de política según si una información de entrada introducida al aparato de cifrado es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo (en lo sucesivo llamada primera información de atributo) o una información de predicado (en lo sucesivo llamada primera información de predicado) a partir de la información de entrada; y una unidad de cifrado adaptada para usar la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave y texto plano, para obtener una información de cifrado que corresponde al texto plano según el algoritmo de cifrado de predicado; el aparato de descifrado comprende una segunda unidad de adquisición de información de lógica de predicado adaptada para usar la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o información de predicado (en lo sucesivo llamada segunda información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del aparato de descifrado; una unidad de descifrado adaptada para usar una clave de descifrado enviada desde el aparato de generación de clave para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado; y una unidad de transferencia adaptada para transferir la información de cifrado a al menos un aparato de descifrado distinto del aparato de descifrado; y cada uno del uno o la pluralidad de aparatos de generación de clave comprende una unidad de generación de clave adaptada para usar la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave, para generar la clave de descifrado usada para descifrar la información de cifrado.

Según un Elemento 17, se proporciona un sistema criptográfico según uno de los Elementos 13 y 14, en donde la unidad de cifrado del aparato de cifrado cifra un texto plano con la clave común para obtener un texto cifrado; y la unidad de descifrado del aparato de descifrado usa la clave común obtenida en el proceso de descifrado para aplicar un segundo proceso de descifrado al texto cifrado o usa una clave común generada a partir de la información que se obtiene en el proceso de descifrado y que se usa para generar la clave común para aplicar un segundo proceso de descifrado al texto cifrado.

Según un Elemento 18, se proporciona un aparato de descifrado el cual se usa en un sistema criptográfico que usa cifrado de predicado e incluye, al menos, uno o una pluralidad de aparatos de cifrado, uno o una pluralidad aparatos de generación de clave, y una pluralidad de aparatos de descifrado, en el sistema criptográfico, una clave privada y una clave pública que corresponde a la clave privada que se determina por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; uno o una pluralidad de pares de información de regla de conversión que se determina por adelantado, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en lo sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo de cifrado de predicado; y una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado que se determina por adelantado. El aparato de descifrado comprende: una unidad de descifrado adaptada para usar una clave de descifrado generada por el aparato de generación de clave para aplicar un proceso de descifrado a una información de cifrado generada por el aparato de cifrado, según el algoritmo de cifrado de predicado; y una unidad de transferencia adaptada para transferir la información de cifrado a al menos un aparato de descifrado distinto del aparato de descifrado.

Según un Elemento 19, se proporciona un aparato de descifrado el cual se usa en un sistema criptográfico que usa cifrado de predicado e incluye, al menos, uno o una pluralidad de aparatos de cifrado, uno o una pluralidad de aparatos de generación de clave, y una pluralidad de aparatos de descifrado, en el sistema criptográfico, una clave privada y una clave pública que corresponde a la clave privada que se determina por adelantado para cada uno del uno o la pluralidad de aparatos de generación de clave; uno o una pluralidad de pares de información de regla de conversión que se determina por adelantado, cada par de los cuales tiene una información (en lo sucesivo llamada información de regla de conversión de atributo) que prescribe una regla de conversión para convertir una información que designa un atributo (en lo sucesivo llamada información de designación de atributo) a una información de atributo usada en un algoritmo e información de cifrado de predicado (en lo sucesivo llamada información de regla de conversión de predicado) que prescribe una regla de conversión para convertir una información que designa un predicado (en lo sucesivo llamada información de designación de predicado) a una información de predicado usada en el algoritmo de cifrado de predicado; y una información de política que identifica

una de la información de regla de conversión de atributo y la información de regla de conversión de predicado que se determina por adelantado. El aparato de descifrado comprende: una segunda unidad de adquisición de información de lógica de predicado adaptada para usar la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo (en lo sucesivo llamada segunda información de atributo) o una información de predicado (en lo sucesivo llamada segunda información de predicado) a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del aparato de descifrado; una unidad de descifrado adaptada para usar una clave de descifrado generada por el aparato de generación de clave para aplicar un proceso de descifrado a una información de cifrado generada por el aparato de cifrado, según el algoritmo de cifrado de predicado; y una unidad de transferencia adaptada para transferir la información de cifrado a al menos un aparato de descifrado distinto del aparato de descifrado.

Según un Elemento 20, se proporciona un programa para hacer una función de ordenador como un aparato de descifrado según uno de los Elementos 18 y 19.

Según un Elemento 21, se proporciona un medio de almacenamiento legible por ordenador que tiene almacenado en el mismo un programa según el Elemento 20.

REIVINDICACIONES

1. Un método de comunicación criptográfico para un sistema criptográfico (1 – Figura 28) que usa un cifrado de predicado e incluye al menos
un aparato de cifrado (10 – Figura 33);
un aparato de generación de clave (20 – Figura 39); y
una pluralidad de aparatos de descifrado (30-1 – Figura 35, 30-2 – Figura 37);
en donde una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para el aparato de generación de clave (20 – Figura 39);
uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información, en lo sucesivo llamada información de regla de conversión de atributo, que prescribe una regla de conversión para convertir una información que designa un atributo, en lo sucesivo llamada información de designación de atributo, a una información de atributo usada en un algoritmo e información de cifrado de predicado, en lo sucesivo llamada información de regla de conversión de predicado, que prescribe una regla de conversión para convertir una información que designa un predicado, en lo sucesivo llamada información de designación de predicado, a una información de predicado usada en el algoritmo de cifrado de predicado; y
una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado se determina por adelantado;
el método de comunicación criptográfico que comprende:

un primer paso de adquisición de información de lógica de predicado (S17a – Figura 34) de uso de una información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, la de una información de regla de conversión que se selecciona junto con la información de política según si una información de entrada introducida al aparato de cifrado (10 – Figura 33) es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo, en lo sucesivo llamada primera información de atributo, o una información de predicado, en lo sucesivo llamada primera información de predicado, a partir de la información de entrada; en una primera unidad de adquisición de información de lógica de predicado (12 – Figura 33) del aparato de cifrado (10 – Figura 33);
un paso de cifrado (S17b – Figura 34) de uso de la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave (20 – Figura 39), para obtener una clave común y una información de cifrado que corresponde a la clave común o que corresponde a una información usada para generar la clave común, según el algoritmo de cifrado de predicado en una unidad de cifrado (13 – Figura 33) del aparato de cifrado (10 – Figura 33);
un paso de transmisión de información de cifrado (S18 – Figura 30) de transmisión de la información de cifrado a un primer aparato de descifrado (30-1 - Figura 35), en una unidad de transmisor (14 – Figura 33) del aparato de cifrado (10 - Figura 33);
un paso de recepción de información de cifrado (S18 – Figura 30) de recepción de la información de cifrado desde el aparato de cifrado (10 – Figura 33), en una unidad de recepción del primer aparato de descifrado (30-1 – Figura 35);
un segundo paso de adquisición de información de lógica de predicado (S24c – Figura 40) de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo, en lo sucesivo llamada segunda información de atributo, o una información de predicado, en lo sucesivo llamada segunda información de predicado, a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del primer aparato de descifrado (30-1 – Figura 35), en una segunda unidad de adquisición de información de lógica de predicado (23 – Figura 39) del aparato de generación de clave (20 – Figura 39);
un paso de generación de clave (S24d – Figura 40) de uso de la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave (20 – Figura 39), para generar una primera clave de descifrado usada para descifrar la información de cifrado, en una unidad de generación de clave (25 – Figura 39) del aparato de generación de clave (20 – Figura 39);
un paso de transmisión de clave de descifrado (S28 – Figura 31) de transmisión de la primera clave de descifrado al primer aparato de descifrado (30-1 - Figura 35), en una unidad de transmisor (24 – Figura 39) del aparato de generación de clave (20 - Figura 39);
un paso de recepción de clave de descifrado (S28 – Figura 31) de recepción de la primera clave de descifrado desde el aparato de generación de clave (20 – Figura 39), en una unidad de recepción del primer aparato de descifrado (30-1 – Figura 35);
un paso de descifrado (S22c – Figura 36) de uso de la primera clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado (33 – Figura 35) del primer aparato de descifrado (30 – Figura 35);
un paso de transferencia (S30 – Figura 32) de transferencia de la información de cifrado a un segundo aparato de descifrado (30-2 – Figura 37), distinto del primer aparato de descifrado (30-1 – Figura 35), en una unidad de transferencia (37 – Figura 35) del primer aparato de descifrado (30-1 – Figura 35);

un paso de recepción (S30 – Figura 32) de recepción de la información de cifrado desde el primer aparato de descifrado (30-1 – Figura 35), en una unidad de recepción del segundo aparato de descifrado (30-2 – Figura 37);
un tercer paso de adquisición de información de lógica de predicado (S36c – Figura 41) de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo, en lo sucesivo llamada tercera información de atributo, o una información de predicado, en lo sucesivo llamada tercera información de predicado, a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del segundo aparato de descifrado (30-2 – Figura 37), en una segunda unidad de adquisición de información de lógica de predicado (23 – Figura 39) del aparato de generación de clave (20 – Figura 39);
un paso de generación de clave (S36d – Figura 41) de uso de la tercera información de atributo o la tercera información de predicado, junto con la clave privada del aparato de generación de clave (20 – Figura 39), para generar una segunda clave de descifrado usada para descifrar la información de cifrado, en una unidad de generación de clave (25 – Figura 39) del aparato de generación de clave (20 – Figura 39);
un paso de transmisión de clave de descifrado (S40 – Figura 32) de transmisión de la segunda clave de descifrado al segundo aparato de descifrado (30-2 - Figura 37), en la unidad de transmisor (24 – Figura 39) del aparato de generación de clave (20 - Figura 39);
un paso de recepción de clave de descifrado (S40 – Figura 32) de recepción de la segunda clave de descifrado desde el aparato de generación de clave (20 – Figura 39), en la unidad de recepción del segundo aparato de descifrado (30-2 – Figura 37); y
un paso de descifrado (S34c – Figura 38) de uso de la segunda clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado (33 – Figura 37) del segundo aparato de descifrado (30-2 – Figura 37).

2. Un método de comunicación criptográfico para un sistema criptográfico (1 – Figura 28) que usa cifrado de predicado e incluye al menos
un aparato de cifrado (10 – Figura 33);
un aparato de generación de clave (20 – Figura 46); y
una pluralidad de aparatos de descifrado (30-1 – Figura 42, 30-2 – Figura 44);
en donde una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para el aparato de generación de clave (20 – Figura 46);
uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información, en lo sucesivo llamada información de regla de conversión de atributo, que prescribe una regla de conversión para convertir una información que designa un atributo, en lo sucesivo llamada información de designación de atributo, a una información de atributo usada en un algoritmo e información de cifrado de predicado, en lo sucesivo llamada información de regla de conversión de predicado, que prescribe una regla de conversión para convertir una información que designa un predicado, en lo sucesivo llamada información de designación de predicado, a una información de predicado usada en el algoritmo de cifrado de predicado; y
una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado se determina por adelantado;
el método de comunicación criptográfico que comprende:

un primer paso de adquisición de información de lógica de predicado (S17a – Figura 34) de uso de una información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, la de una información de regla de conversión que se selecciona junto con la información de política según si una información de entrada introducida al aparato de cifrado (10 – Figura 33) es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo, en lo sucesivo llamada primera información de atributo, o una información de predicado, en lo sucesivo llamada primera información de predicado, a partir de la información de entrada, en una primera unidad de adquisición de información de lógica de predicado (12 – Figura 33) del aparato de cifrado (10 – Figura 33);
un paso de cifrado (S17b – Figura 34) de uso de la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave (20 – Figura 46), para obtener una clave común y una información de cifrado que corresponde a la clave común o que corresponde a una información usada para generar la clave común, según el algoritmo de cifrado de predicado en una unidad de cifrado (13 – Figura 33) del aparato de cifrado (10 – Figura 33);
un paso de transmisión de información de cifrado (S18 – Figura 30) de transmisión de la información de cifrado a un primer aparato de descifrado (30-1 - Figura 42), en una unidad de transmisor (14 – Figura 33) del aparato de cifrado (10 - Figura 33);
un paso de recepción de información de cifrado (S18 – Figura 30) de recepción de la información de cifrado desde el aparato de cifrado (10 – Figura 33), en una unidad de recepción del primer aparato de descifrado (30-1 – Figura 42);
un segundo paso de adquisición de información de lógica de predicado (S23g – Figura 43) de uso de la

información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo, en lo sucesivo llamada segunda información de atributo, o una información de predicado, en lo sucesivo llamada segunda información de predicado, a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del primer aparato de descifrado (30-1 – Figura 42), en una segunda unidad de adquisición de información de lógica de predicado (35 – Figura 42) del primer aparato de descifrado (30-1 – Figura 42);

un paso de transmisión de información de lógica de transmisión de la segunda información de atributo o la segunda información de predicado al aparato de generación de clave (20 – Figura 46), en una unidad de transmisor (34 – Figura 42) del primer aparato de descifrado (30-1 – Figura 42);

un paso de recepción de información de lógica de recepción de la segunda información de atributo o la segunda información de predicado desde el primer aparato de descifrado (30-1 – Figura 42), en una unidad de receptor del aparato de generación de clave (20 – Figura 46);

un paso de generación de clave (S24d – Figura 47) de uso de la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave (20 – Figura 46), para generar una primera clave de descifrado usada para descifrar la información de cifrado, en una unidad de generación de clave (25 – Figura 46) del aparato de generación de clave (20 – Figura 46);

un paso de transmisión de clave de descifrado (S28 – Figura 31) de transmisión de la primera clave de descifrado al primer aparato de descifrado (30-1 - Figura 42), en una unidad de transmisor (24 – Figura 46) del aparato de generación de clave (20 - Figura 46);

un paso de recepción de clave de descifrado (S28 – Figura 31) de recepción de la primera clave de descifrado desde el aparato de generación de clave (20 – Figura 46), en la unidad de recepción del primer aparato de descifrado (30-1 – Figura 42);

un paso de descifrado (S22c – Figura 43) de uso de la primera clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado (33 – Figura 42) del primer aparato de descifrado (30-1 – Figura 42);

un paso de transferencia (S30 – Figura 32) de transferencia de la información de cifrado a un segundo aparato de descifrado (30-2 - Figura 44), distinto del primer aparato de descifrado (30-1 – Figura 42), en una unidad de transferencia (37 – Figura 42) del primer aparato de descifrado (30-1 - Figura 42);

un paso de recepción (S30 – Figura 32) de recepción de la información de cifrado desde el primer aparato de descifrado (30-1 – Figura 42), en una unidad de recepción del segundo aparato de descifrado (30-2 – Figura 44);

un tercer paso de adquisición de información de lógica de predicado (S35g – Figura 45) de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo, en lo sucesivo llamada tercera información de atributo, o una información de predicado, en lo sucesivo llamada tercera información de predicado, a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del segundo aparato de descifrado (30-2 – Figura 44), en la segunda unidad de adquisición de información de lógica de predicado (35 – Figura 44) del segundo aparato de descifrado (30-2 – Figura 44);

un paso de transmisión de información de lógica de transmisión de la tercera información de atributo o la tercera información de predicado al aparato de generación de clave (20 – Figura 46), en una unidad de transmisor (34 – Figura 44) del segundo aparato de descifrado (30-2 – Figura 44);

un paso de recepción de información de lógica de recepción de la tercera información de atributo o la tercera información de predicado desde el segundo aparato de descifrado (30-2 – Figura 44), en una unidad de receptor del aparato de generación de clave (20 – Figura 46);

un paso de generación de clave (S36d – Figura 48) de uso de la tercera información de atributo o la tercera información de predicado, junto con la clave privada del aparato de generación de clave (20 – Figura 46), para generar una segunda clave de descifrado usada para descifrar la información de cifrado, en la unidad de generación de clave (25 – Figura 46) del aparato de generación de clave (20 – Figura 46);

un paso de transmisión de clave de descifrado (S40 – Figura 32) de transmisión de la segunda clave de descifrado al segundo aparato de descifrado (30-2 - Figura 44), en la unidad de transmisor (24 – Figura 46) del aparato de generación de clave (20 - Figura 46);

un paso de recepción de clave de descifrado (S40 – Figura 32) de recepción de la segunda clave de descifrado desde el aparato de generación de clave (20 – Figura 46), en la unidad de recepción del segundo aparato de descifrado (30-2 – Figura 44); y

un paso de descifrado (S34c – Figura 45) de uso de la segunda clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado (33 – Figura 44) del segundo aparato de descifrado (30-2 – Figura 44).

3. Un método de comunicación criptográfico para un sistema criptográfico (1 – Figura 28) que usa un cifrado de predicado e incluye al menos

un aparato de cifrado (10 – Figura 49);

un aparato de generación de clave (20 – Figura 39); y

una pluralidad de aparatos de descifrado (30-1 – Figura 51, 30-2 – Figura 53);

en donde una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para el aparato de generación de clave (20 – Figura 39);
uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información, en lo sucesivo llamada información de regla de conversión de atributo, que prescribe una regla de conversión para convertir una información que designa un atributo, en lo sucesivo llamada información de designación de atributo, a una información de atributo usada en un algoritmo e información de cifrado de predicado, en lo sucesivo llamada información de regla de conversión de predicado, que prescribe una regla de conversión para convertir una información que designa un predicado, en lo sucesivo llamada información de designación de predicado, a una información de predicado usada en el algoritmo de cifrado de predicado; y
una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado se determina por adelantado;
el método de comunicación criptográfico que comprende:

un primer paso de adquisición de información de lógica de predicado (S17a – Figura 50) de uso de una información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, la de una información de regla de conversión que se selecciona junto con la información de política según si una información de entrada introducida al aparato de cifrado (10 – Figura 49) es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo, en lo sucesivo llamada primera información de atributo, o una información de predicado, en lo sucesivo llamada primera información de predicado, a partir de la información de entrada, en una primera unidad de adquisición de información de lógica de predicado (12 – Figura 49) del aparato de cifrado (10 – Figura 49);
un paso de cifrado (S17b1 – Figura 50) de uso de la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave (20 – Figura 39) y texto plano, para obtener una información de cifrado que corresponde al texto plano, según el algoritmo de cifrado de predicado en una unidad de cifrado (13 – Figura 49) del aparato de cifrado (10 – Figura 49);
un paso de transmisión de información de cifrado (S18 – Figura 30) de transmisión de la información de cifrado a un primer aparato de descifrado (30-1 - Figura 51), en una unidad de transmisor (14 – Figura 49) del aparato de cifrado (10 - Figura 49);
un paso de recepción de información de cifrado (S18 – Figura 30) de recepción de la información de cifrado desde el aparato de cifrado (10 – Figura 49), en una unidad de recepción del primer aparato de descifrado (30-1 – Figura 51);
un segundo paso de adquisición de información de lógica de predicado (S24c – Figura 40) de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo, en lo sucesivo llamada segunda información de atributo, o una información de predicado, en lo sucesivo llamada segunda información de predicado, a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del primer aparato de descifrado (30-1 – Figura 51), en una segunda unidad de adquisición de información de lógica de predicado (23 – Figura 39) del aparato de generación de clave (20 – Figura 39);
un paso de generación de clave (S24d – Figura 40) de uso de la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave (20 – Figura 39), para generar una primera clave de descifrado usada para descifrar la información de cifrado, en una unidad de generación de clave (25 – Figura 39) del aparato de generación de clave (20 – Figura 39);
un paso de transmisión de clave de descifrado (S28 – Figura 31) de transmisión de la primera clave de descifrado al primer aparato de descifrado (30-1 - Figura 51), en una unidad de transmisor (24 – Figura 39) del aparato de generación de clave (20 - Figura 39);
un paso de recepción de clave de descifrado (S28 – Figura 31) de recepción de la primera clave de descifrado desde el aparato de generación de clave (20 – Figura 39), en la unidad de recepción del primer aparato de descifrado (30-1 – Figura 51);
un paso de descifrado (S22c1 – Figura 52) de uso de la primera clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado (33 – Figura 51) del primer aparato de descifrado (30 – Figura 51);
un paso de transferencia (S30 – Figura 32) de transferencia de la información de cifrado a un segundo aparato de descifrado (30-2 - Figura 53), distinto del primer aparato de descifrado (30-1 – Figura 51), en una unidad de transferencia (37 – Figura 51) del primer aparato de descifrado (30-1 - Figura 51);
un paso de recepción (S30 – Figura 32) de recepción de la información de cifrado desde el primer aparato de descifrado (30-1 – Figura 51), en una unidad de recepción del segundo aparato de descifrado (30-2 – Figura 53);
un tercer paso de adquisición de información de lógica de predicado (S36c – Figura 41) de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo, en lo sucesivo llamada tercera información de atributo, o una información de predicado, en lo sucesivo llamada tercera información de predicado, a partir de una información de designación de atributo o una información de designación de predicado que

corresponde a un usuario del segundo aparato de descifrado (30-2 – Figura 53), en la segunda unidad de adquisición de información de lógica de predicado (23 – Figura 39) del aparato de generación de clave (20 – Figura 39);
un paso de generación de clave (S36d – Figura 41) de uso de la tercera información de atributo o la tercera información de predicado, junto con la clave privada del aparato de generación de clave (20 – Figura 39), para generar una segunda clave de descifrado usada para descifrar la información de cifrado, en la unidad de generación de clave (25 – Figura 39) del aparato de generación de clave (20 – Figura 39);
un paso de transmisión de clave de descifrado (S40 – Figura 32) de transmisión de la segunda clave de descifrado al segundo aparato de descifrado (30-2 - Figura 53), en la unidad de transmisor (24 – Figura 39) del aparato de generación de clave (20 - Figura 39);
un paso de recepción de clave de descifrado (S40 – Figura 32) de recepción de la segunda clave de descifrado desde el aparato de generación de clave (20 – Figura 39), en la unidad de recepción del segundo aparato de descifrado (30-2 – Figura 53); y
un paso de descifrado (S34c1 – Figura 54) de uso de la segunda clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado (33 – Figura 53) del segundo aparato de descifrado (30-2 – Figura 53).

4. Un método de comunicación criptográfico para un sistema criptográfico (1 – Figura 28) que usa cifrado de predicado e incluye al menos
un aparato de cifrado (10 – Figura 49);
un aparato de generación de clave (20 – Figura 46); y
una pluralidad de aparatos de descifrado (30-1 – Figura 55, 30-2 – Figura 57);
en donde una clave privada y una clave pública que corresponde a la clave privada se determinan por adelantado para el aparato de generación de clave (20 – Figura 46);
uno o una pluralidad de pares de información de regla de conversión se determinan por adelantado, cada par de los cuales tiene una información, en lo sucesivo llamada información de regla de conversión de atributo, que prescribe una regla de conversión para convertir una información que designa un atributo, en lo sucesivo llamada información de designación de atributo, a una información de atributo usada en un algoritmo e información de cifrado de predicado, en lo sucesivo llamada información de regla de conversión de predicado, que prescribe una regla de conversión para convertir una información que designa un predicado, en lo sucesivo llamada información de designación de predicado, a una información de predicado usada en el algoritmo de cifrado de predicado; y
una información de política que identifica una de la información de regla de conversión de atributo y la información de regla de conversión de predicado se determina por adelantado;
el método de comunicación criptográfico que comprende:

un primer paso de adquisición de información de lógica de predicado (S17a – Figura 50) de uso de una de una información de regla de conversión de la información de regla de conversión de atributo y la información de regla de conversión de predicado incluida en un par de información de regla de conversión seleccionado a partir del uno o la pluralidad de pares de información de regla de conversión, la de una información de regla de conversión que se selecciona junto con la información de política según si una información de entrada introducida al aparato de cifrado (10 – Figura 49) es o bien una información de designación de atributo o bien una información de designación de predicado, para obtener una información de atributo, en lo sucesivo llamada primera información de atributo, o una información de predicado, en lo sucesivo llamada primera información de predicado, a partir de la información de entrada, en una primera unidad de adquisición de información de lógica de predicado (12 – Figura 49) del aparato de cifrado (10 – Figura 49);
un paso de cifrado (S17b1 – Figura 50) de uso de la primera información de atributo o la primera información de predicado, junto con la clave pública del aparato de generación de clave (20 – Figura 46) y texto plano, para obtener una información de cifrado que corresponde al texto plano, según el algoritmo de cifrado de predicado en una unidad de cifrado (13 – Figura 49) del aparato de cifrado (10 – Figura 49);
un paso de transmisión de información de cifrado (S18 – Figura 30) de transmisión de la información de cifrado a un primer aparato de descifrado (30-1 - Figura 55), en una unidad de transmisor (14 – Figura 49) del aparato de cifrado (10 - Figura 49);
un paso de recepción de información de cifrado (S18 – Figura 30) de recepción de la información de cifrado desde el aparato de cifrado (10 – Figura 49), en una unidad de recepción del primer aparato de descifrado (30-1 – Figura 55);
un segundo paso de adquisición de información de lógica de predicado (S23g – Figura 56) de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo, en lo sucesivo llamada segunda información de atributo, o una información de predicado, en lo sucesivo llamada segunda información de predicado, a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del primer aparato de descifrado (30-1 – Figura 55), en una segunda unidad de adquisición de información de lógica de predicado (35 – Figura 55) del primer aparato de descifrado (30-1 – Figura 55);
un paso de transmisión de información de lógica de transmisión de la segunda información de atributo o la segunda información de predicado al aparato de generación de clave (20 – Figura 46), en una unidad de

transmisor (34 – Figura 55) del primer aparato de descifrado (30-1 – Figura 55);
un paso de recepción de información de lógica de recepción de la segunda información de atributo o la segunda información de predicado desde el primer aparato de descifrado (30-1 – Figura 55), en una unidad de receptor del aparato de generación de clave (20 – Figura 46);
un paso de generación de clave (S24d – Figura 47) de uso de la segunda información de atributo o la segunda información de predicado, junto con la clave privada del aparato de generación de clave (20 – Figura 46), para generar una primera clave de descifrado usada para descifrar la información de cifrado, en una unidad de generación de clave (25 – Figura 46) del aparato de generación de clave (20 – Figura 46);
un paso de transmisión de clave de descifrado (S28 – Figura 31) de transmisión de la primera clave de descifrado al primer aparato de descifrado (30-1 - Figura 55), en una unidad de transmisor (24 – Figura 46) del aparato de generación de clave (20 - Figura 46);
un paso de recepción de clave de descifrado (S28 – Figura 31) de recepción de la primera clave de descifrado desde el aparato de generación de clave (20 – Figura 46), en la unidad de recepción del primer aparato de descifrado (30-1 – Figura 55);
un paso de descifrado (S22c1 – Figura 56) de uso de la primera clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado (35 – Figura 55) del primer aparato de descifrado (30-1 – Figura 55);
un paso de transferencia (S30 – Figura 32) de transferencia de la información de cifrado a un segundo aparato de descifrado (30-2 - Figura 57), distinto del primer aparato de descifrado (30-1 – Figura 55), en una unidad de transferencia (37 – Figura 55) del primer aparato de descifrado (30-1 - Figura 55);
un paso de recepción (S30 – Figura 32) de recepción de la información de cifrado desde el primer aparato de descifrado (30-1 – Figura 55), en una unidad de recepción del segundo aparato de descifrado (30-2 – Figura 57);
un tercer paso de adquisición de información de lógica de predicado (S35g – Figura 58) de uso de la información de regla de conversión emparejada con la información de regla de conversión identificada por la información de política para obtener una información de atributo, en lo sucesivo llamada tercera información de atributo, o una información de predicado, en lo sucesivo llamada tercera información de predicado, a partir de una información de designación de atributo o una información de designación de predicado que corresponde a un usuario del segundo aparato de descifrado (30-2 – Figura 57), en la segunda unidad de adquisición de información de lógica de predicado (35 – Figura 57) del segundo aparato de descifrado (30-2 – Figura 57);
un paso de transmisión de información de lógica de transmisión de la tercera información de atributo o la tercera información de predicado al aparato de generación de clave (20 – Figura 46), en una unidad de transmisor (34 – Figura 57) del segundo aparato de descifrado (30-2 – Figura 57);
un paso de recepción de información de lógica de recepción de la tercera información de atributo o la tercera información de predicado desde el segundo aparato de descifrado (30-2 – Figura 57), en una unidad de receptor del aparato de generación de clave (20 – Figura 46);
un paso de generación de clave (S36d – Figura 48) de uso de la tercera información de atributo o la tercera información de predicado, junto con la clave privada del aparato de generación de clave (20 – Figura 46), para generar una segunda clave de descifrado usada para descifrar la información de cifrado, en la unidad de generación de clave (25 – Figura 46) del aparato de generación de clave (20 – Figura 46);
un paso de transmisión de clave de descifrado (S40 – Figura 32) de transmisión de la segunda clave de descifrado al segundo aparato de descifrado (30-2 - Figura 57), en la unidad de transmisor (24 – Figura 46) del aparato de generación de clave (20 - Figura 46);
un paso de recepción de clave de descifrado (S40 – Figura 32) de recepción de la segunda clave de descifrado desde el aparato de generación de clave (20 – Figura 46), en la unidad de recepción del segundo aparato de descifrado (30-2 – Figura 57); y
un paso de descifrado (S34c1 – Figura 58) de uso de la segunda clave de descifrado para aplicar un proceso de descifrado a la información de cifrado según el algoritmo de cifrado de predicado en una unidad de descifrado (33 – Figura 57) del segundo aparato de descifrado (30-2 – Figura 57).

FIG.1

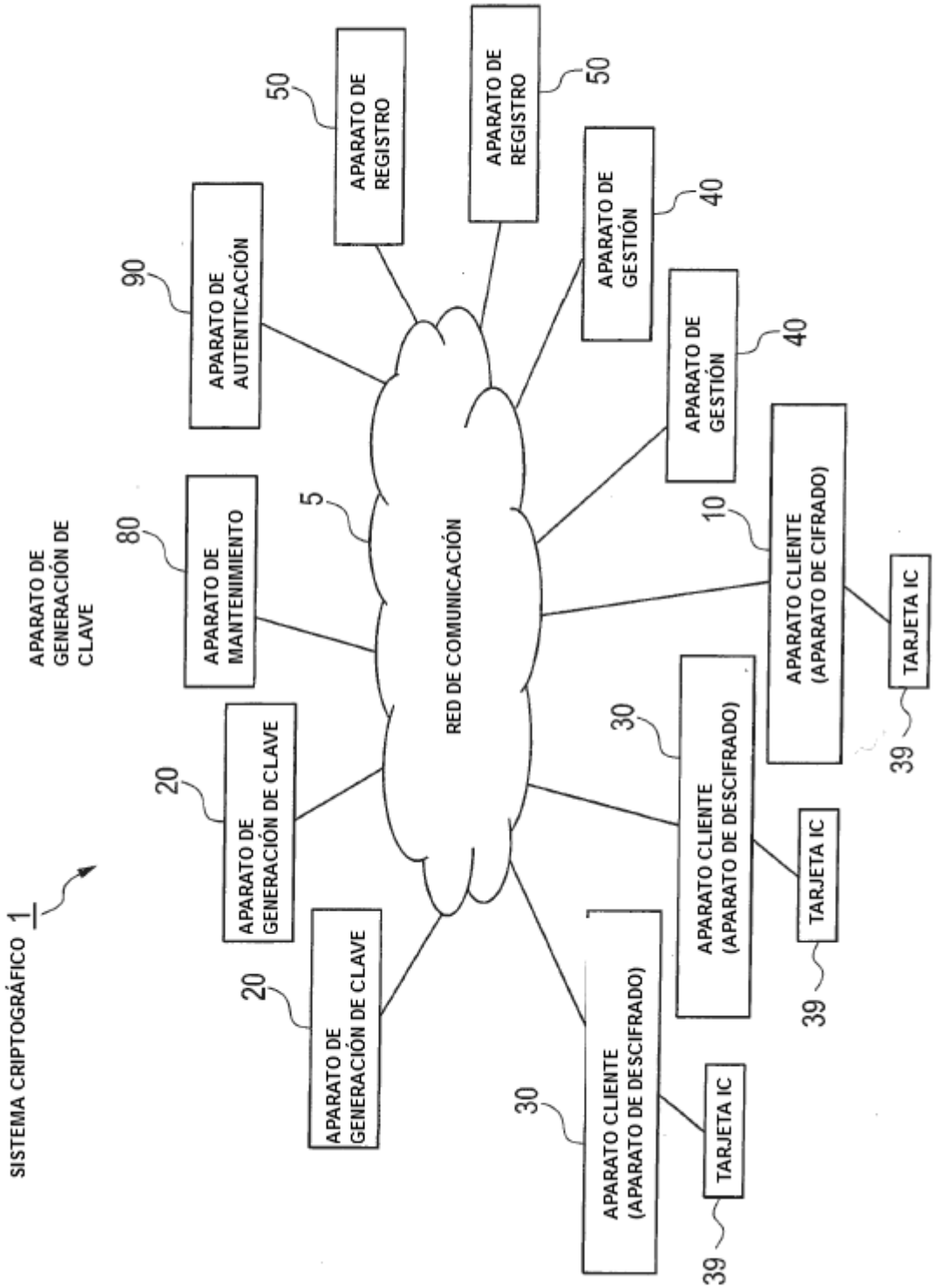

SISTEMA CRIPTOGRÁFICO 1
APARATO DE GENERACIÓN DE CLAVE
APARATO DE GENERACIÓN DE CLAVE
20
APARATO DE GENERACIÓN DE CLAVE
20
APARATO DE MANTENIMIENTO
80
APARATO DE AUTENTICACIÓN
90
APARATO DE REGISTRO
50
APARATO DE REGISTRO
50
APARATO DE GESTIÓN
40
APARATO DE GESTIÓN
40
RED DE COMUNICACIÓN
5
APARATO CLIENTE (APARATO DE CIFRADO)
10
TARJETA IC
39
APARATO CLIENTE (APARATO DE DESCIFRADO)
30
TARJETA IC
39
APARATO CLIENTE (APARATO DE DESCIFRADO)
30
TARJETA IC
39

FIG.2

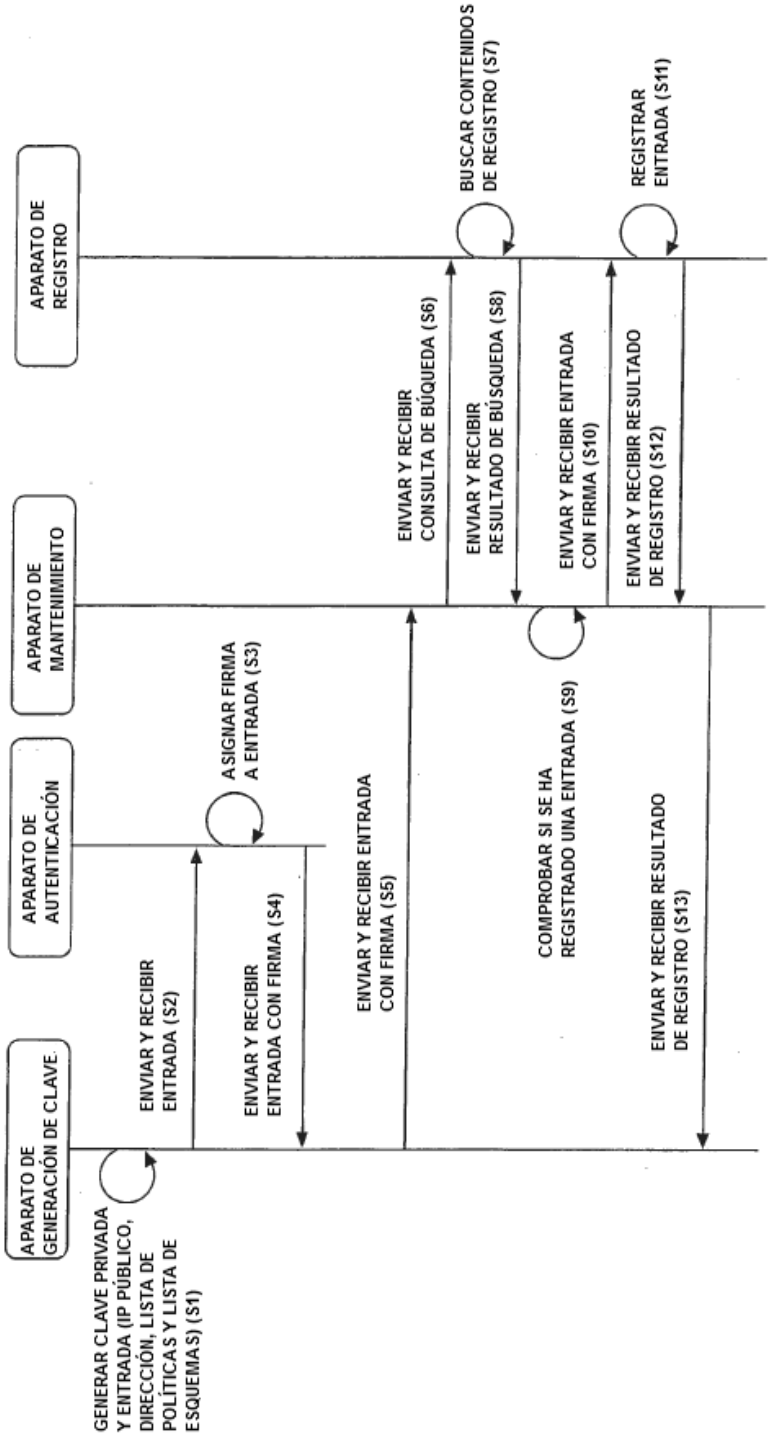

APARATO DE GENERACIÓN DE CLAVE
APARATO DE AUTENTICACIÓN
APARATO DE MANTENIMIENTO
APARATO DE REGISTRO
GENERAR CLAVE PRIVADA Y ENTRADA (IP PÚBLICO, DIRECCIÓN, LISTA DE POLÍTICAS Y LISTA DE ESQUEMAS) (S1)
ENVIAR Y RECIBIR ENTRADA (S2)
ASIGNAR FIRMA A ENTRADA (S3)
ENVIAR Y RECIBIR ENTRADA CON FIRMA (S4)
ENVIAR Y RECIBIR ENTRADA CON FIRMA (S5)
ENVIAR Y RECIBIR CONSULTA DE BÚQUEDA (S6)
BUSCAR CONTENIDOS DE REGISTRO (S7)
ENVIAR Y RECIBIR RESULTADO DE BÚSQUEDA (S8)
COMPROBAR SI SE HA REGISTRADO UNA ENTRADA (S9)
ENVIAR Y RECIBIR ENTRADA CON FIRMA (S10)
REGISTRAR ENTRADA (S11)
ENVIAR Y RECIBIR RESULTADO DE REGISTRO (S12)
ENVIAR Y RECIBIR RESULTADO DE REGISTRO (S13)

FIG.3

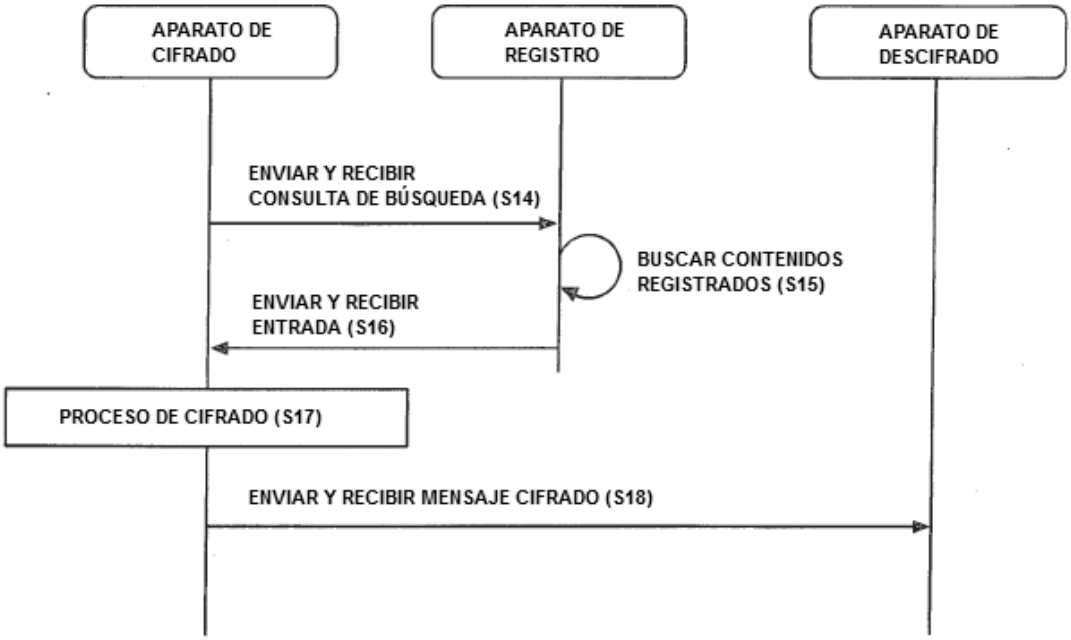

APARATO DE CIFRADO
APARATO DE REGISTRO
APARATO DE DESCIFRADO
ENVIAR Y RECIBIR CONSULTA DE BÚSQUEDA (S14)
BUSCAR CONTENIDOS REGISTRADOS (S15)
ENVIAR Y RECIBIR ENTRADA (S16)
PROCESO DE CIFRADO (S17)
ENVIAR Y RECIBIR MENSAJE CIFRADO (S18)

FIG.4

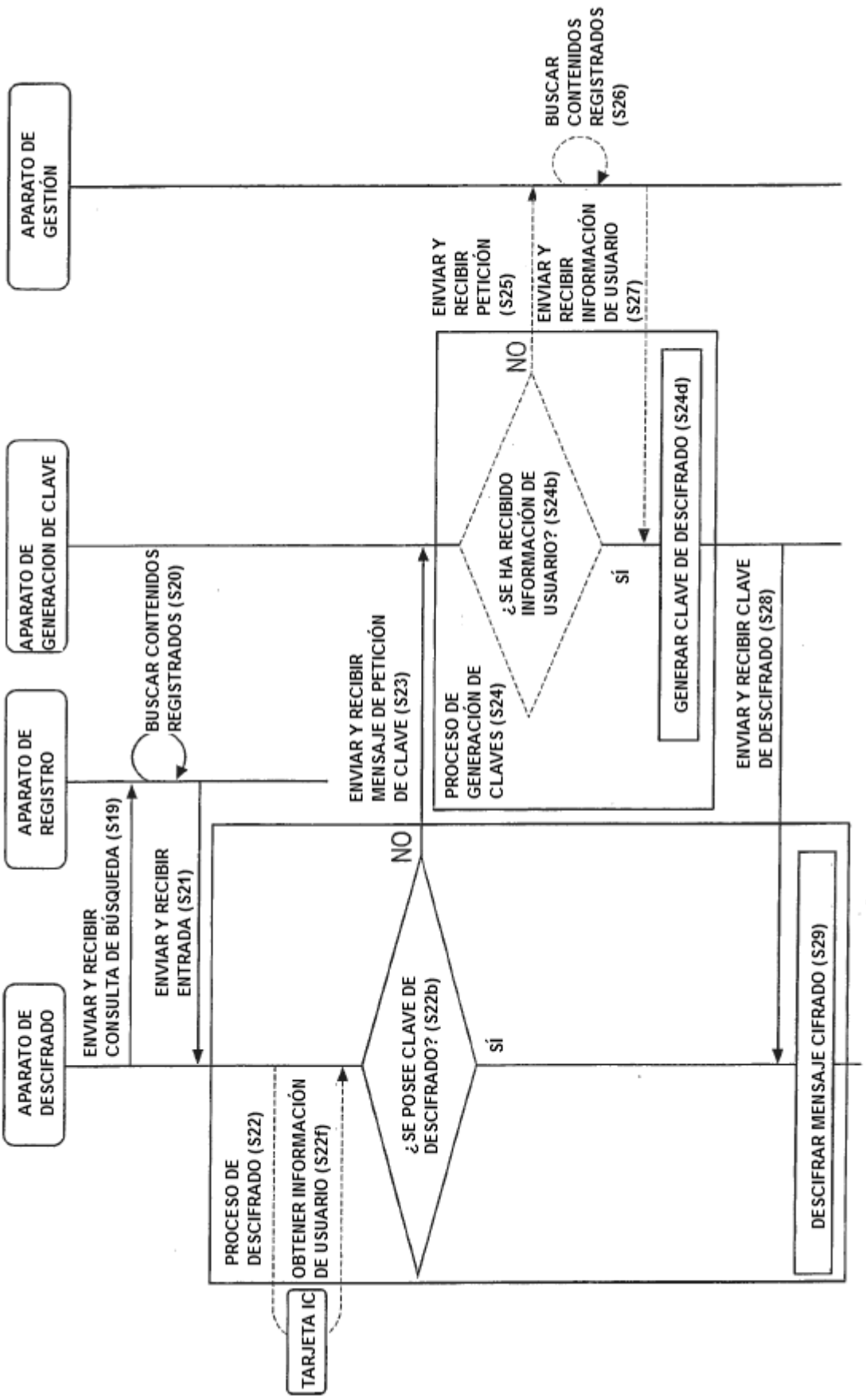

APARATO DE GESTIÓN
APARATO DE GENERACION DE CLAVE
APARATO DE REGISTRO
APARATO DE DESCIFRADO
TARJETA IC
BUSCAR CONTENIDOS REGISTRADOS (S26)
ENVIAR Y RECIBIR PETICIÓN (S25)
ENVIAR Y RECIBIR INFORMACIÓN DE USUARIO (S27)
NO
¿SE HA RECIBIDO INFORMACIÓN DE USUARIO? (S24b)
sí
PROCESO DE GENERACIÓN DE CLAVES (S24)
GENERAR CLAVE DE DESCIFRADO (S24d)
BUSCAR CONTENIDOS REGISTRADOS (S20)
ENVIAR Y RECIBIR MENSAJE DE PETICIÓN DE CLAVE (S23)
ENVIAR Y RECIBIR CLAVE DE DESCIFRADO (S28)
ENVIAR Y RECIBIR CONSULTA DE BÚSQUEDA (S19)
ENVIAR Y RECIBIR ENTRADA (S21)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S22b)
sí
PROCESO DE DESCIFRADO (S22)
OBTENER INFORMACIÓN DE USUARIO (S22f)
DESCIFRAR MENSAJE CIFRADO (S29)

FIG.5

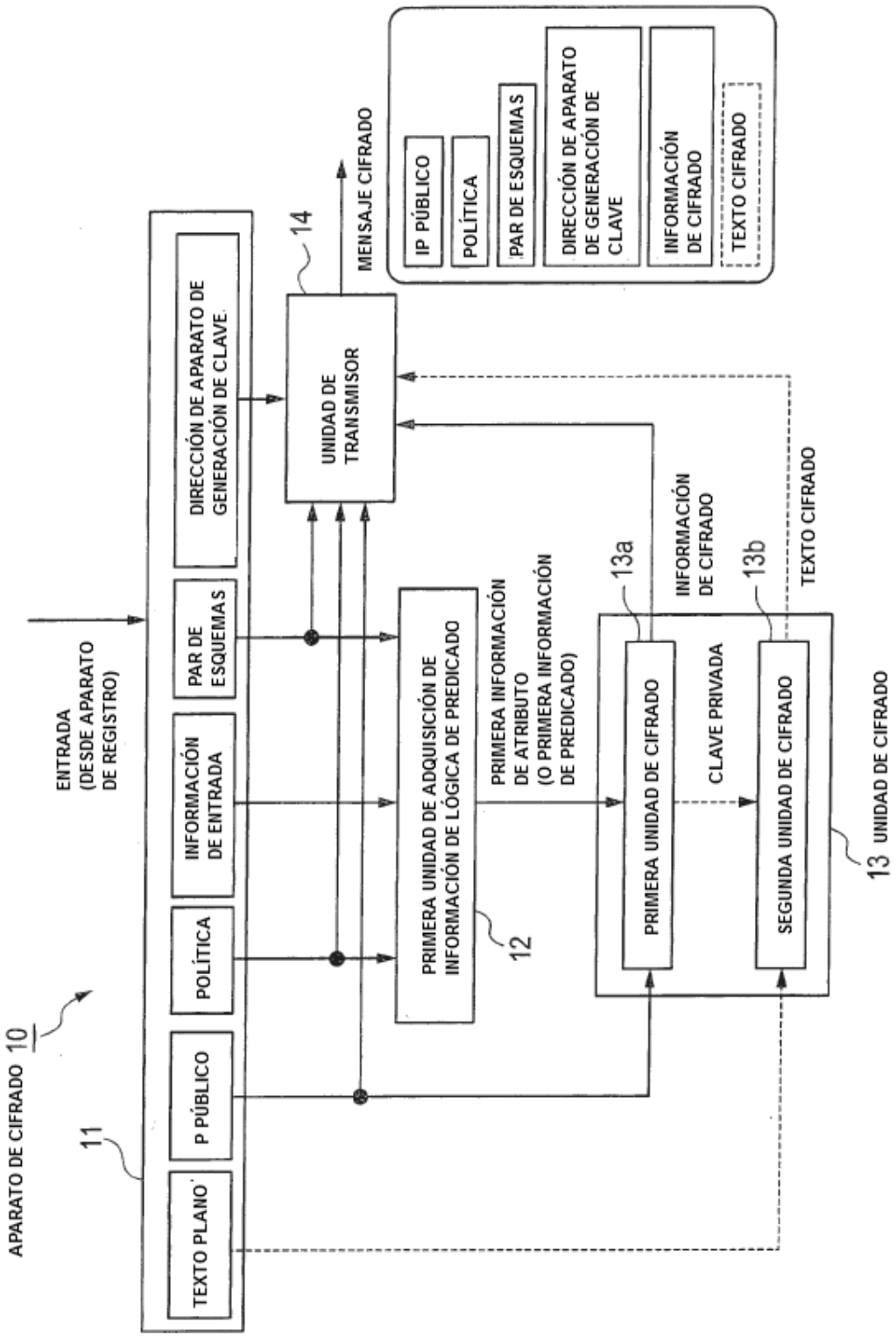

APARATO DE CIFRADO 10
11
TEXTO PLANO
P PÚBLICO
POLÍTICA
INFORMACIÓN DE ENTRADA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
ENTRADA (DESDE APARATO DE REGISTRO)
UNIDAD DE TRANSMISOR
14
MENSAJE CIFRADO
IP PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
INFORMACIÓN DE CIFRADO
TEXTO CIFRADO
PRIMERA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
12
PRIMERA INFORMACIÓN DE ATRIBUTO (O PRIMERA INFORMACIÓN DE PREDICADO)
13a
PRIMERA UNIDAD DE CIFRADO
CLAVE PRIVADA
13b
SEGUNDA UNIDAD DE CIFRADO
INFORMACIÓN DE CIFRADO
TEXTO CIFRADO
13 UNIDAD DE CIFRADO

FIG.6

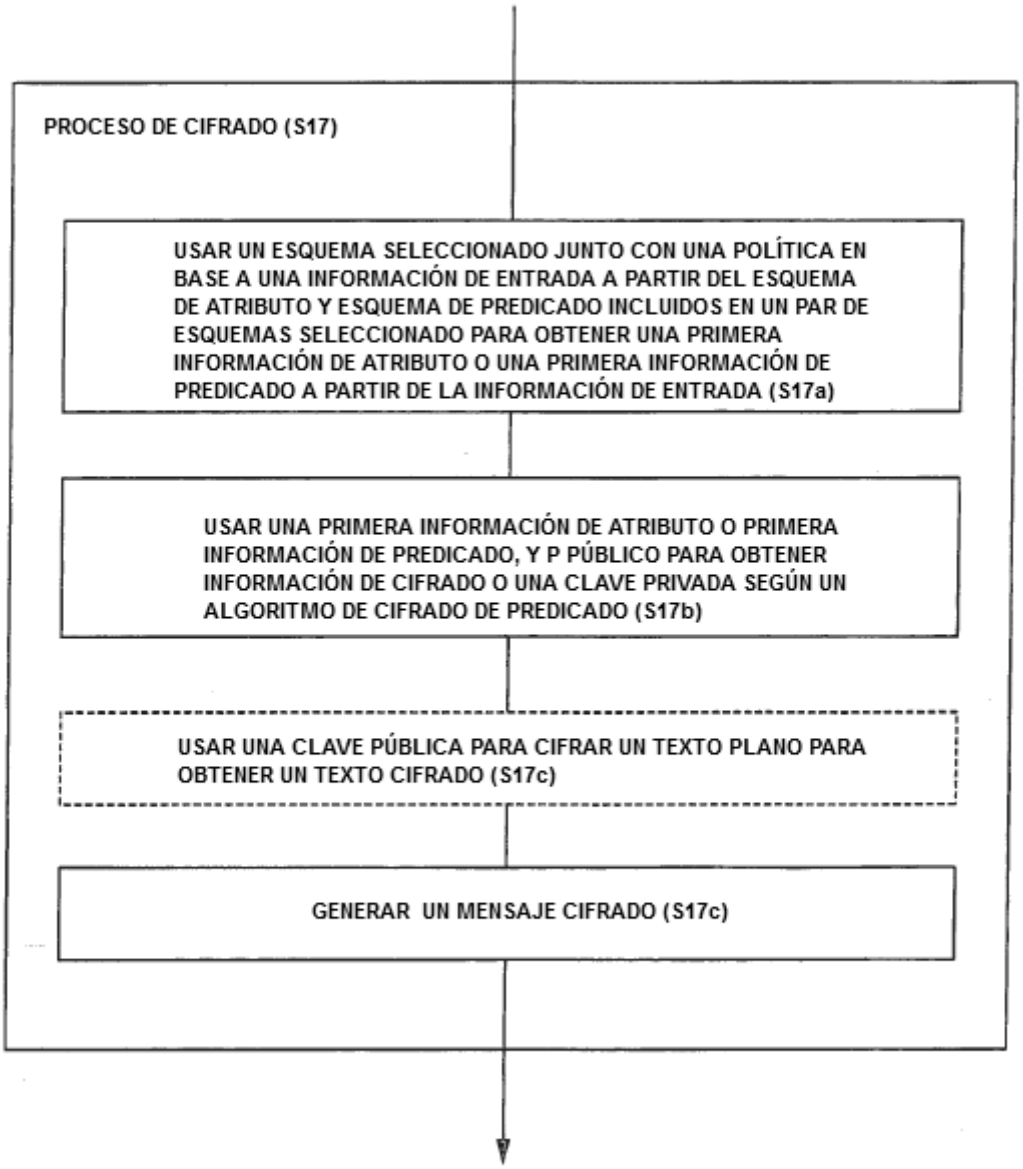

PROCESO DE CIFRADO (S17)
USAR UN ESQUEMA SELECCIONADO JUNTO CON UNA POLÍTICA EN BASE A UNA INFORMACIÓN DE ENTRADA A PARTIR DEL ESQUEMA DE ATRIBUTO Y ESQUEMA DE PREDICADO INCLUIDOS EN UN PAR DE ESQUEMAS SELECCIONADO PARA OBTENER UNA PRIMERA INFORMACIÓN DE ATRIBUTO O UNA PRIMERA INFORMACIÓN DE PREDICADO A PARTIR DE LA INFORMACIÓN DE ENTRADA (S17a)
USAR UNA PRIMERA INFORMACIÓN DE ATRIBUTO O PRIMERA INFORMACIÓN DE PREDICADO, Y P PÚBLICO PARA OBTENER INFORMACIÓN DE CIFRADO O UNA CLAVE PRIVADA SEGÚN UN ALGORITMO DE CIFRADO DE PREDICADO (S17b)
USAR UNA CLAVE PÚBLICA PARA CIFRAR UN TEXTO PLANO PARA OBTENER UN TEXTO CIFRADO (S17c)
GENERAR UN MENSAJE CIFRADO (S17c)

FIG.7

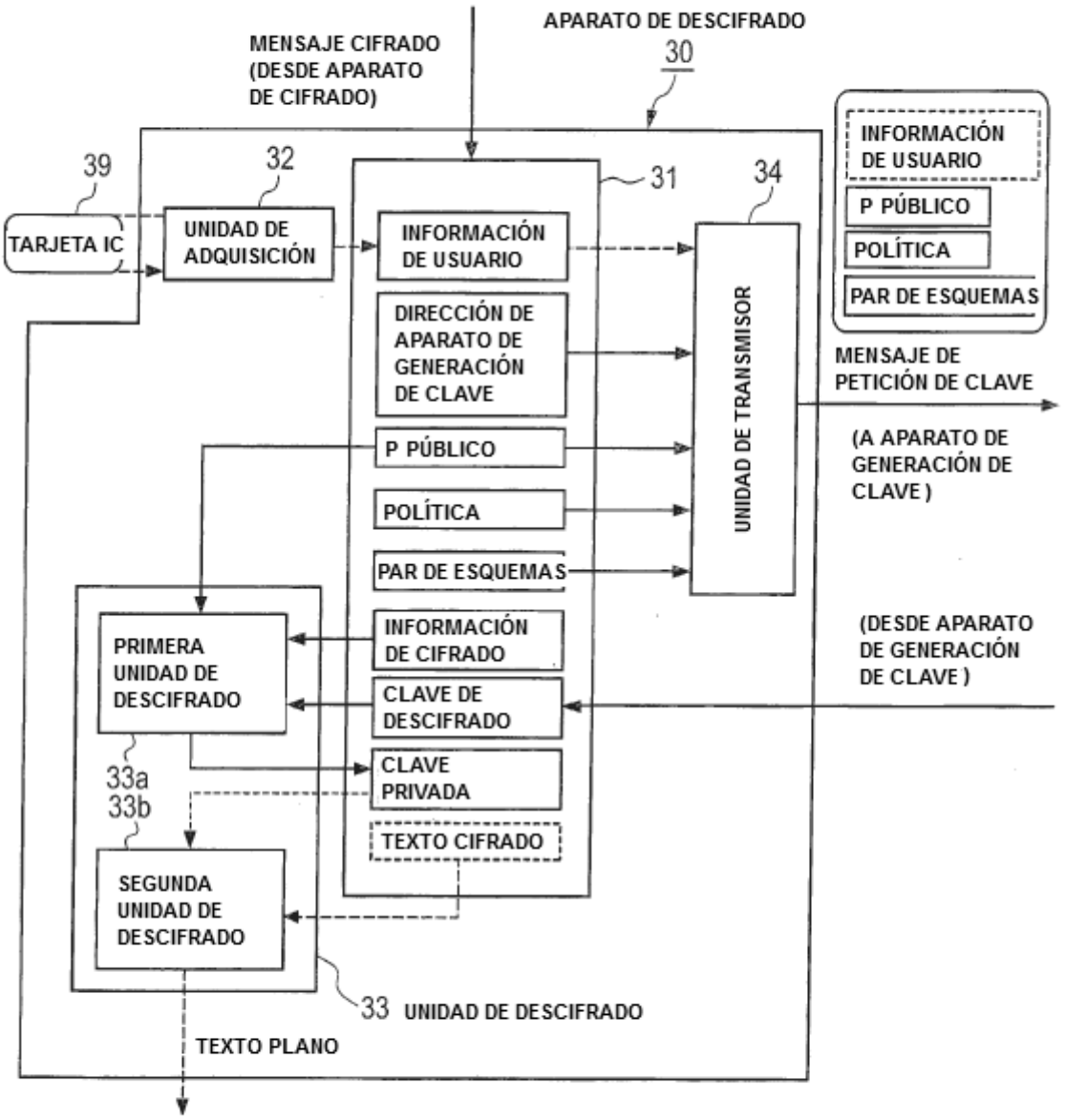

MENSAJE CIFRADO
(DESDE APARATO
DE CIFRADO)
APARATO DE DESCIFRADO
30
39
32
31
34
TARJETA IC
UNIDAD DE
ADQUISICIÓN
INFORMACIÓN
DE USUARIO
DIRECCIÓN DE
APARATO DE
GENERACIÓN
DE CLAVE
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
UNIDAD DE TRANSMISOR
INFORMACIÓN
DE USUARIO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
MENSAJE DE
PETICIÓN DE CLAVE
(A APARATO DE
GENERACIÓN DE
CLAVE)
(DESDE APARATO
DE GENERACIÓN
DE CLAVE)
PRIMERA
UNIDAD DE
DESCIFRADO
INFORMACIÓN
DE CIFRADO
CLAVE DE
DESCIFRADO
CLAVE
PRIVADA
TEXTO CIFRADO
33a
33b
SEGUNDA
UNIDAD DE
DESCIFRADO
33 UNIDAD DE DESCIFRADO
TEXTO PLANO

FIG.8

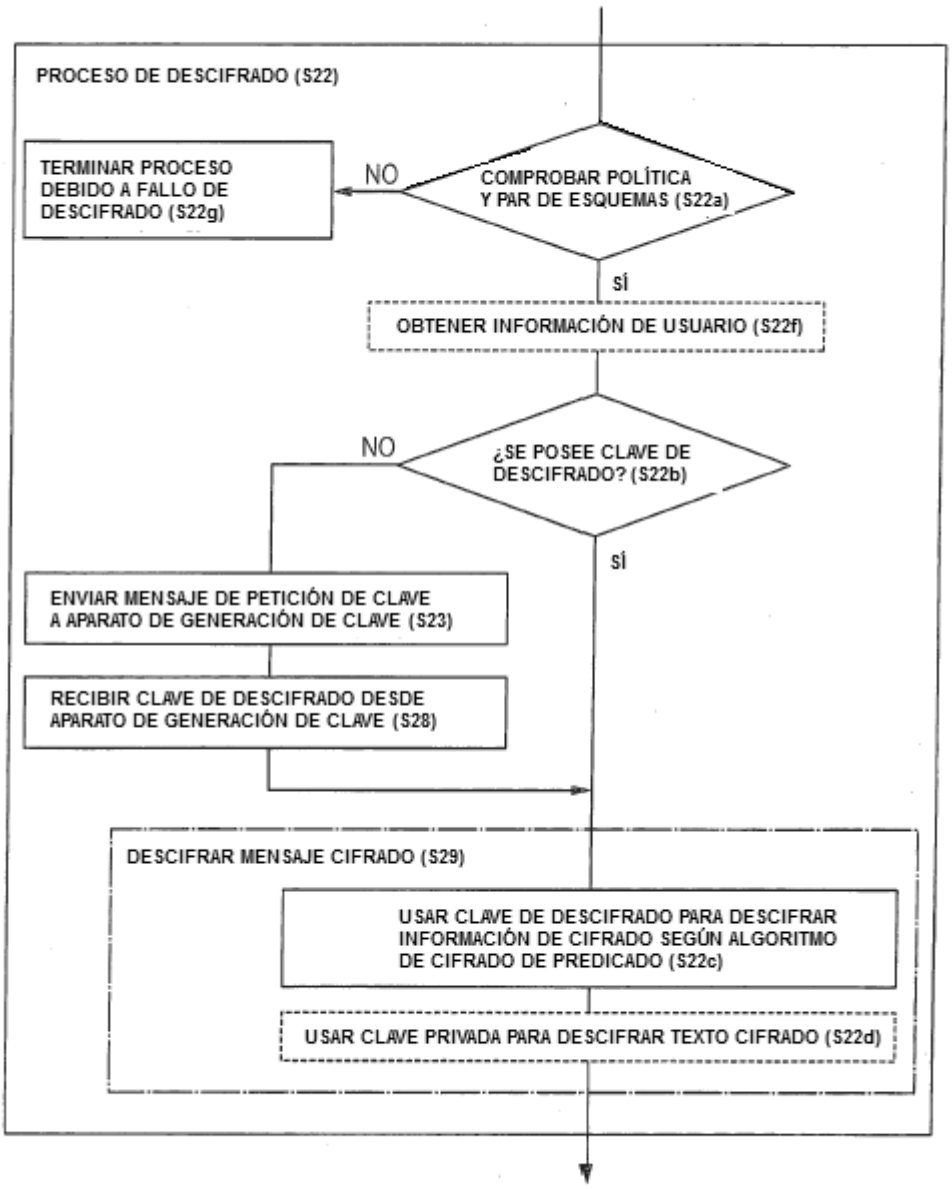

PROCESO DE DESCIFRADO (S22)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S22g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S22a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S22f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S22b)
SÍ
ENVIAR MENSAJE DE PETICIÓN DE CLAVE A APARATO DE GENERACIÓN DE CLAVE (S23)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACIÓN DE CLAVE (S28)
DESCIFRAR MENSAJE CIFRADO (S29)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGÚN ALGORITMO DE CIFRADO DE PREDICADO (S22c)
USAR CLAVE PRIVADA PARA DESCIFRAR TEXTO CIFRADO (S22d)

FIG.9

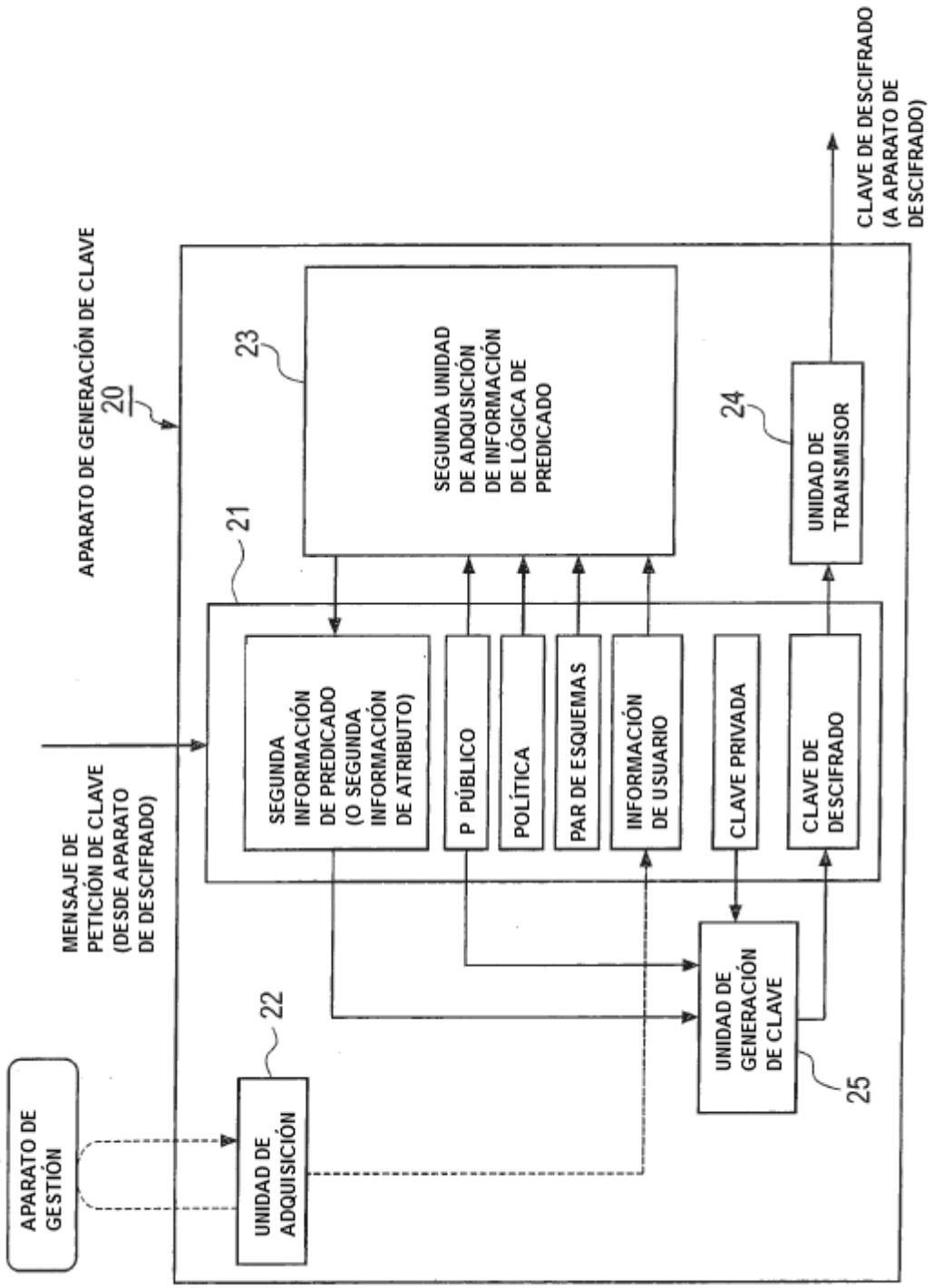
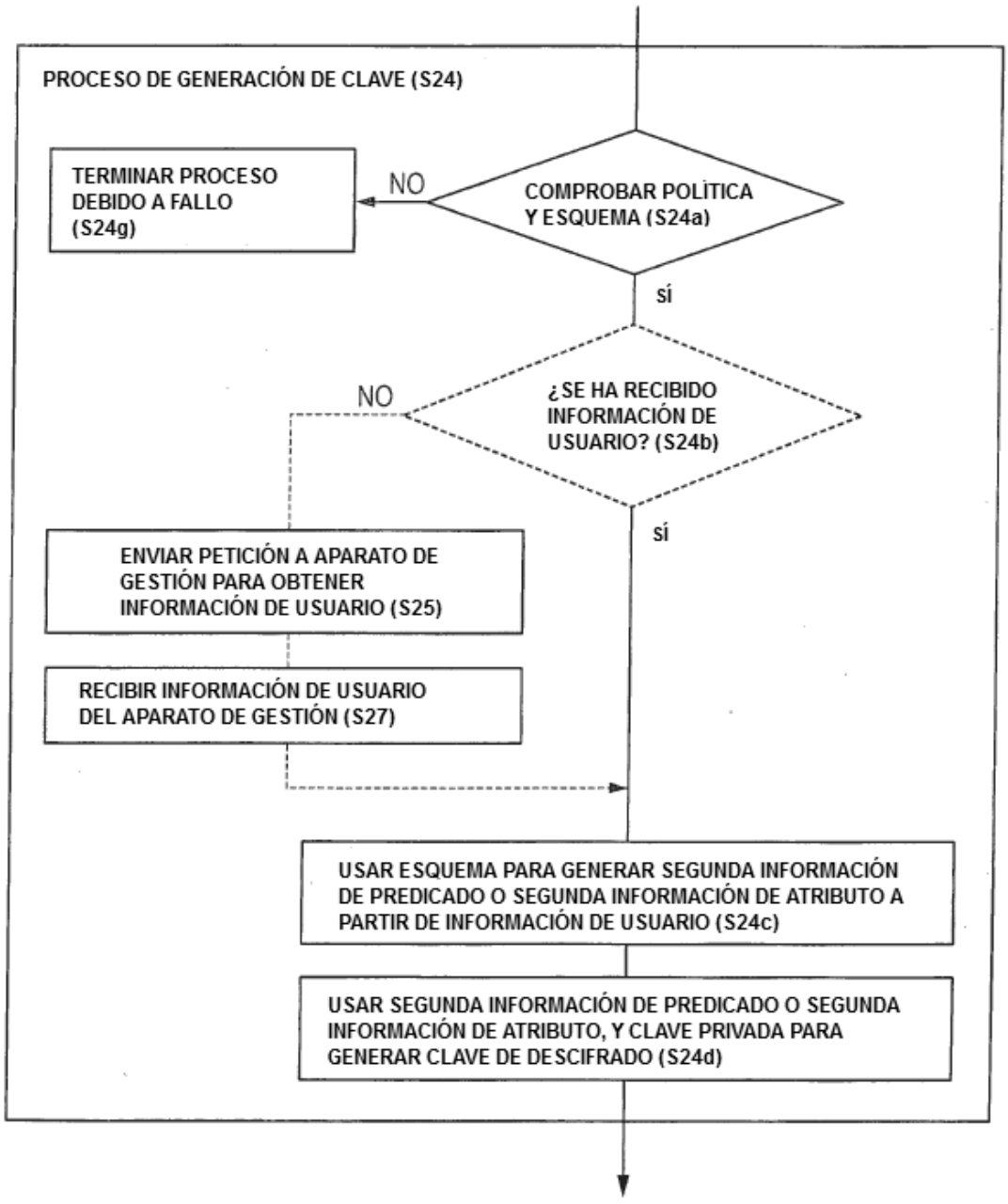

APARATO DE GESTIÓN
MENSAJE DE PETICIÓN DE CLAVE (DESDE APARATO DE DESCIFRADO)
APARATO DE GENERACIÓN DE CLAVE
20
21
22
23
24
25
UNIDAD DE ADQUISICIÓN
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
INFORMACIÓN DE USUARIO
CLAVE PRIVADA
CLAVE DE DESCIFRADO
SEGUNDA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
UNIDAD DE GENERACIÓN DE CLAVE
UNIDAD DE TRANSMISOR
CLAVE DE DESCIFRADO (A APARATO DE DESCIFRADO)

FIG.10


PROCESO DE GENERACIÓN DE CLAVE (S24)
COMPROBAR POLÍTICA Y ESQUEMA (S24a)
NO
TERMINAR PROCESO DEBIDO A FALLO (S24g)
SÍ
¿SE HA RECIBIDO INFORMACIÓN DE USUARIO? (S24b)
NO
SÍ
ENVIAR PETICIÓN A APARATO DE GESTIÓN PARA OBTENER INFORMACIÓN DE USUARIO (S25)
RECIBIR INFORMACIÓN DE USUARIO DEL APARATO DE GESTIÓN (S27)
USAR ESQUEMA PARA GENERAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO A PARTIR DE INFORMACIÓN DE USUARIO (S24c)
USAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO, Y CLAVE PRIVADA PARA GENERAR CLAVE DE DESCIFRADO (S24d)

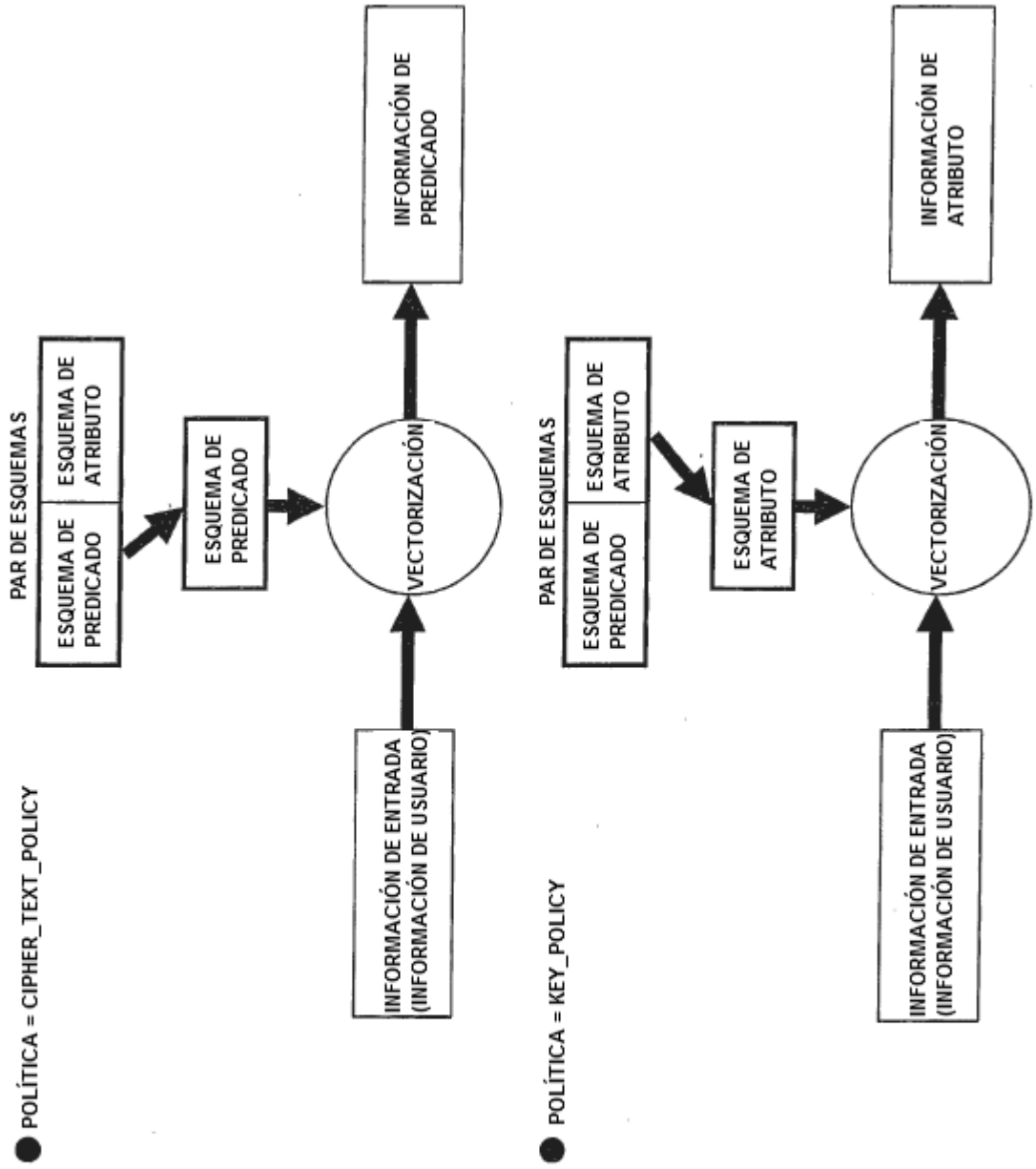

POLÍTICA = CIPHER_TEXT_POLICY
PAR DE ESQUEMAS
ESQUEMA DE PREDICADO
ESQUEMA DE ATRIBUTO
ESQUEMA DE PREDICADO
VECTORIZACIÓN
INFORMACIÓN DE PREDICADO
INFORMACIÓN DE ENTRADA (INFORMACIÓN DE USUARIO)
POLÍTICA = KEY_POLICY
PAR DE ESQUEMAS
ESQUEMA DE PREDICADO
ESQUEMA DE ATRIBUTO
ESQUEMA DE ATRIBUTO
VECTORIZACIÓN
INFORMACIÓN DE ATRIBUTO
INFORMACIÓN DE ENTRADA (INFORMACIÓN DE USUARIO)

FIG.11

FIG.12

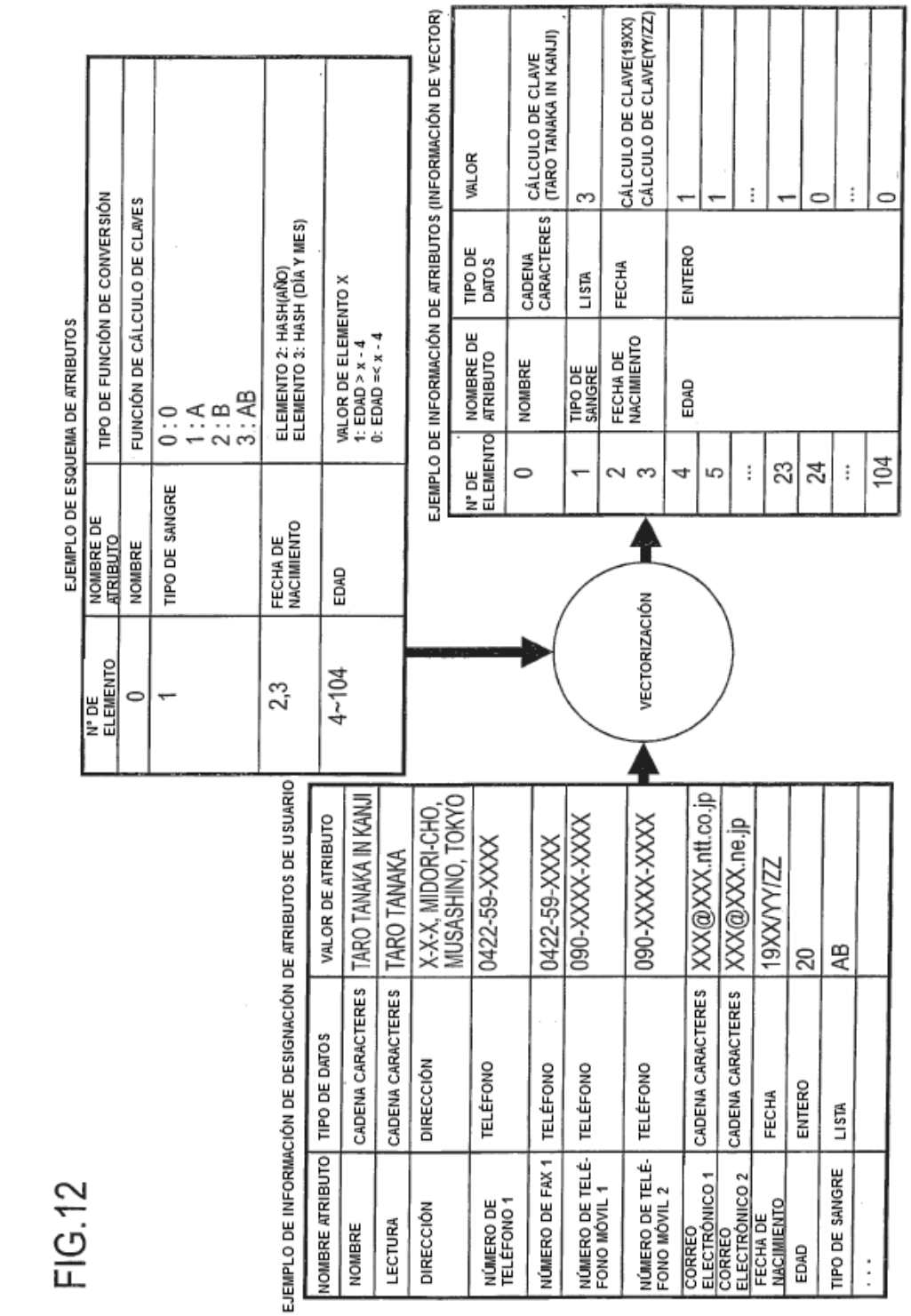

EJEMPLO DE ESQUEMA DE ATRIBUTOS
Nº DE ELEMENTO
NOMBRE DE ATRIBUTO
TIPO DE FUNCIÓN DE CONVERSIÓN
0
NOMBRE
FUNCIÓN DE CÁLCULO DE CLAVES
1
TIPO DE SANGRE
0 : 0
1 : A
2 : B
3 : AB
2,3
FECHA DE NACIMIENTO
ELEMENTO 2: HASH(AÑO)
ELEMENTO 3: HASH (DÍA Y MES)
4~104
EDAD
VALOR DE ELEMENTO X
1: EDAD > x - 4
0: EDAD =< x - 4
EJEMPLO DE INFORMACIÓN DE DESIGNACIÓN DE ATRIBUTOS DE USUARIO
NOMBRE ATRIBUTO
TIPO DE DATOS
VALOR DE ATRIBUTO
NOMBRE
CADENA CARACTERES
TARO TANAKA IN KANJI
LECTURA
CADENA CARACTERES
TARO TANAKA
DIRECCIÓN
DIRECCIÓN
X-X-X, MIDORI-CHO, MUSASHINO, TOKYO
NÚMERO DE TELÉFONO 1
TELÉFONO
0422-59-XXXX
NÚMERO DE FAX 1
TELÉFONO
0422-59-XXXX
NÚMERO DE TELÉFONO MÓVIL 1
TELÉFONO
090-XXXX-XXXX
NÚMERO DE TELÉFONO MÓVIL 2
TELÉFONO
090-XXXX-XXXX
CORREO ELECTRÓNICO 1
CADENA CARACTERES
XXX@XXX.ntt.co.jp
CORREO ELECTRÓNICO 2
CADENA CARACTERES
XXX@XXX.ne.jp
FECHA DE NACIMIENTO
FECHA
19XX/YY/ZZ
EDAD
ENTERO
20
TIPO DE SANGRE
LISTA
AB
VECTORIZACIÓN
EJEMPLO DE INFORMACIÓN DE ATRIBUTOS (INFORMACIÓN DE VECTOR)
Nº DE ELEMENTO
NOMBRE DE ATRIBUTO
TIPO DE DATOS
VALOR
0
NOMBRE
CADENA CARACTERES
CÁLCULO DE CLAVE (TARO TANAKA IN KANJI)
1
TIPO DE SANGRE
LISTA
3
2
FECHA DE NACIMIENTO
FECHA
CÁLCULO DE CLAVE(19XX) CÁLCULO DE CLAVE(YY/ZZ)
3
4
EDAD
ENTERO
1
5
1
...
...
23
1
24
0
...
...
104
0

FIG.13

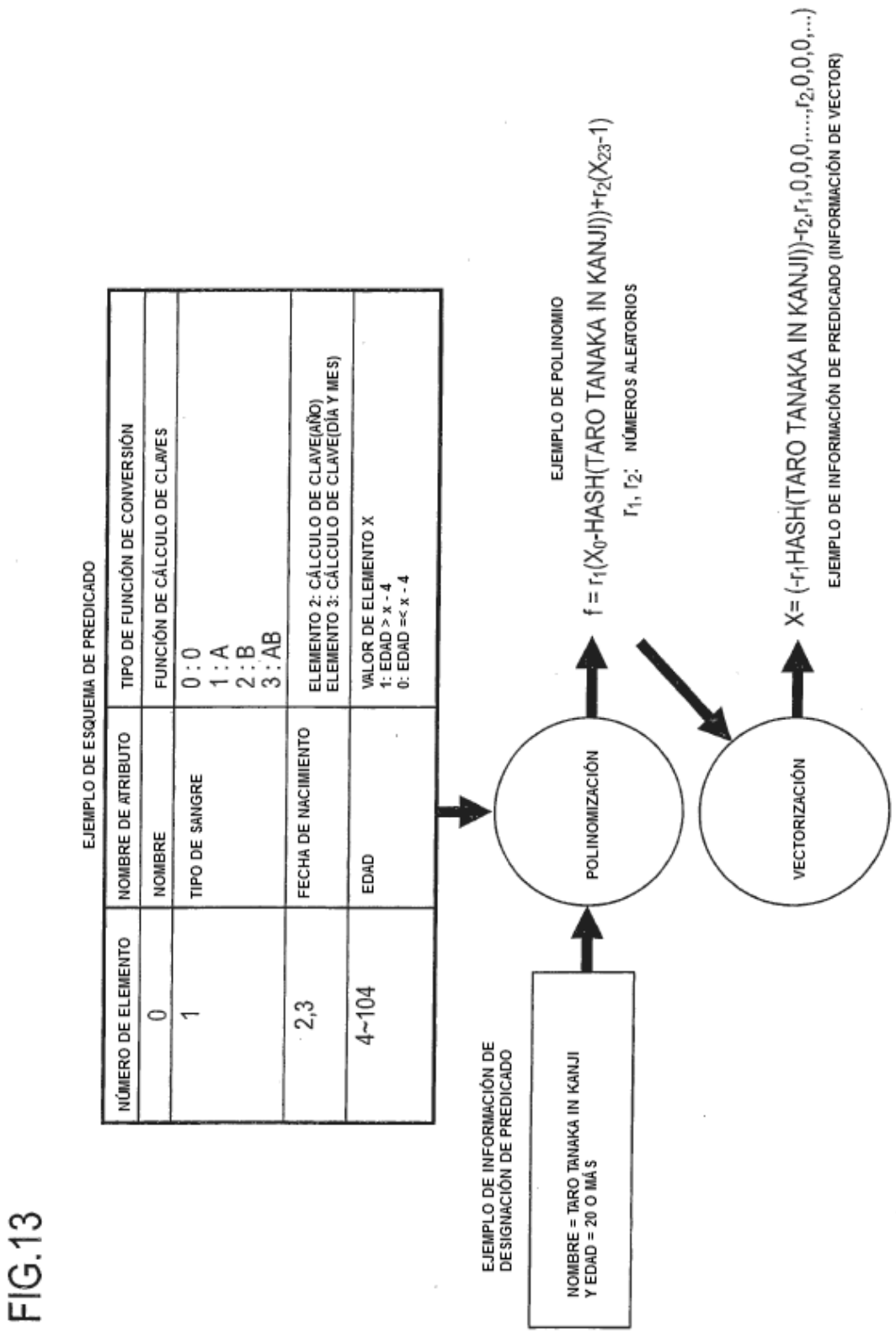

EJEMPLO DE ESQUEMA DE PREDICADO
NÚMERO DE ELEMENTO
NOMBRE DE ATRIBUTO
TIPO DE FUNCIÓN DE CONVERSIÓN
0
NOMBRE
FUNCIÓN DE CÁLCULO DE CLAVES
1
TIPO DE SANGRE
0 : 0
1 : A
2 : B
3 : AB
2,3
FECHA DE NACIMIENTO
ELEMENTO 2: CÁLCULO DE CLAVE(AÑO)
ELEMENTO 3: CÁLCULO DE CLAVE(DÍA Y MES)
4~104
EDAD
VALOR DE ELEMENTO X
1: EDAD > x - 4
0: EDAD =< x - 4
EJEMPLO DE INFORMACIÓN DE DESIGNACIÓN DE PREDICADO
NOMBRE = TARO TANAKA IN KANJI
Y EDAD = 20 O MÁS
POLINOMIZACIÓN
EJEMPLO DE POLINOMIO
f = r1(X0-HASH(TARO TANAKA IN KANJI))+r2(X23-1)
r1, r2: NÚMEROS ALEATORIOS
VECTORIZACIÓN
X= (-r1HASH(TARO TANAKA IN KANJI))-r2,r1,0,0,0,...,r2,0,0,0,...)
EJEMPLO DE INFORMACIÓN DE PREDICADO (INFORMACIÓN DE VECTOR)

FIG.14

EJEMPLO: LISTA DE POLÍTICAS LIMITADAS A CIPHER_TEXT_POLICY

Nº DE ELEMENTO	POLÍTICA
1	CIPHER_TEXT_POLICY

EJEMPLO: LISTA DE POLÍTICAS LIMITADAS A KEY_POLICY

Nº DE ELEMENTO	POLÍTICA
1	KEY_POLICY

EJEMPLO: LISTA DE POLÍTICAS PARA CIPHER_TEXT_POLICY Y KEY_POLICY

Nº DE ELEMENTO	POLÍTICA
1	CIPHER_TEXT_POLICY
2	KEY_POLICY

FIG.15

IDENTIFICADOR DE APARATO DE GENERACIÓN DE CLAVE	PARÁMETRO PÚBLICO	PAR DE ESQUEMAS	OBJETIVO DE CLAVE DE DESCIFRADO	INFORMACIÓN DE DESIGNACIÓN DE PREDICADO	CLAVE DE DESCIFRADO
APARATO DE GENERACIÓN DE CLAVE 20-1	PARÁMETRO PÚBLICO 1	PAR DE ESQUEMAS 1			CLAVE DE DESCIFRADO 1
APARATO DE GENERACIÓN DE CLAVE 20-2	PARÁMETRO PÚBLICO 2	PAR DE ESQUEMAS 2			CLAVE DE DESCIFRADO 2
...	...	...			...
APARATO DE GENERACIÓN DE CLAVE 20-N	PARÁMETRO PÚBLICO N	PAR DE ESQUEMAS N			CLAVE DE DESCIFRADO N

FIG.16

ID DE USUARIO	CONTRASEÑA
USUARIO 1	CONTRASEÑA 1
USUARIO 2	CONTRASEÑA 2
...	...
USUARIO N	CONTRASEÑA N

FIG.17

ID DE USUARIO	NOMBRE DE ATRIBUTO	VALOR DE ATRIBUTO
USUARIO 1	NOMBRE DE ATRIBUTO 1	VALOR DE ATRIBUTO 1
USUARIO 2	NOMBRE DE ATRIBUTO 2	VALOR DE ATRIBUTO 2
...	...	...
USUARIO 1	NOMBRE DE ATRIBUTO N	VALOR DE ATRIBUTO N
...	...	...
USUARIO M	NOMBRE DE ATRIBUTO K	VALOR DE ATRIBUTO K
...	...	...

ID DE USUARIO	PREDICADO
USUARIO 1	PREDICADO 1
USUARIO 2	PREDICADO 2
...	...
USUARIO N	PREDICADO N

FIG.18

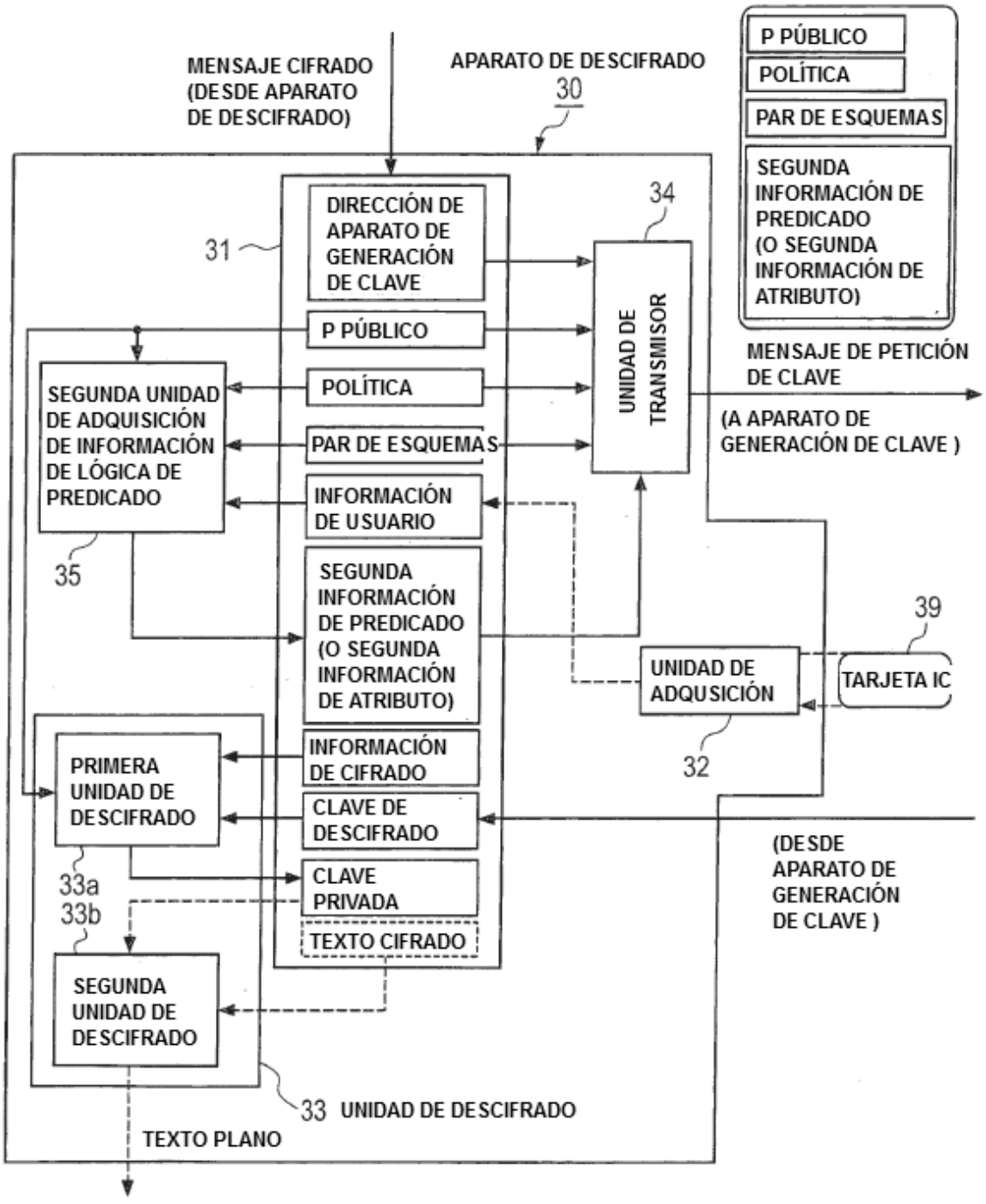

MENSAJE CIFRADO (DESDE APARATO DE DESCIFRADO)
APARATO DE DESCIFRADO
30
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
31
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
34
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
INFORMACIÓN DE USUARIO
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
UNIDAD DE TRANSMISOR
MENSAJE DE PETICIÓN DE CLAVE
(A APARATO DE GENERACIÓN DE CLAVE)
SEGUNDA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
35
39
UNIDAD DE ADQUISICIÓN
TARJETA IC
32
PRIMERA UNIDAD DE DESCIFRADO
INFORMACIÓN DE CIFRADO
CLAVE DE DESCIFRADO
CLAVE PRIVADA
TEXTO CIFRADO
(DESDE APARATO DE GENERACIÓN DE CLAVE)
33a
33b
SEGUNDA UNIDAD DE DESCIFRADO
33 UNIDAD DE DESCIFRADO
TEXTO PLANO

FIG.19

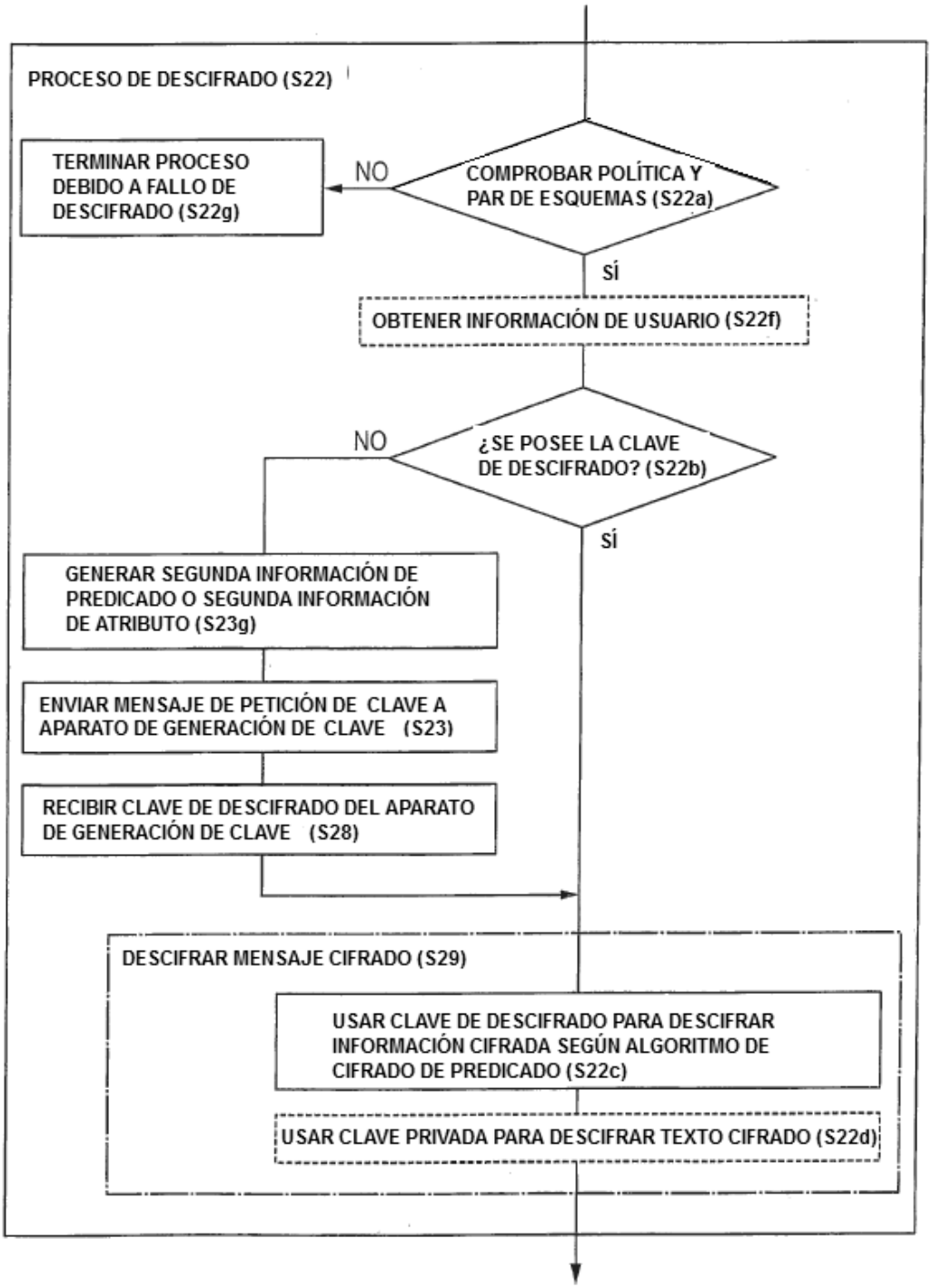

PROCESO DE DESCIFRADO (S22)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S22g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S22a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S22f)
NO
¿SE POSEE LA CLAVE DE DESCIFRADO? (S22b)
SÍ
GENERAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO (S23g)
ENVIAR MENSAJE DE PETICIÓN DE CLAVE A APARATO DE GENERACIÓN DE CLAVE (S23)
RECIBIR CLAVE DE DESCIFRADO DEL APARATO DE GENERACIÓN DE CLAVE (S28)
DESCIFRAR MENSAJE CIFRADO (S29)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN CIFRADA SEGÚN ALGORITMO DE CIFRADO DE PREDICADO (S22c)
USAR CLAVE PRIVADA PARA DESCIFRAR TEXTO CIFRADO (S22d)

FIG.20

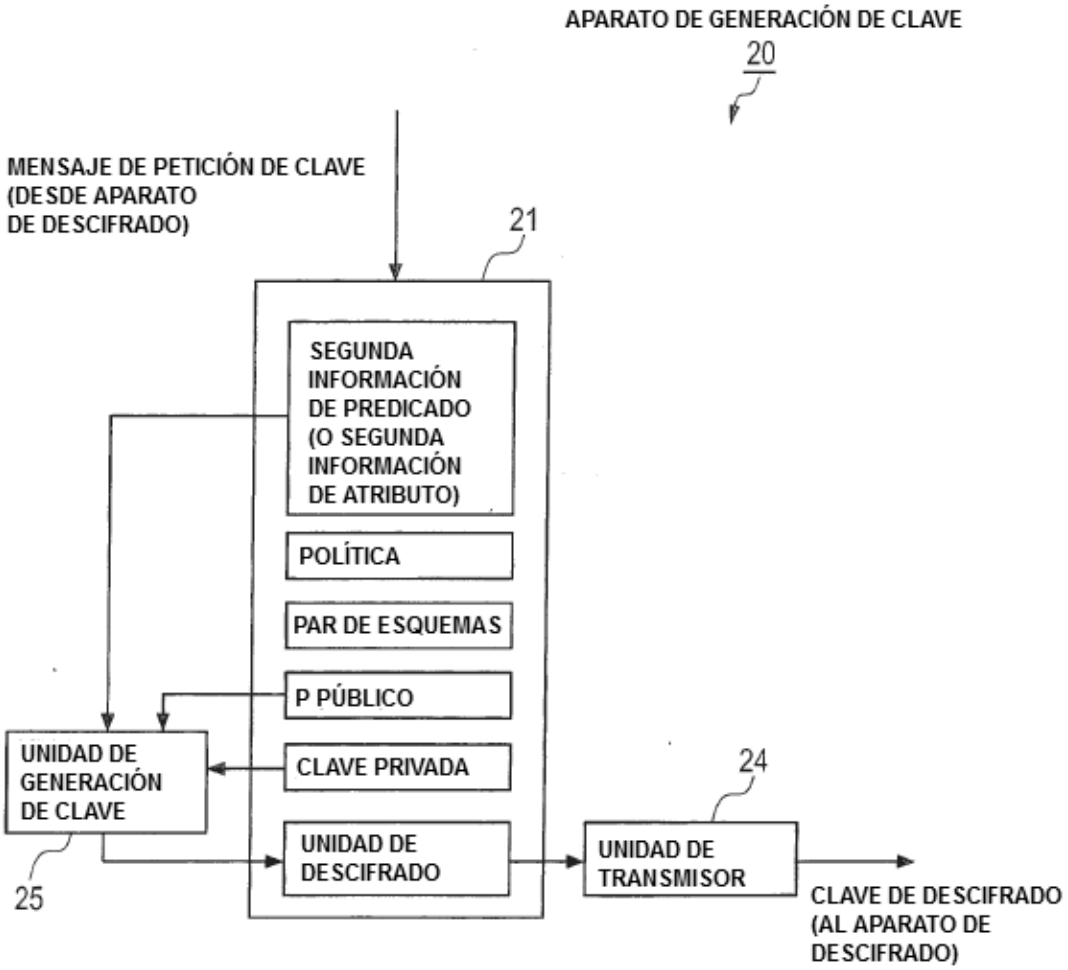

APARATO DE GENERACIÓN DE CLAVE
20
MENSAJE DE PETICIÓN DE CLAVE (DESDE APARATO DE DESCIFRADO)
21
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
POLÍTICA
PAR DE ESQUEMAS
P PÚBLICO
CLAVE PRIVADA
UNIDAD DE GENERACIÓN DE CLAVE
UNIDAD DE DESCIFRADO
24
UNIDAD DE TRANSMISOR
25
CLAVE DE DESCIFRADO (AL APARATO DE DESCIFRADO)

FIG.21

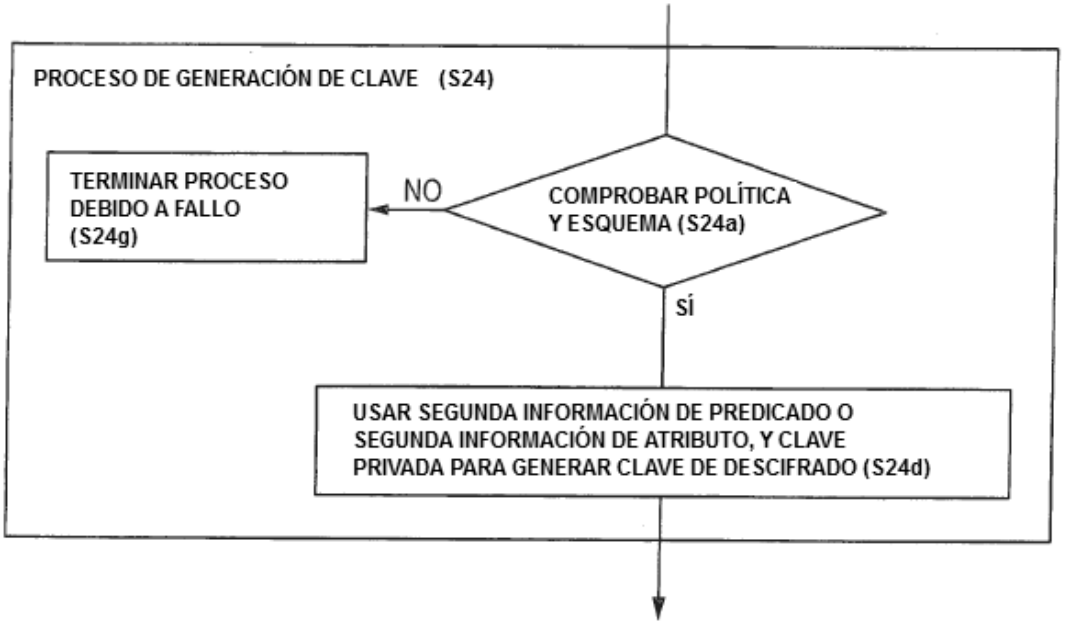

PROCESO DE GENERACIÓN DE CLAVE (S24)
TERMINAR PROCESO DEBIDO A FALLO (S24g)
NO
COMPROBAR POLÍTICA Y ESQUEMA (S24a)
SÍ
USAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO, Y CLAVE PRIVADA PARA GENERAR CLAVE DE DESCIFRADO (S24d)

FIG.22

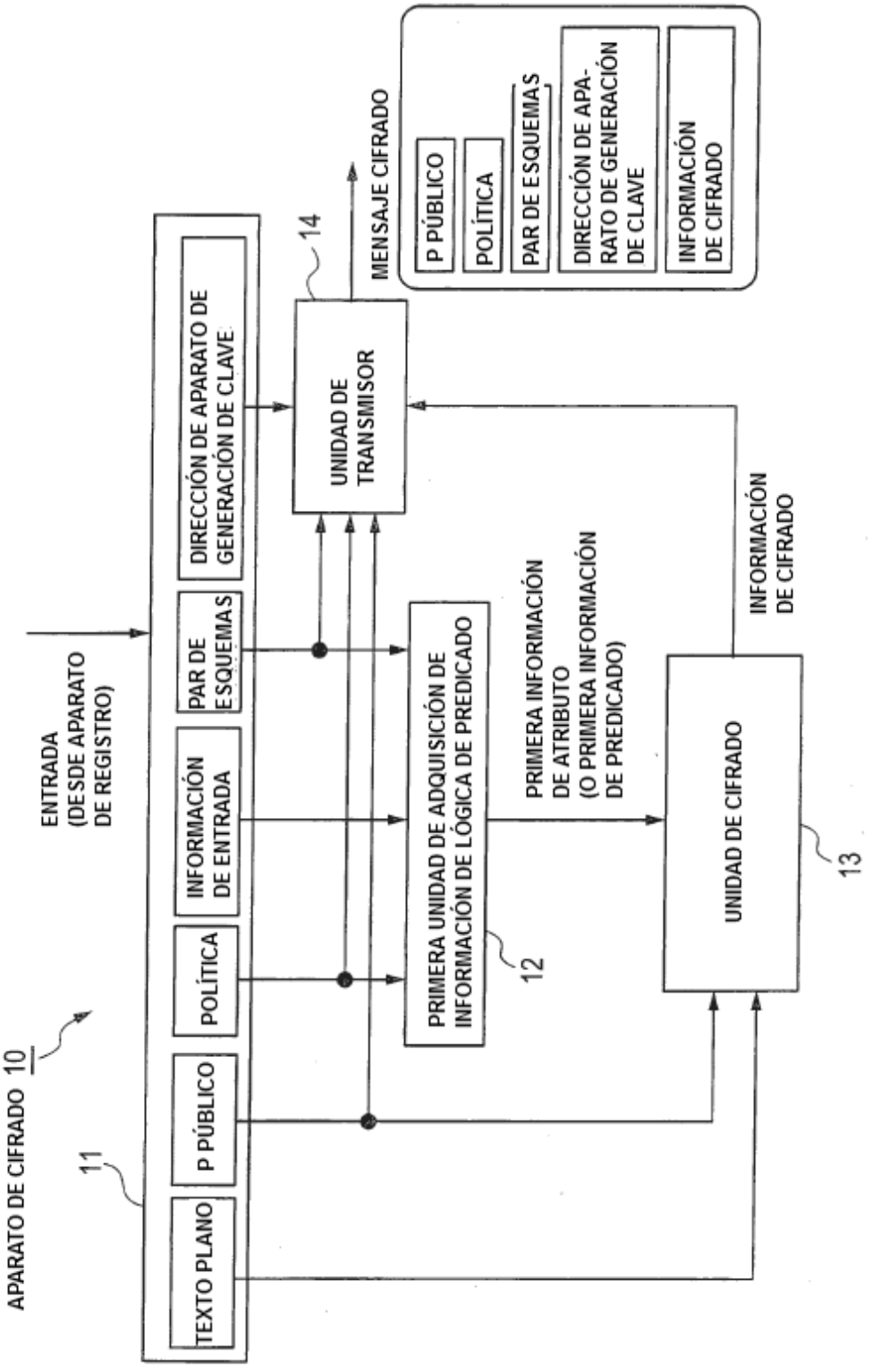

APARATO DE CIFRADO 10
11
TEXTO PLANO
P PÚBLICO
POLÍTICA
INFORMACIÓN DE ENTRADA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
ENTRADA (DESDE APARATO DE REGISTRO)
PRIMERA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
12
UNIDAD DE TRANSMISOR
14
MENSAJE CIFRADO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
INFORMACIÓN DE CIFRADO
PRIMERA INFORMACIÓN DE ATRIBUTO (O PRIMERA INFORMACIÓN DE PREDICADO)
UNIDAD DE CIFRADO
13
INFORMACIÓN DE CIFRADO

FIG.23

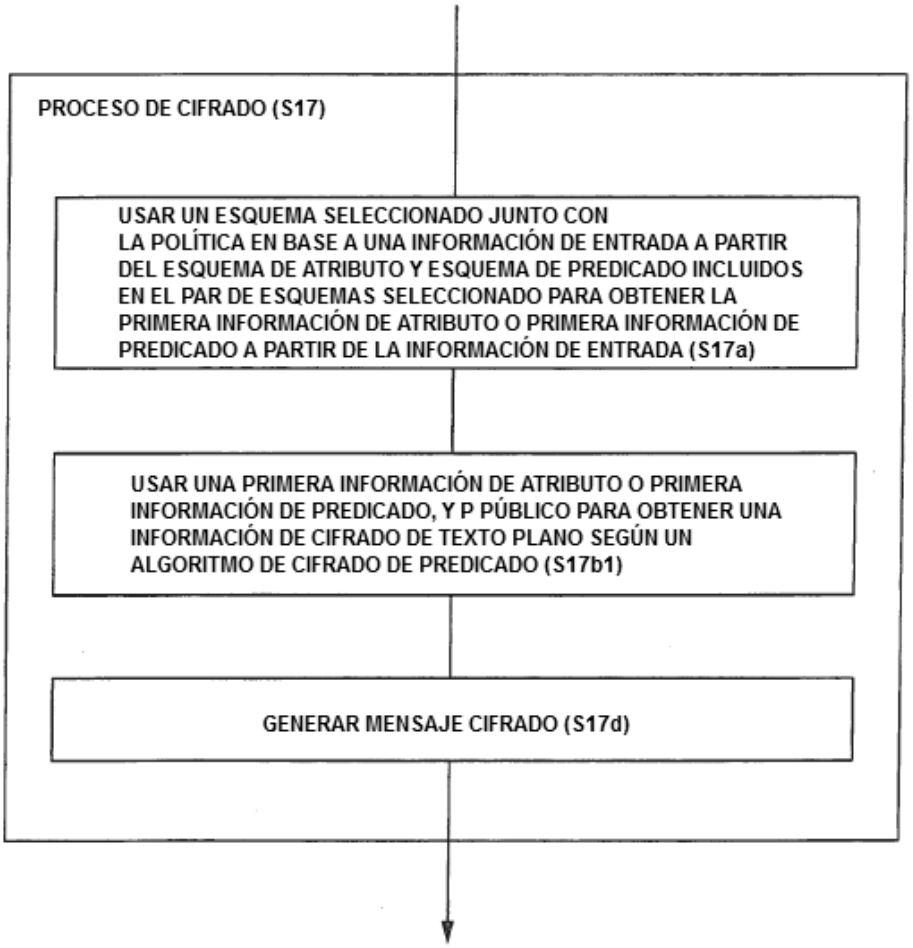

PROCESO DE CIFRADO (S17)
USAR UN ESQUEMA SELECCIONADO JUNTO CON LA POLÍTICA EN BASE A UNA INFORMACIÓN DE ENTRADA A PARTIR DEL ESQUEMA DE ATRIBUTO Y ESQUEMA DE PREDICADO INCLUIDOS EN EL PAR DE ESQUEMAS SELECCIONADO PARA OBTENER LA PRIMERA INFORMACIÓN DE ATRIBUTO O PRIMERA INFORMACIÓN DE PREDICADO A PARTIR DE LA INFORMACIÓN DE ENTRADA (S17a)
USAR UNA PRIMERA INFORMACIÓN DE ATRIBUTO O PRIMERA INFORMACIÓN DE PREDICADO, Y P PÚBLICO PARA OBTENER UNA INFORMACIÓN DE CIFRADO DE TEXTO PLANO SEGÚN UN ALGORITMO DE CIFRADO DE PREDICADO (S17b1)
GENERAR MENSAJE CIFRADO (S17d)

FIG.24

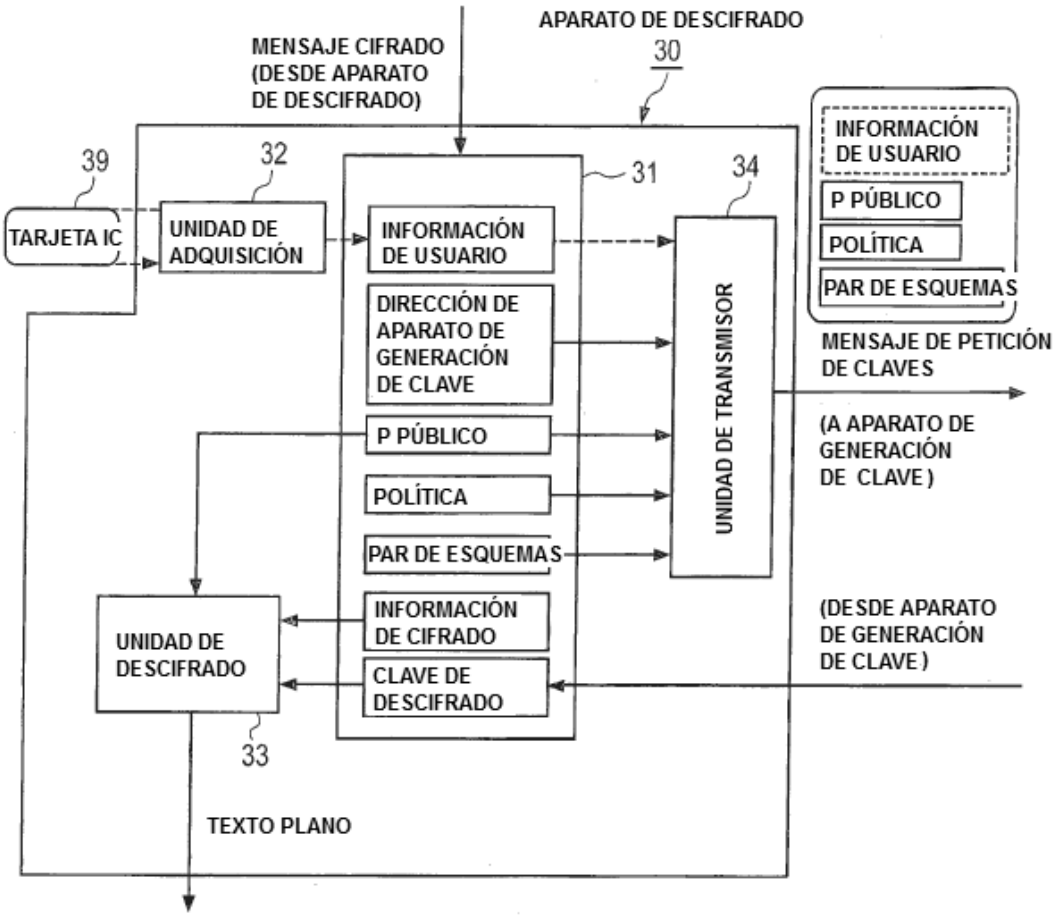

APARATO DE DESCIFRADO
30
MENSAJE CIFRADO (DESDE APARATO DE DESCIFRADO)
39
32
31
34
TARJETA IC
UNIDAD DE ADQUISICIÓN
INFORMACIÓN DE USUARIO
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
UNIDAD DE TRANSMISOR
INFORMACIÓN DE USUARIO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
MENSAJE DE PETICIÓN DE CLAVES
(A APARATO DE GENERACIÓN DE CLAVE)
(DESDE APARATO DE GENERACIÓN DE CLAVE)
INFORMACIÓN DE CIFRADO
CLAVE DE DESCIFRADO
UNIDAD DE DESCIFRADO
33
TEXTO PLANO

FIG.25

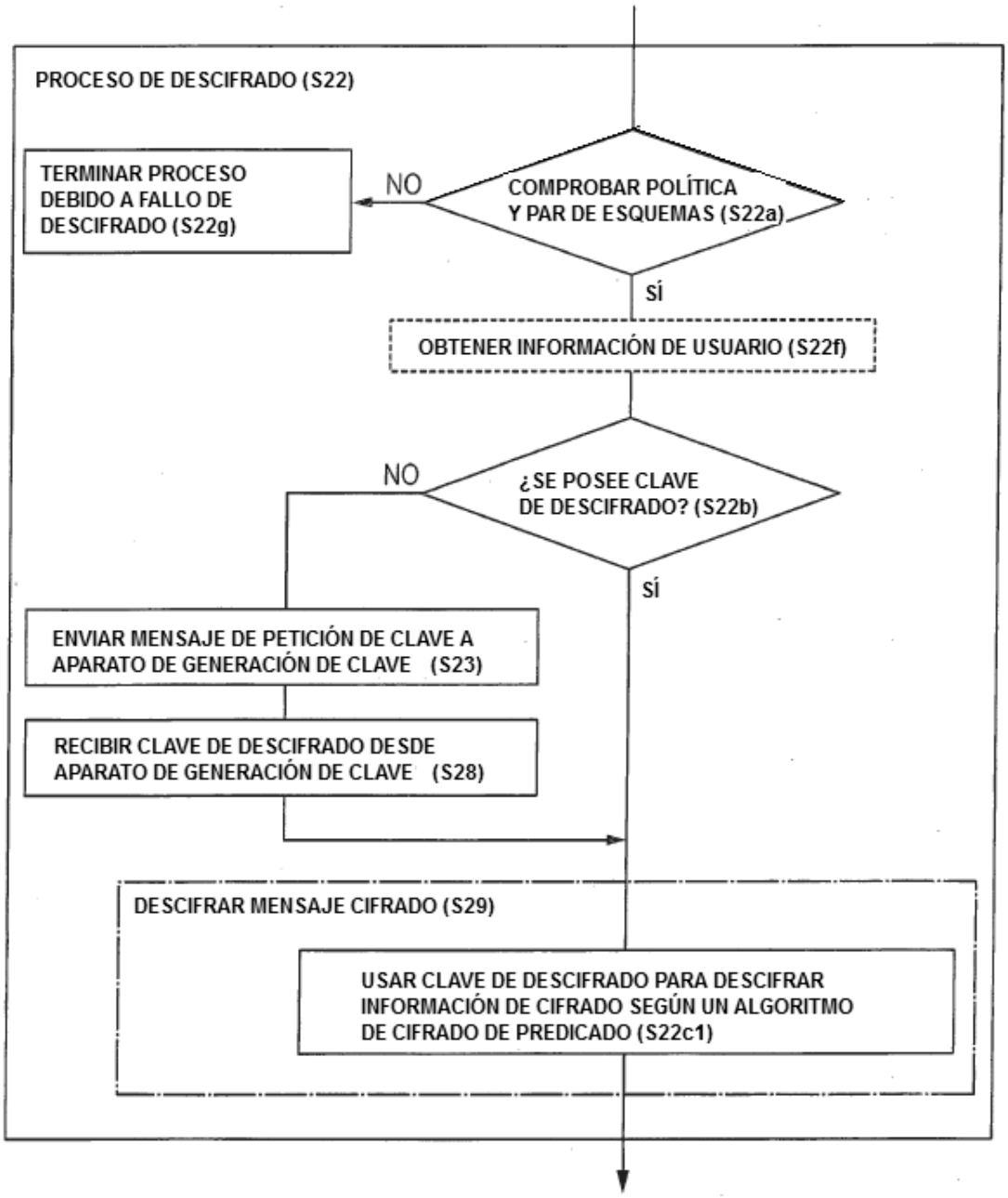

PROCESO DE DESCIFRADO (S22)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S22g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S22a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S22f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S22b)
SÍ
ENVIAR MENSAJE DE PETICIÓN DE CLAVE A APARATO DE GENERACIÓN DE CLAVE (S23)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACIÓN DE CLAVE (S28)
DESCIFRAR MENSAJE CIFRADO (S29)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGÚN UN ALGORITMO DE CIFRADO DE PREDICADO (S22c1)

FIG.26

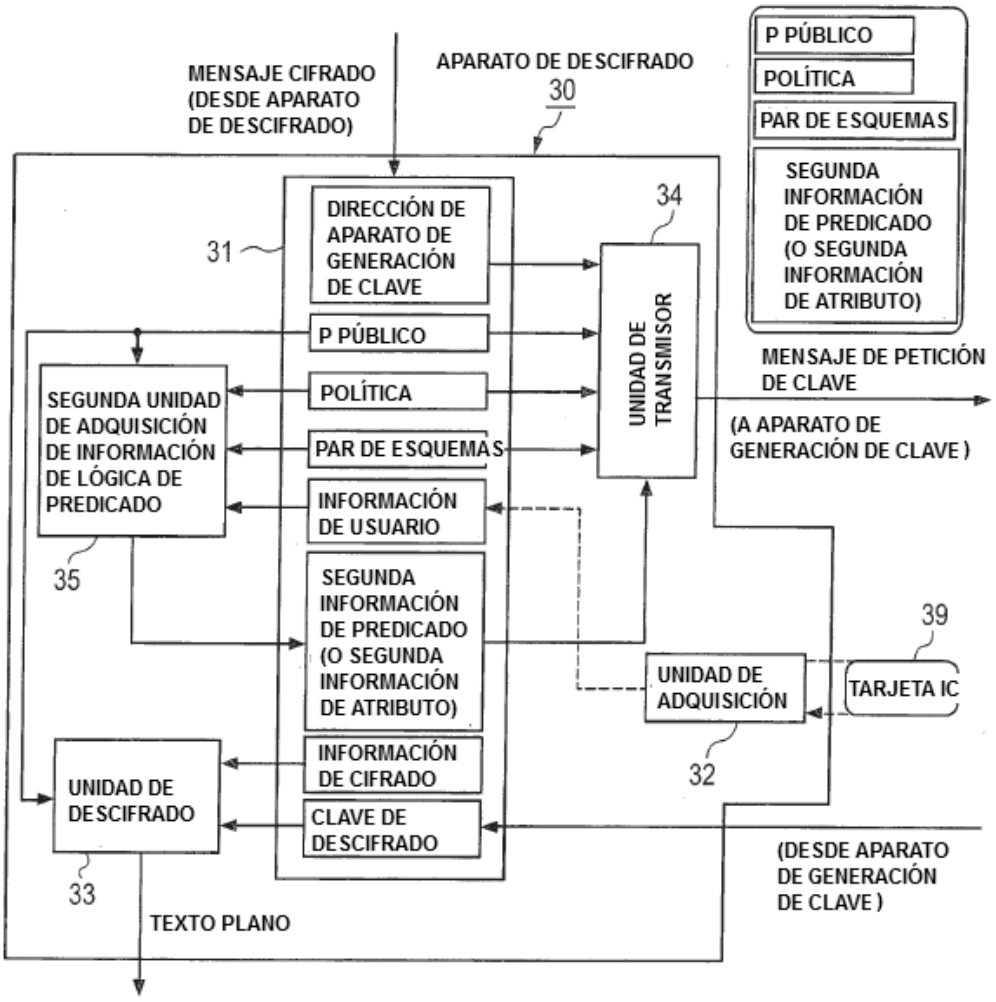

MENSAJE CIFRADO (DESDE APARATO DE DESCIFRADO)
APARATO DE DESCIFRADO
30
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
31
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
34
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
UNIDAD DE TRANSMISOR
MENSAJE DE PETICIÓN DE CLAVE
(A APARATO DE GENERACIÓN DE CLAVE)
SEGUNDA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
35
INFORMACIÓN DE USUARIO
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
39
UNIDAD DE ADQUISICIÓN
TARJETA IC
32
INFORMACIÓN DE CIFRADO
UNIDAD DE DESCIFRADO
CLAVE DE DESCIFRADO
(DESDE APARATO DE GENERACIÓN DE CLAVE)
33
TEXTO PLANO

FIG.27

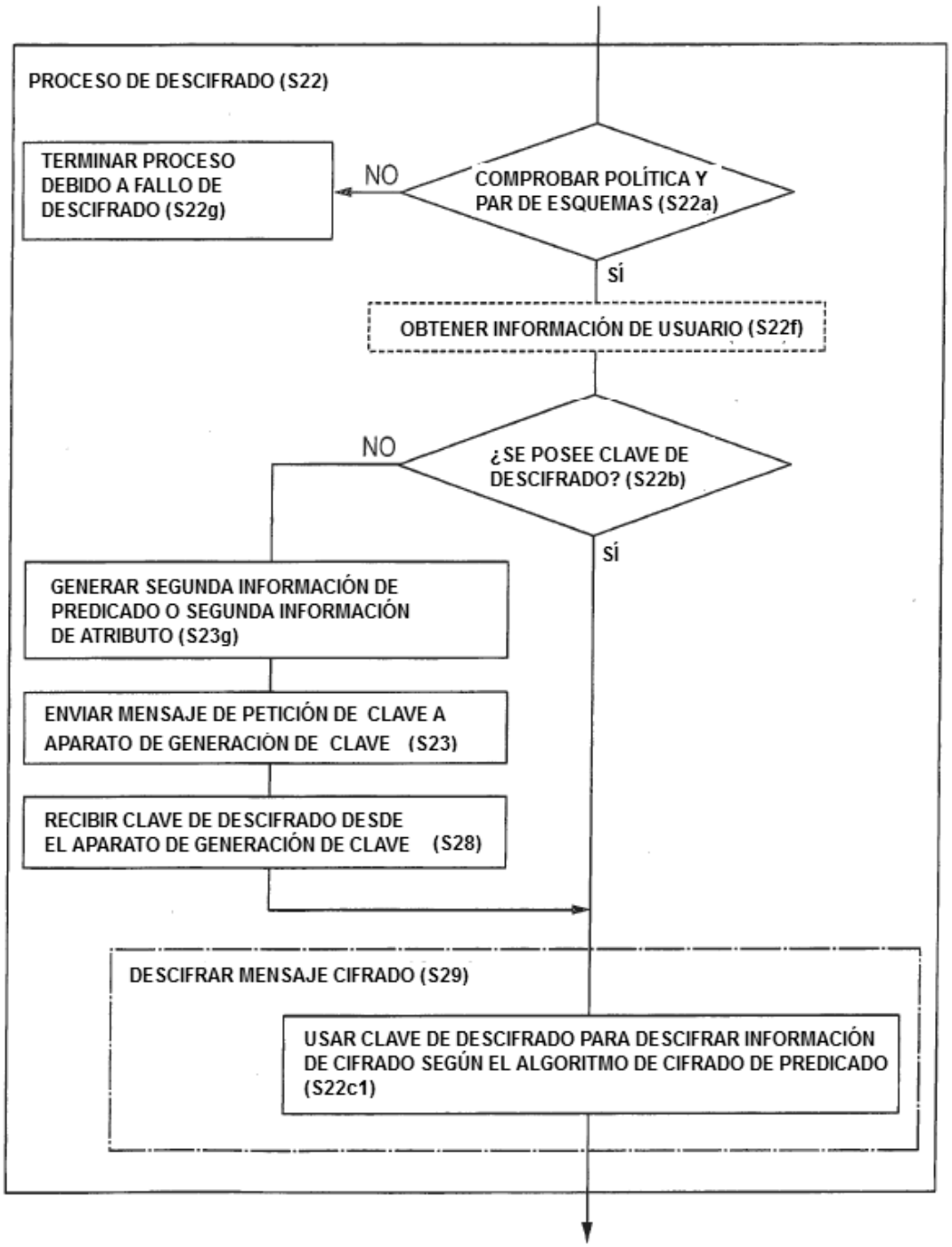

PROCESO DE DESCIFRADO (S22)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S22g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S22a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S22f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S22b)
SÍ
GENERAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO (S23g)
ENVIAR MENSAJE DE PETICIÓN DE CLAVE A APARATO DE GENERACIÓN DE CLAVE (S23)
RECIBIR CLAVE DE DESCIFRADO DESDE EL APARATO DE GENERACIÓN DE CLAVE (S28)
DESCIFRAR MENSAJE CIFRADO (S29)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGÚN EL ALGORITMO DE CIFRADO DE PREDICADO (S22c1)

FIG.28

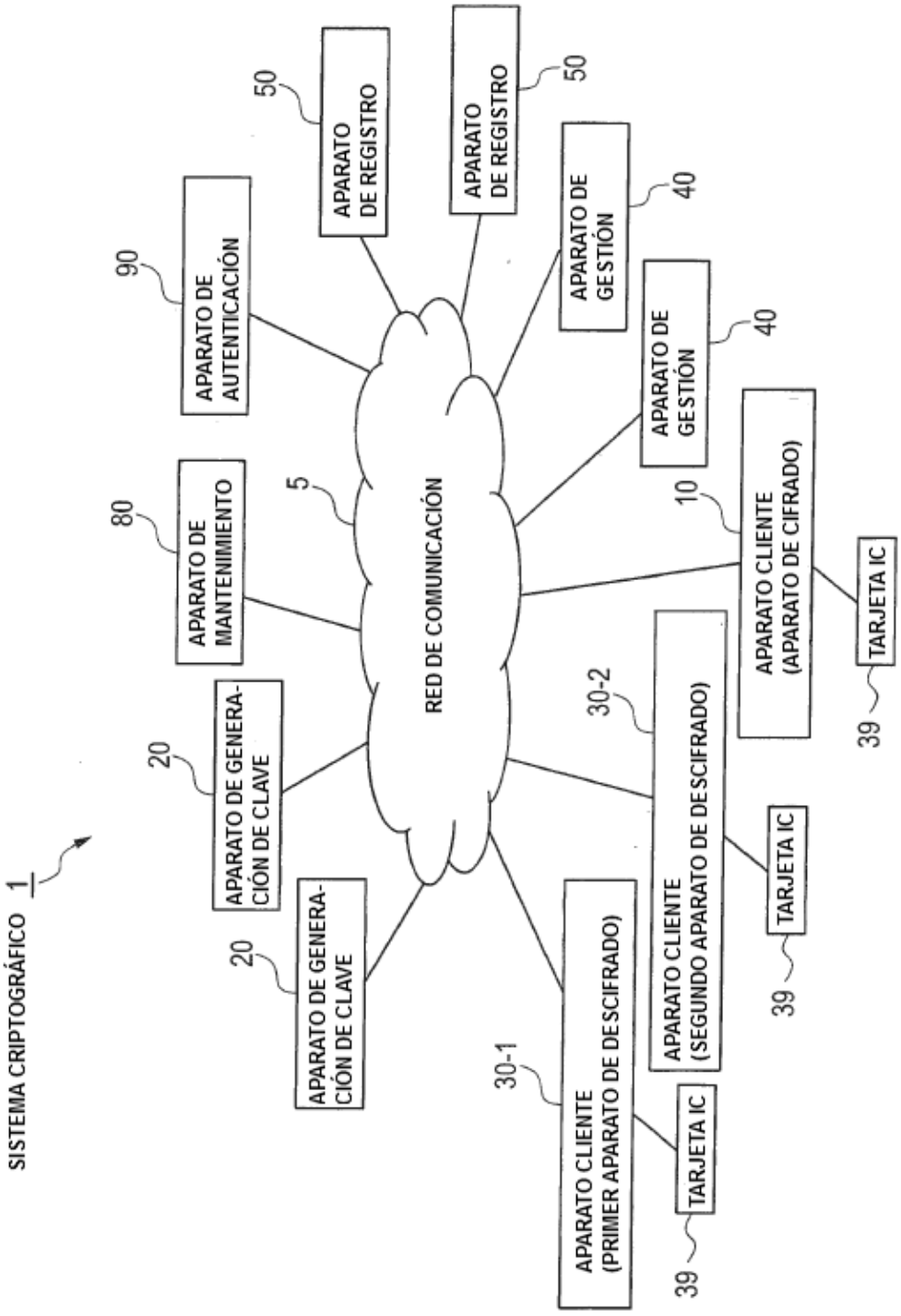

SISTEMA CRIPTOGRÁFICO 1
RED DE COMUNICACIÓN
5
APARATO DE GENERACIÓN DE CLAVE
20
APARATO DE GENERACIÓN DE CLAVE
20
APARATO DE MANTENIMIENTO
80
APARATO DE AUTENTICACIÓN
90
APARATO DE REGISTRO
50
APARATO DE REGISTRO
50
APARATO DE GESTIÓN
40
APARATO DE GESTIÓN
40
APARATO CLIENTE (APARATO DE CIFRADO)
10
TARJETA IC
39
APARATO CLIENTE (SEGUNDO APARATO DE DESCIFRADO)
30-2
TARJETA IC
39
APARATO CLIENTE (PRIMER APARATO DE DESCIFRADO)
30-1
TARJETA IC
39

FIG.29

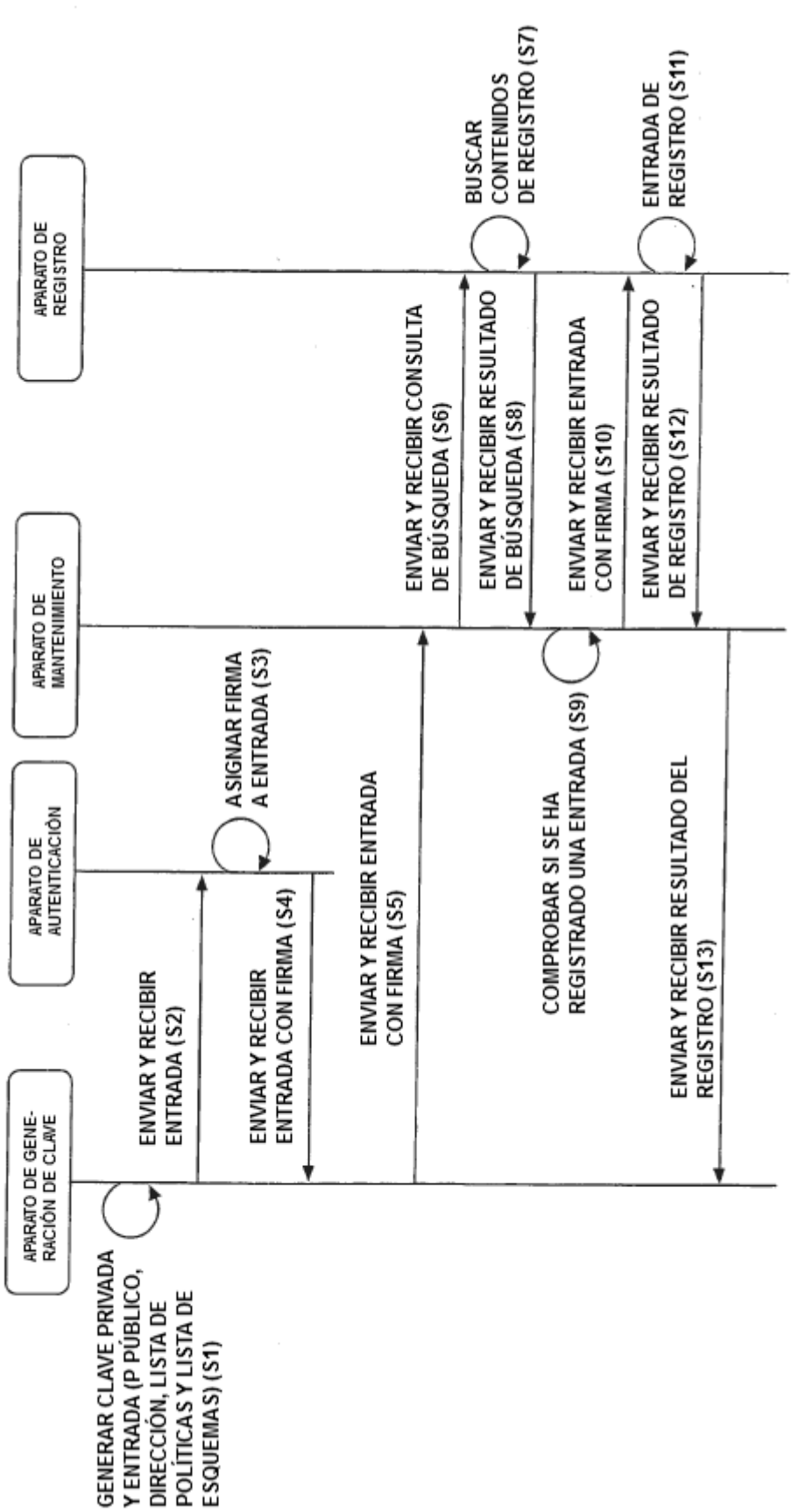

APARATO DE GENE-RACIÓN DE CLAVE
APARATO DE AUTENTICACIÓN
APARATO DE MANTENIMIENTO
APARATO DE REGISTRO
GENERAR CLAVE PRIVADA Y ENTRADA (P PÚBLICO, DIRECCIÓN, LISTA DE POLÍTICAS Y LISTA DE ESQUEMAS) (S1)
ENVIAR Y RECIBIR ENTRADA (S2)
ASIGNAR FIRMA A ENTRADA (S3)
ENVIAR Y RECIBIR ENTRADA CON FIRMA (S4)
ENVIAR Y RECIBIR ENTRADA CON FIRMA (S5)
ENVIAR Y RECIBIR CONSULTA DE BÚSQUEDA (S6)
BUSCAR CONTENIDOS DE REGISTRO (S7)
ENVIAR Y RECIBIR RESULTADO DE BÚSQUEDA (S8)
COMPROBAR SI SE HA REGISTRADO UNA ENTRADA (S9)
ENVIAR Y RECIBIR ENTRADA CON FIRMA (S10)
ENTRADA DE REGISTRO (S11)
ENVIAR Y RECIBIR RESULTADO DE REGISTRO (S12)
ENVIAR Y RECIBIR RESULTADO DEL REGISTRO (S13)

FIG.30

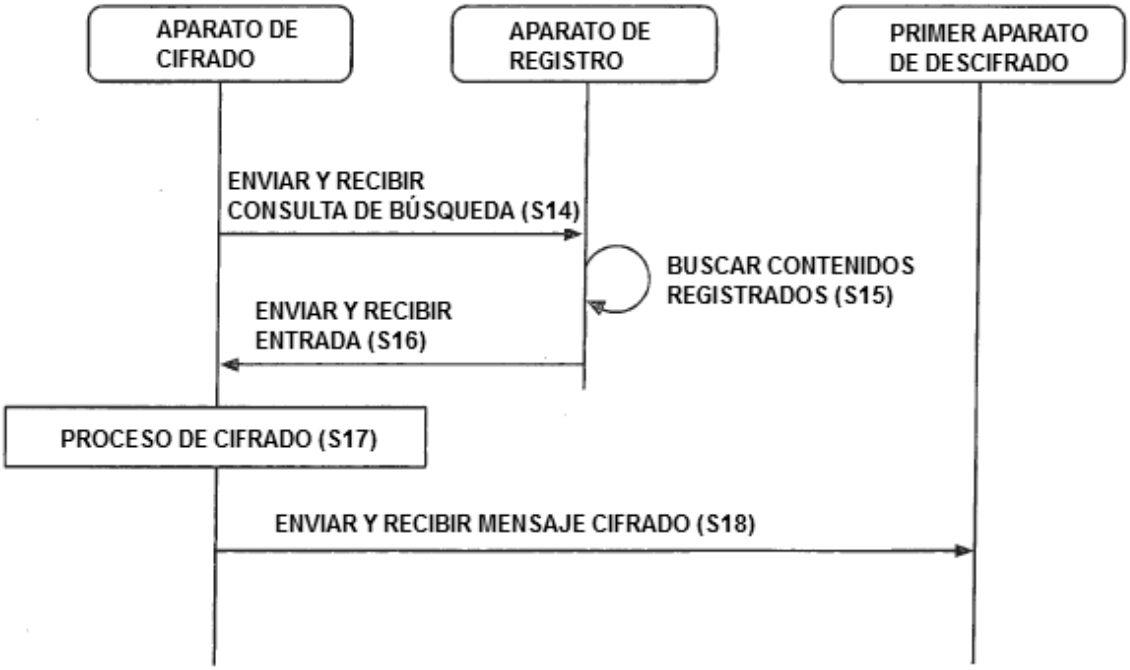

APARATO DE CIFRADO
APARATO DE REGISTRO
PRIMER APARATO DE DESCIFRADO
ENVIAR Y RECIBIR CONSULTA DE BÚSQUEDA (S14)
BUSCAR CONTENIDOS REGISTRADOS (S15)
ENVIAR Y RECIBIR ENTRADA (S16)
PROCESO DE CIFRADO (S17)
ENVIAR Y RECIBIR MENSAJE CIFRADO (S18)

FIG.31

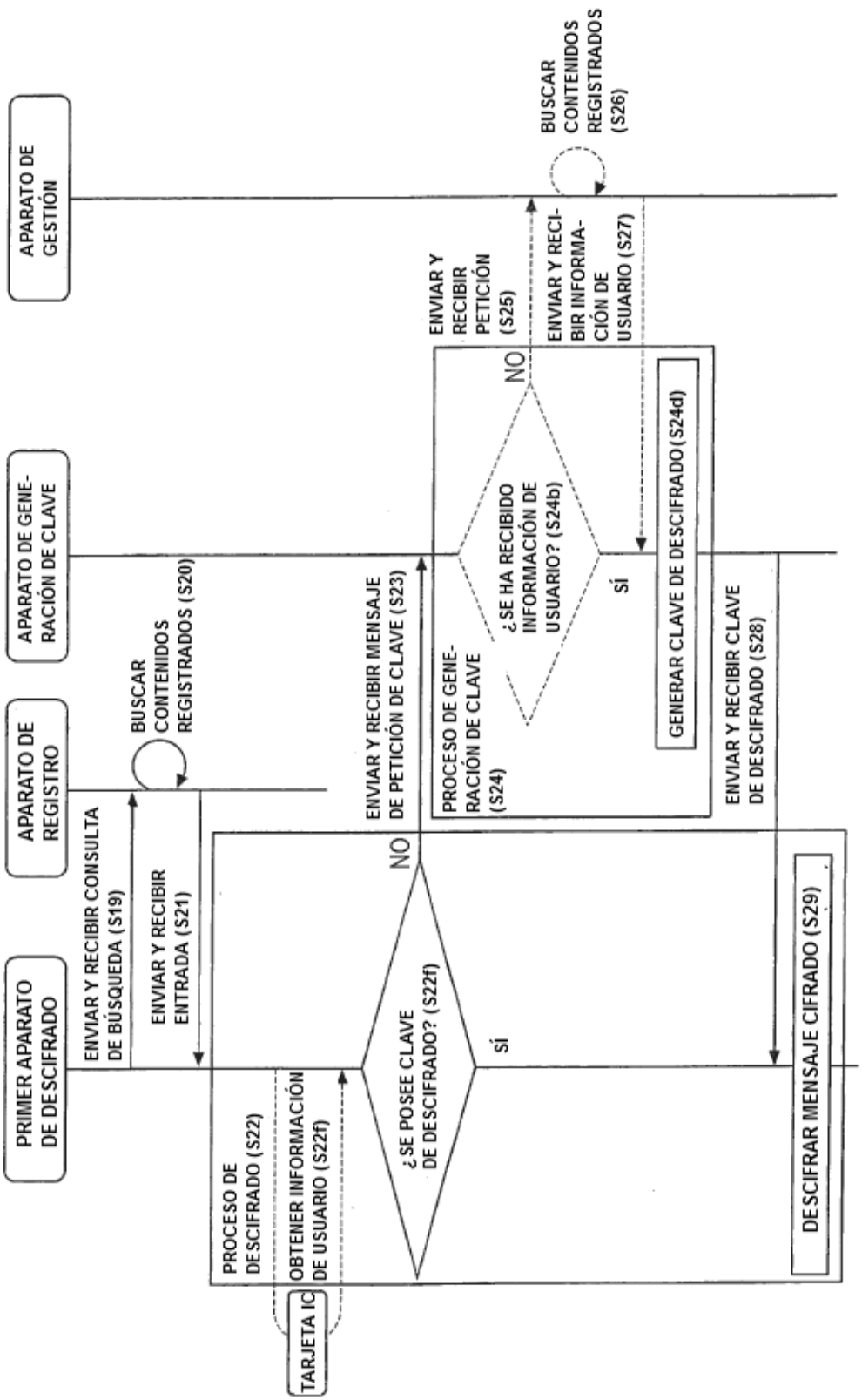

PRIMER APARATO DE DESCIFRADO
APARATO DE REGISTRO
APARATO DE GENERACIÓN DE CLAVE
APARATO DE GESTIÓN
ENVIAR Y RECIBIR CONSULTA DE BÚSQUEDA (S19)
BUSCAR CONTENIDOS REGISTRADOS (S20)
ENVIAR Y RECIBIR ENTRADA (S21)
PROCESO DE DESCIFRADO (S22)
OBTENER INFORMACIÓN DE USUARIO (S22f)
TARJETA IC
¿SE POSEE CLAVE DE DESCIFRADO? (S22f)
NO
SÍ
ENVIAR Y RECIBIR MENSAJE DE PETICIÓN DE CLAVE (S23)
PROCESO DE GENERACIÓN DE CLAVE (S24)
¿SE HA RECIBIDO INFORMACIÓN DE USUARIO? (S24b)
NO
SÍ
ENVIAR Y RECIBIR PETICIÓN (S25)
BUSCAR CONTENIDOS REGISTRADOS (S26)
ENVIAR Y RECIBIR INFORMACIÓN DE USUARIO (S27)
GENERAR CLAVE DE DESCIFRADO (S24d)
ENVIAR Y RECIBIR CLAVE DE DESCIFRADO (S28)
DESCIFRAR MENSAJE CIFRADO (S29)

FIG.32

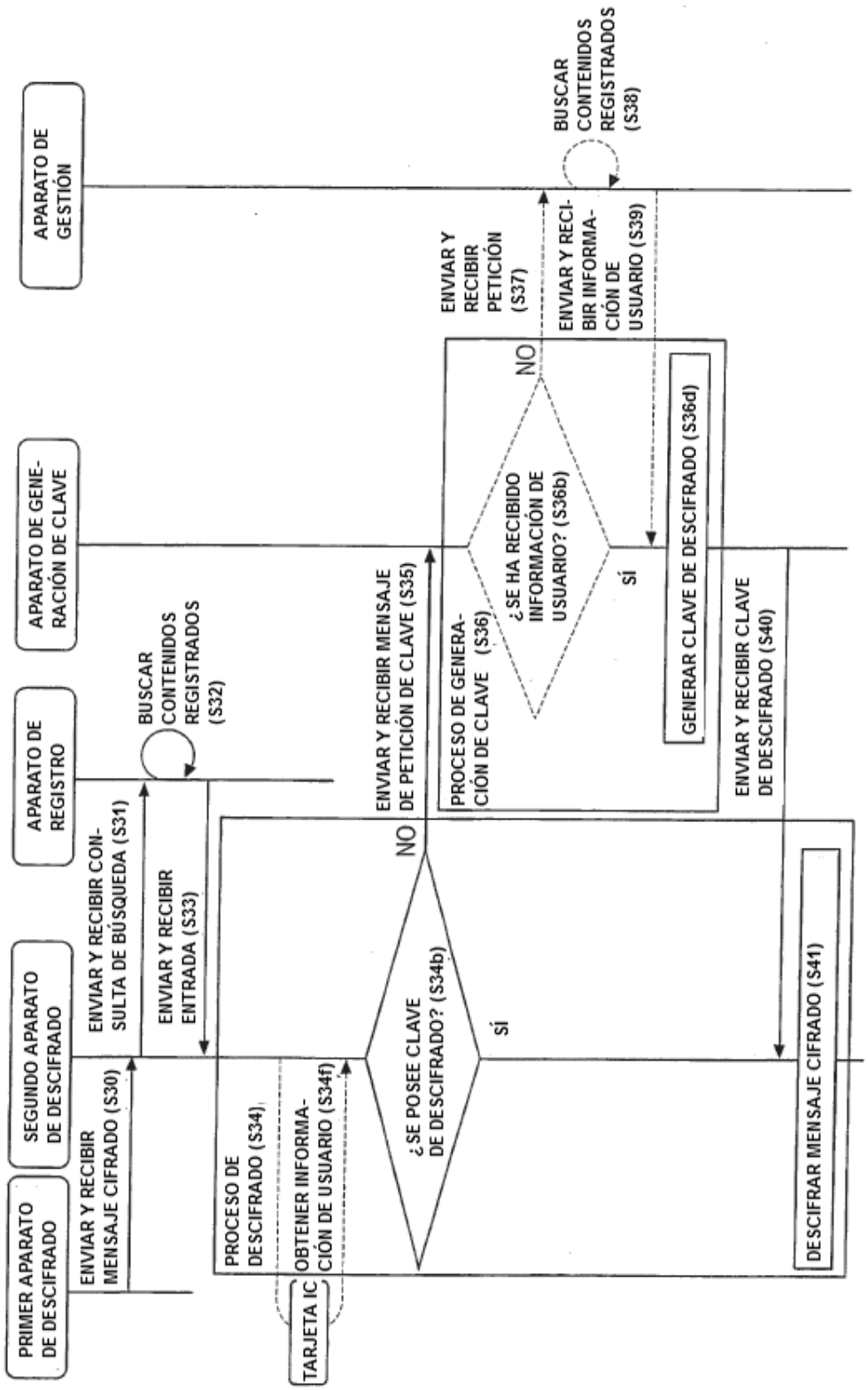

PRIMER APARATO DE DESCIFRADO
SEGUNDO APARATO DE DESCIFRADO
APARATO DE REGISTRO
APARATO DE GENERACIÓN DE CLAVE
APARATO DE GESTIÓN
TARJETA IC
ENVIAR Y RECIBIR MENSAJE CIFRADO (S30)
ENVIAR Y RECIBIR CONSULTA DE BÚSQUEDA (S31)
BUSCAR CONTENIDOS REGISTRADOS (S32)
ENVIAR Y RECIBIR ENTRADA (S33)
PROCESO DE DESCIFRADO (S34)
OBTENER INFORMACIÓN DE USUARIO (S34f)
¿SE POSEE CLAVE DE DESCIFRADO? (S34b)
NO
SÍ
ENVIAR Y RECIBIR MENSAJE DE PETICIÓN DE CLAVE (S35)
PROCESO DE GENERACIÓN DE CLAVE (S36)
¿SE HA RECIBIDO INFORMACIÓN DE USUARIO? (S36b)
NO
SÍ
ENVIAR Y RECIBIR PETICIÓN (S37)
BUSCAR CONTENIDOS REGISTRADOS (S38)
ENVIAR Y RECIBIR INFORMACIÓN DE USUARIO (S39)
GENERAR CLAVE DE DESCIFRADO (S36d)
ENVIAR Y RECIBIR CLAVE DE DESCIFRADO (S40)
DESCIFRAR MENSAJE CIFRADO (S41)

FIG.33

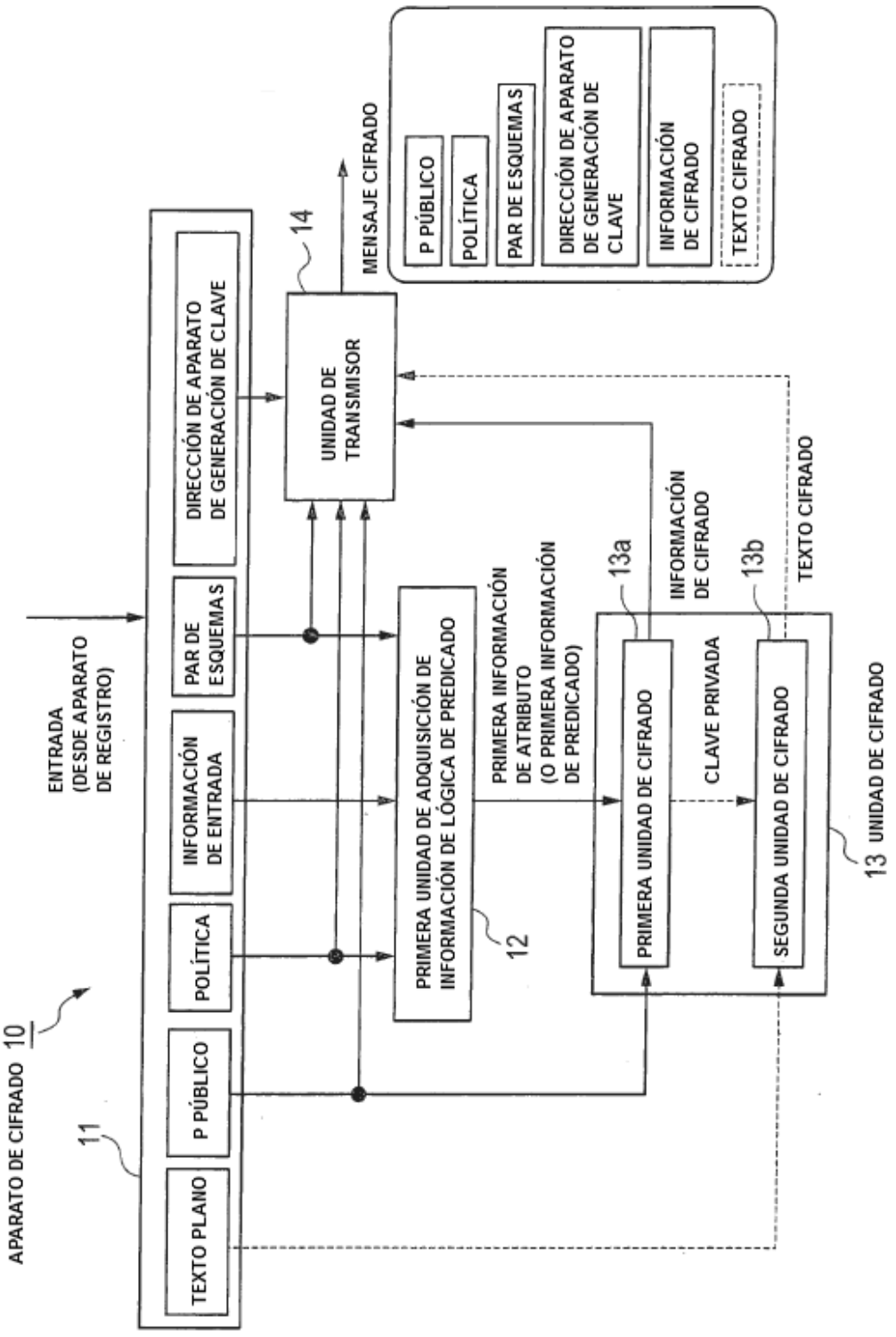

APARATO DE CIFRADO 10
11
TEXTO PLANO
P PÚBLICO
POLÍTICA
INFORMACIÓN DE ENTRADA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
ENTRADA (DESDE APARATO DE REGISTRO)
PRIMERA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
12
PRIMERA INFORMACIÓN DE ATRIBUTO (O PRIMERA INFORMACIÓN DE PREDICADO)
UNIDAD DE TRANSMISOR
14
MENSAJE CIFRADO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
INFORMACIÓN DE CIFRADO
TEXTO CIFRADO
13a
PRIMERA UNIDAD DE CIFRADO
INFORMACIÓN DE CIFRADO
CLAVE PRIVADA
13b
SEGUNDA UNIDAD DE CIFRADO
TEXTO CIFRADO
13 UNIDAD DE CIFRADO

FIG.34


PROCESO DE CIFRADO (S17)
USAR UN ESQUEMA SELECCIONADO JUNTO CON LA POLÍTICA EN BASE A UNA INFORMACIÓN DE ENTRADA A PARTIR DE UN ESQUEMA DE ATRIBUTO Y ESQUEMA DE PREDICADO INCLUIDOS EN UN PAR DE ESQUEMAS SELECCIONADO PARA OBTENER UNA PRIMERA INFORMACIÓN DE ATRIBUTO O UNA PRIMERA INFORMACIÓN DE PREDICADO A PARTIR DE LA INFORMACIÓN DE ENTRADA (S17a)
USAR UNA PRIMERA INFORMACIÓN DE ATRIBUTO O PRIMERA INFORMACIÓN DE PREDICADO, Y P PÚBLICO PARA OBTENER UNA INFORMACIÓN DE CIFRADO DE CLAVE PRIVADA SEGÚN UN ALGORITMO DE PREDICADO (S17b)
USAR LA CLAVE PÚBLICA PARA CIFRAR TEXTO PLANO PARA OBTENER UN TEXTO CIFRADO (S17c)
GENERAR MENSAJE CIFRADO (S17d)

FIG.35

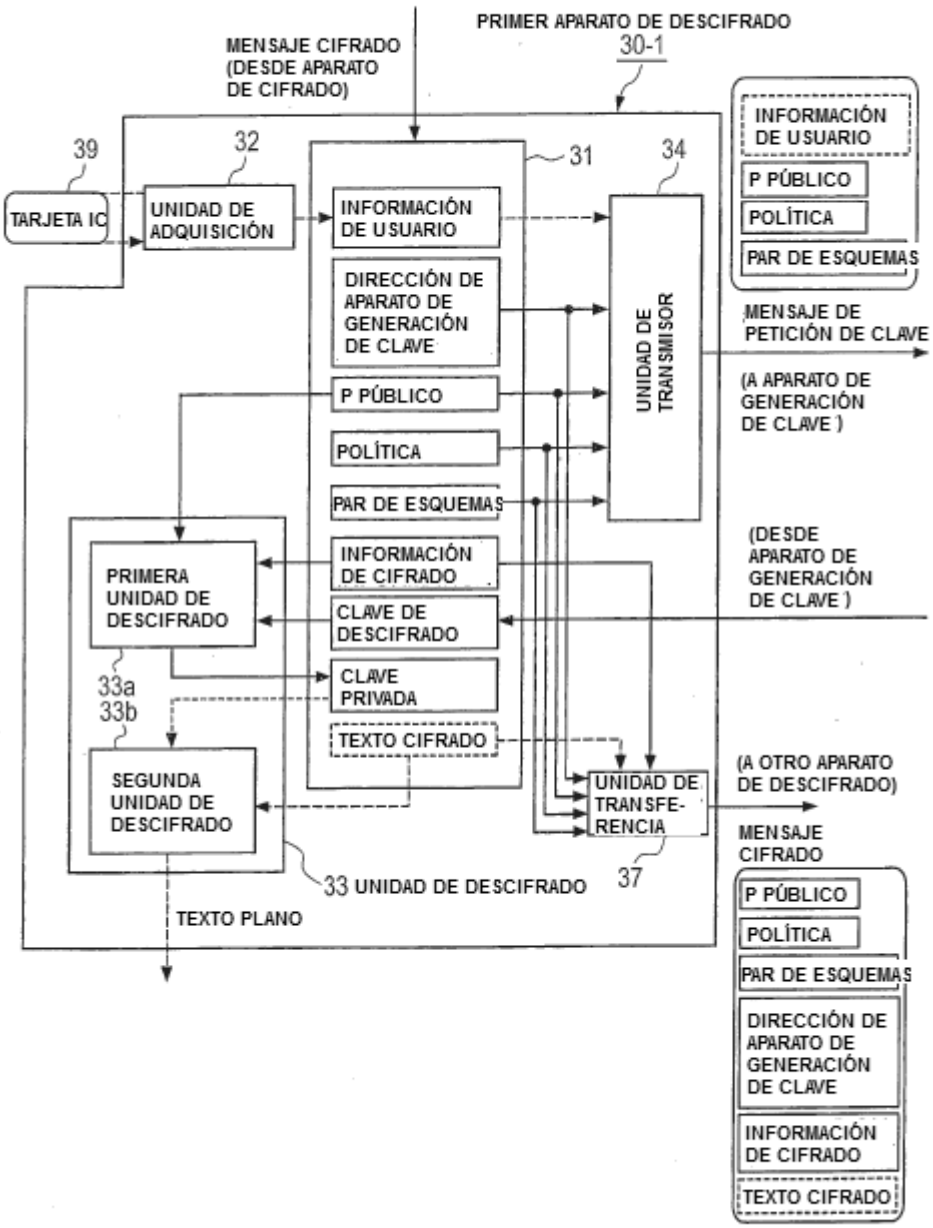

PRIMER APARATO DE DESCIFRADO
30-1
MENSAJE CIFRADO (DESDE APARATO DE CIFRADO)
39
32
31
34
TARJETA IC
UNIDAD DE ADQUISICIÓN
INFORMACIÓN DE USUARIO
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
UNIDAD DE TRANSMISOR
INFORMACIÓN DE USUARIO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
MENSAJE DE PETICIÓN DE CLAVE
(A APARATO DE GENERACIÓN DE CLAVE)
(DESDE APARATO DE GENERACIÓN DE CLAVE)
PRIMERA UNIDAD DE DESCIFRADO
INFORMACIÓN DE CIFRADO
CLAVE DE DESCIFRADO
CLAVE PRIVADA
TEXTO CIFRADO
33a
33b
SEGUNDA UNIDAD DE DESCIFRADO
UNIDAD DE TRANSFE-RENCIA
(A OTRO APARATO DE DESCIFRADO)
MENSAJE CIFRADO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
INFORMACIÓN DE CIFRADO
TEXTO CIFRADO
33 UNIDAD DE DESCIFRADO
37
TEXTO PLANO

FIG.36

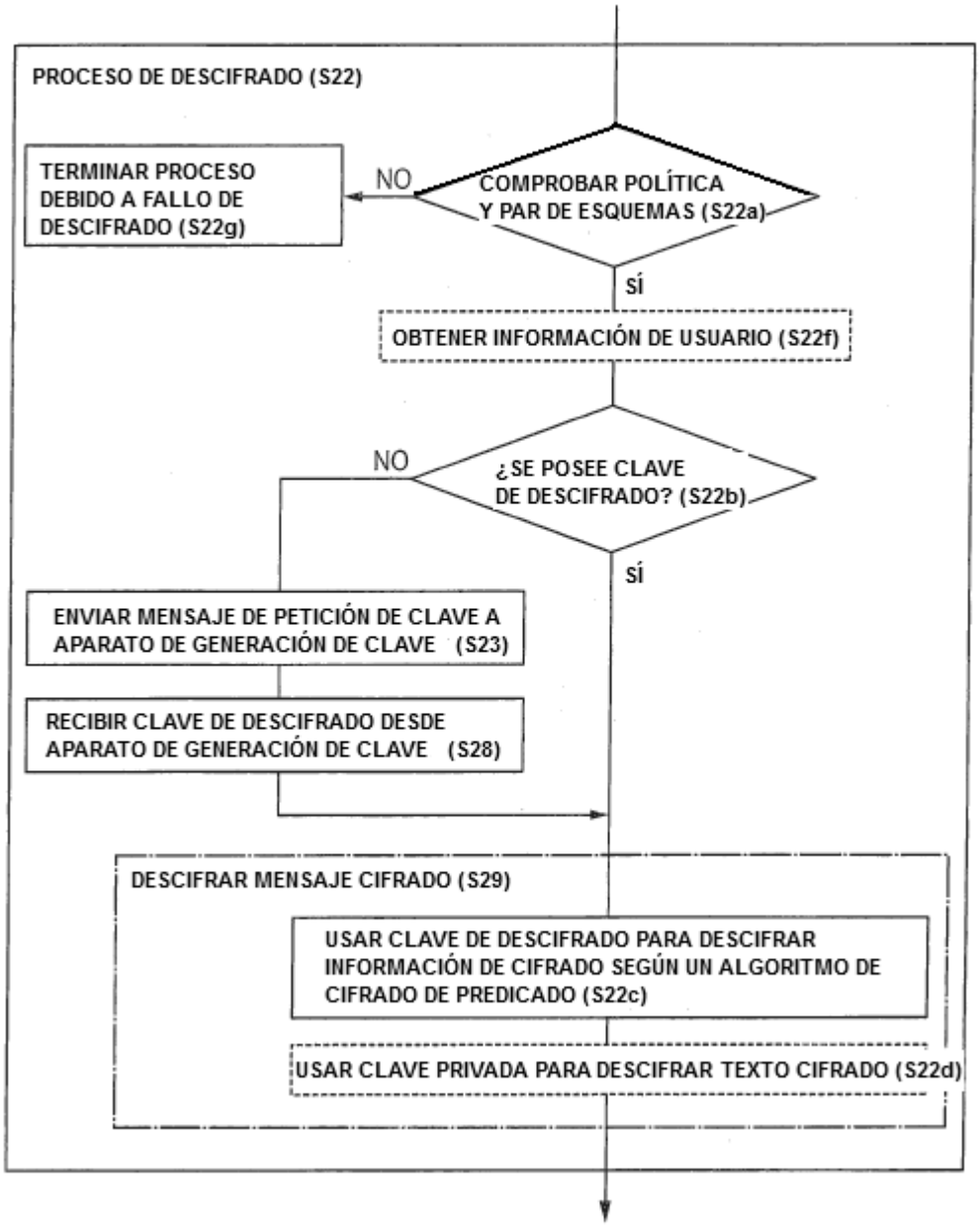

PROCESO DE DESCIFRADO (S22)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S22g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S22a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S22f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S22b)
SÍ
ENVIAR MENSAJE DE PETICIÓN DE CLAVE A APARATO DE GENERACIÓN DE CLAVE (S23)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACIÓN DE CLAVE (S28)
DESCIFRAR MENSAJE CIFRADO (S29)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGÚN UN ALGORITMO DE CIFRADO DE PREDICADO (S22c)
USAR CLAVE PRIVADA PARA DESCIFRAR TEXTO CIFRADO (S22d)

FIG.37

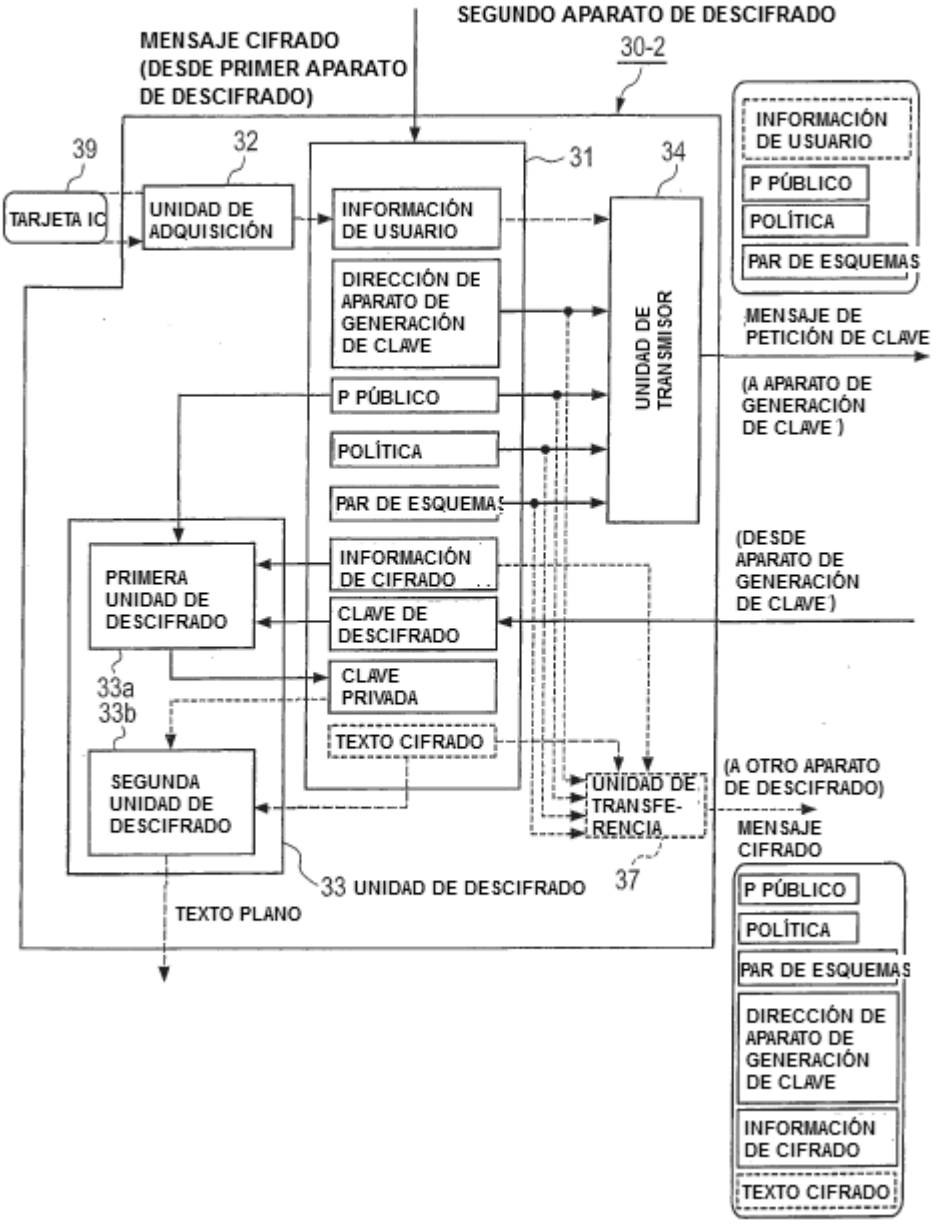

SEGUNDO APARATO DE DESCIFRADO
30-2
MENSAJE CIFRADO
(DESDE PRIMER APARATO
DE DESCIFRADO)
39
32
31
34
TARJETA IC
UNIDAD DE
ADQUISICIÓN
INFORMACIÓN
DE USUARIO
DIRECCIÓN DE
APARATO DE
GENERACIÓN
DE CLAVE
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
UNIDAD DE
TRANSMISOR
INFORMACIÓN
DE USUARIO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
MENSAJE DE
PETICIÓN DE CLAVE
(A APARATO DE
GENERACIÓN
DE CLAVE)
(DESDE
APARATO DE
GENERACIÓN
DE CLAVE)
PRIMERA
UNIDAD DE
DESCIFRADO
INFORMACIÓN
DE CIFRADO
CLAVE DE
DESCIFRADO
CLAVE
PRIVADA
TEXTO CIFRADO
33a
33b
SEGUNDA
UNIDAD DE
DESCIFRADO
UNIDAD DE
TRANSFE-
RENCIA
37
(A OTRO APARATO
DE DESCIFRADO)
MENSAJE
CIFRADO
33 UNIDAD DE DESCIFRADO
TEXTO PLANO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE
APARATO DE
GENERACIÓN
DE CLAVE
INFORMACIÓN
DE CIFRADO
TEXTO CIFRADO

FIG.38

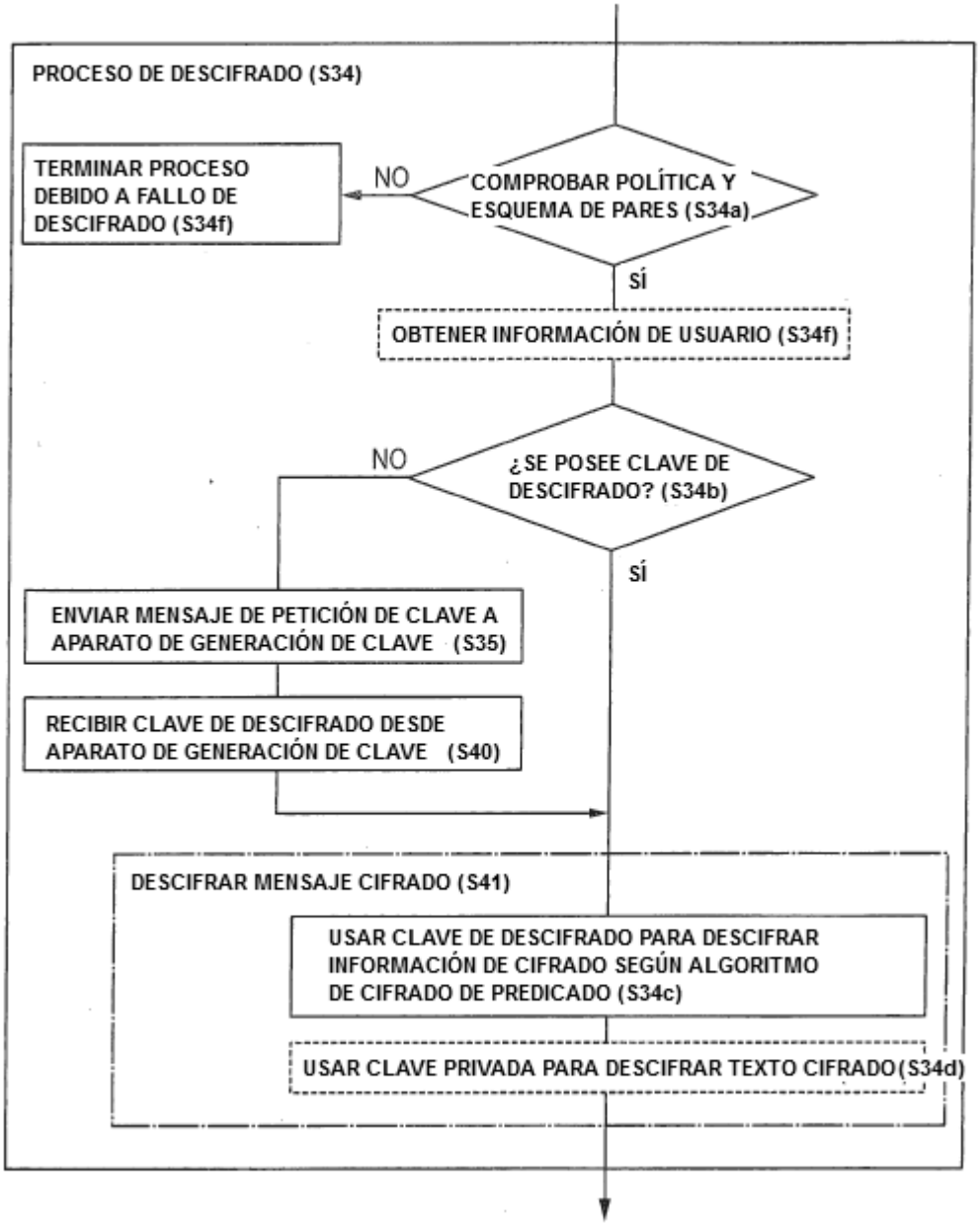

PROCESO DE DESCIFRADO (S34)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S34f)
NO
COMPROBAR POLÍTICA Y ESQUEMA DE PARES (S34a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S34f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S34b)
SÍ
ENVIAR MENSAJE DE PETICIÓN DE CLAVE A APARATO DE GENERACIÓN DE CLAVE (S35)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACIÓN DE CLAVE (S40)
DESCIFRAR MENSAJE CIFRADO (S41)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGÚN ALGORITMO DE CIFRADO DE PREDICADO (S34c)
USAR CLAVE PRIVADA PARA DESCIFRAR TEXTO CIFRADO (S34d)

FIG.39

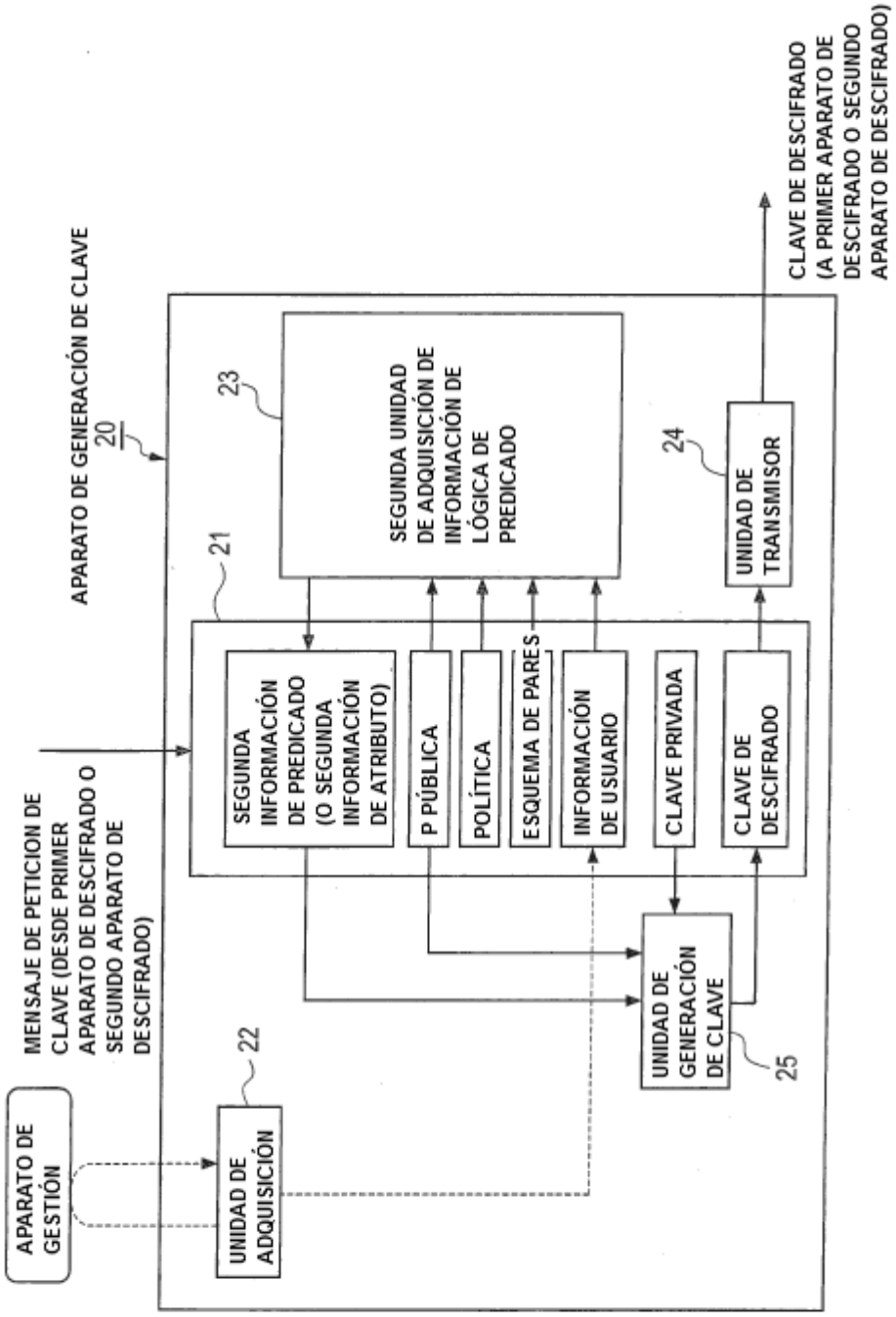

APARATO DE GESTIÓN
MENSAJE DE PETICION DE CLAVE (DESDE PRIMER APARATO DE DESCIFRADO O SEGUNDO APARATO DE DESCIFRADO)
APARATO DE GENERACIÓN DE CLAVE
20
UNIDAD DE ADQUISICIÓN
22
21
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
P PÚBLICA
POLÍTICA
ESQUEMA DE PARES
INFORMACIÓN DE USUARIO
CLAVE PRIVADA
CLAVE DE DESCIFRADO
23
SEGUNDA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
UNIDAD DE GENERACIÓN DE CLAVE
25
24
UNIDAD DE TRANSMISOR
CLAVE DE DESCIFRADO (A PRIMER APARATO DE DESCIFRADO O SEGUNDO APARATO DE DESCIFRADO)

FIG.40

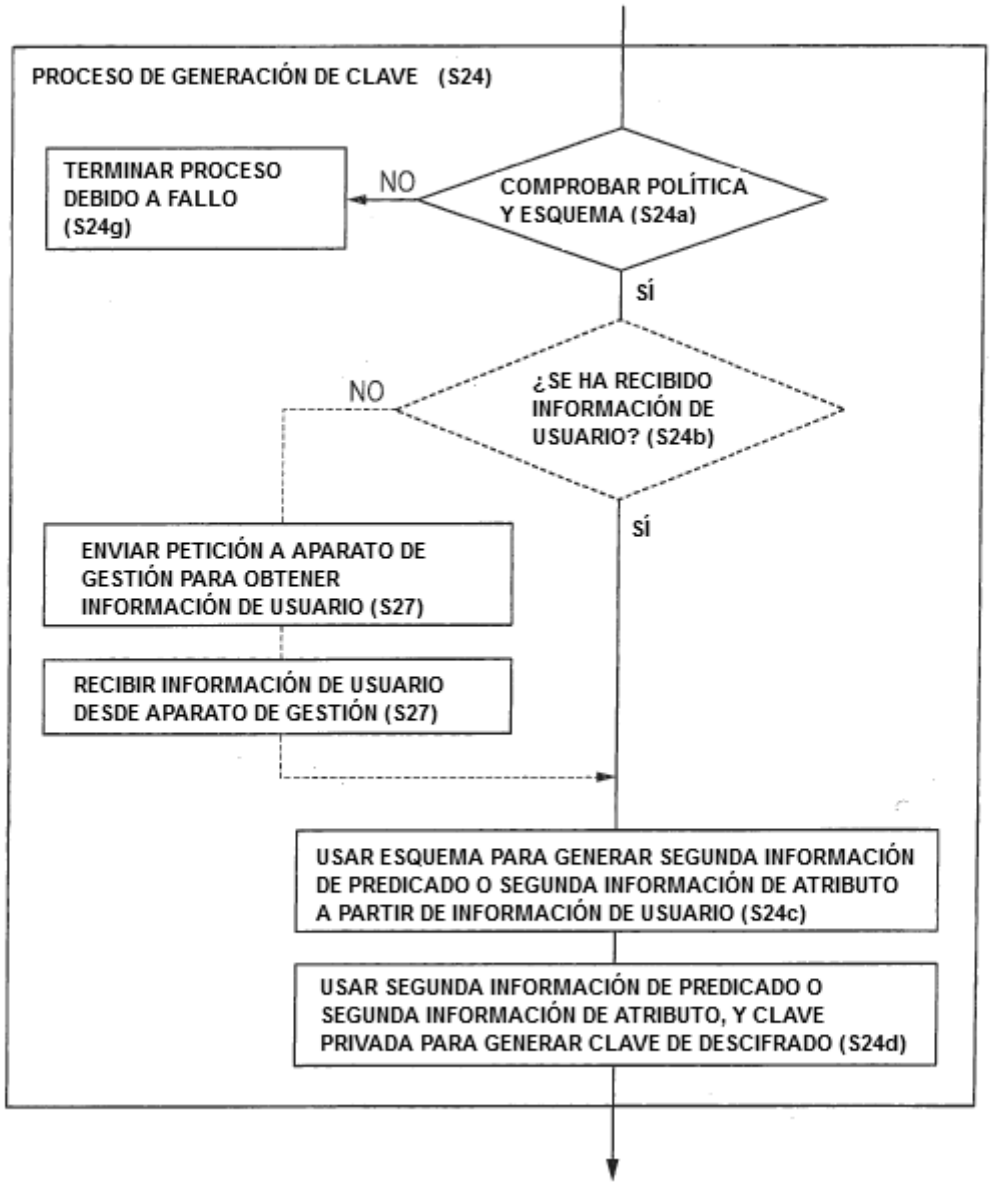

PROCESO DE GENERACIÓN DE CLAVE (S24)
COMPROBAR POLÍTICA Y ESQUEMA (S24a)
NO
TERMINAR PROCESO DEBIDO A FALLO (S24g)
SÍ
¿SE HA RECIBIDO INFORMACIÓN DE USUARIO? (S24b)
NO
SÍ
ENVIAR PETICIÓN A APARATO DE GESTIÓN PARA OBTENER INFORMACIÓN DE USUARIO (S27)
RECIBIR INFORMACIÓN DE USUARIO DESDE APARATO DE GESTIÓN (S27)
USAR ESQUEMA PARA GENERAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO A PARTIR DE INFORMACIÓN DE USUARIO (S24c)
USAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO, Y CLAVE PRIVADA PARA GENERAR CLAVE DE DESCIFRADO (S24d)

FIG.41

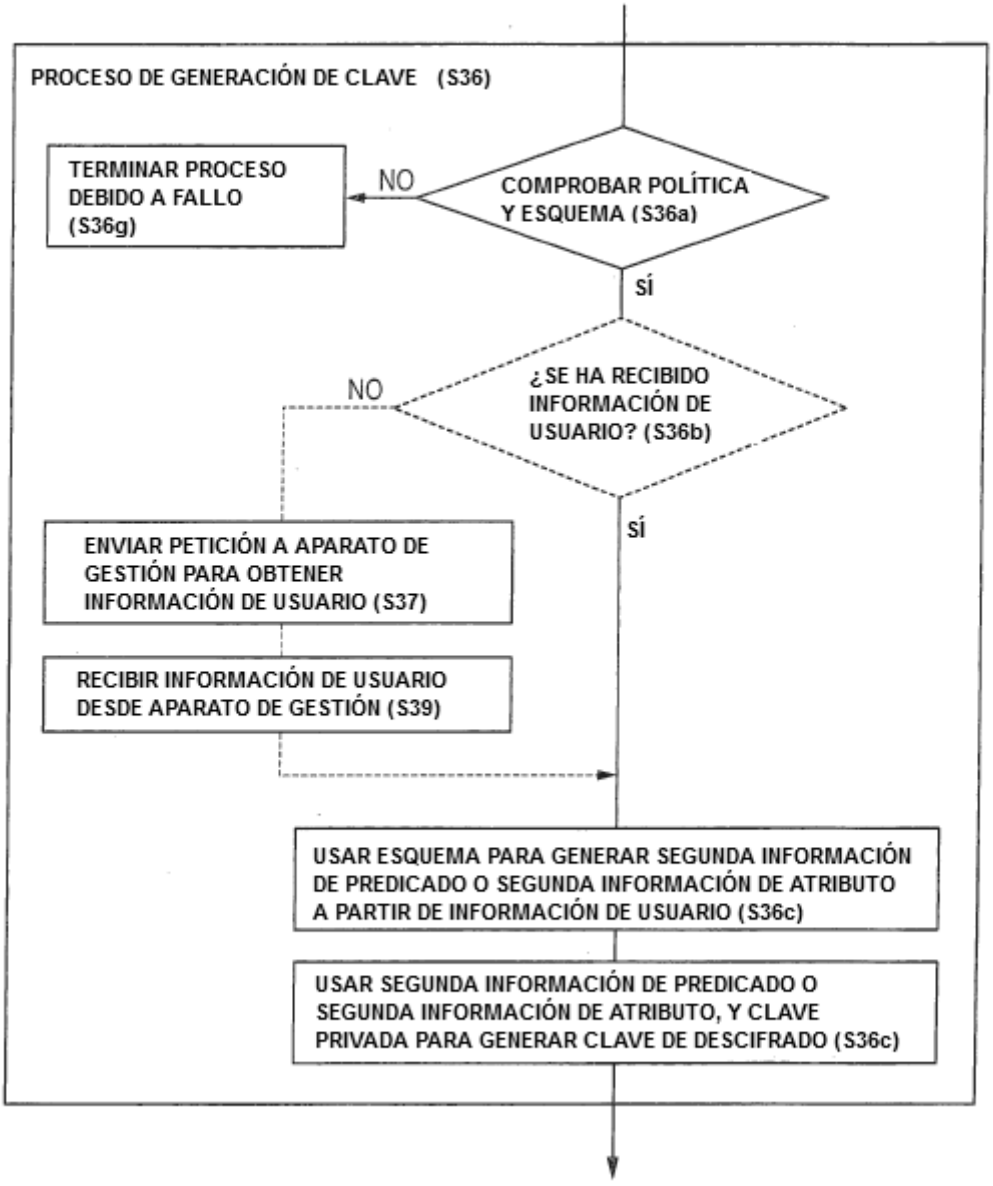

PROCESO DE GENERACIÓN DE CLAVE (S36)
COMPROBAR POLÍTICA Y ESQUEMA (S36a)
NO
TERMINAR PROCESO DEBIDO A FALLO (S36g)
SÍ
¿SE HA RECIBIDO INFORMACIÓN DE USUARIO? (S36b)
NO
SÍ
ENVIAR PETICIÓN A APARATO DE GESTIÓN PARA OBTENER INFORMACIÓN DE USUARIO (S37)
RECIBIR INFORMACIÓN DE USUARIO DESDE APARATO DE GESTIÓN (S39)
USAR ESQUEMA PARA GENERAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO A PARTIR DE INFORMACIÓN DE USUARIO (S36c)
USAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO, Y CLAVE PRIVADA PARA GENERAR CLAVE DE DESCIFRADO (S36c)

FIG.42

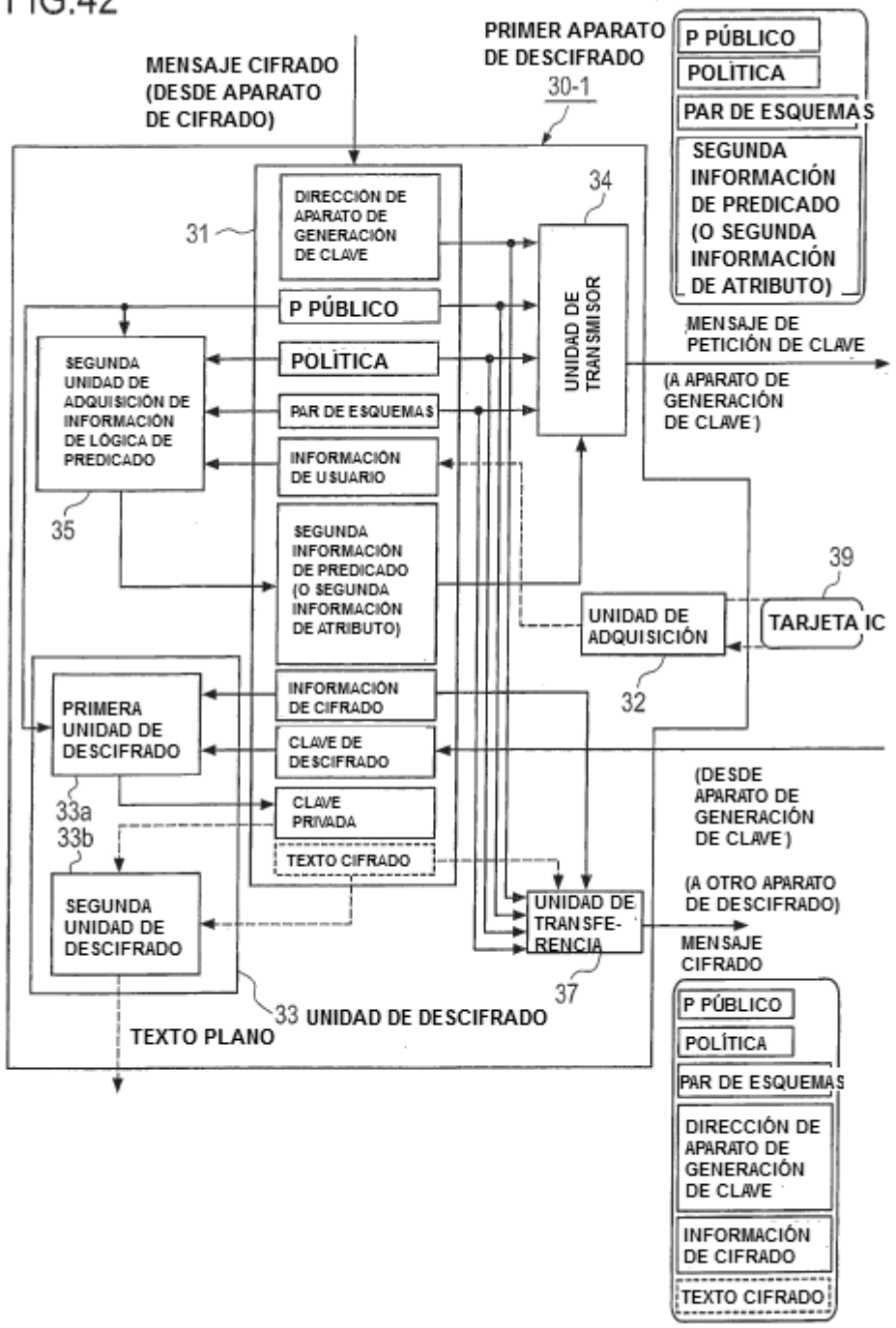

MENSAJE CIFRADO (DESDE APARATO DE CIFRADO)
PRIMER APARATO DE DESCIFRADO
30-1
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
31
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
34
UNIDAD DE TRANSMISOR
MENSAJE DE PETICIÓN DE CLAVE
(A APARATO DE GENERACIÓN DE CLAVE)
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
SEGUNDA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
INFORMACIÓN DE USUARIO
35
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
39
UNIDAD DE ADQUISICIÓN
TARJETA IC
32
PRIMERA UNIDAD DE DESCIFRADO
INFORMACIÓN DE CIFRADO
CLAVE DE DESCIFRADO
33a
33b
CLAVE PRIVADA
TEXTO CIFRADO
(DESDE APARATO DE GENERACIÓN DE CLAVE)
(A OTRO APARATO DE DESCIFRADO)
SEGUNDA UNIDAD DE DESCIFRADO
UNIDAD DE TRANSFE-RENCIA
37
MENSAJE CIFRADO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
INFORMACIÓN DE CIFRADO
TEXTO CIFRADO
33 UNIDAD DE DESCIFRADO
TEXTO PLANO

FIG.43

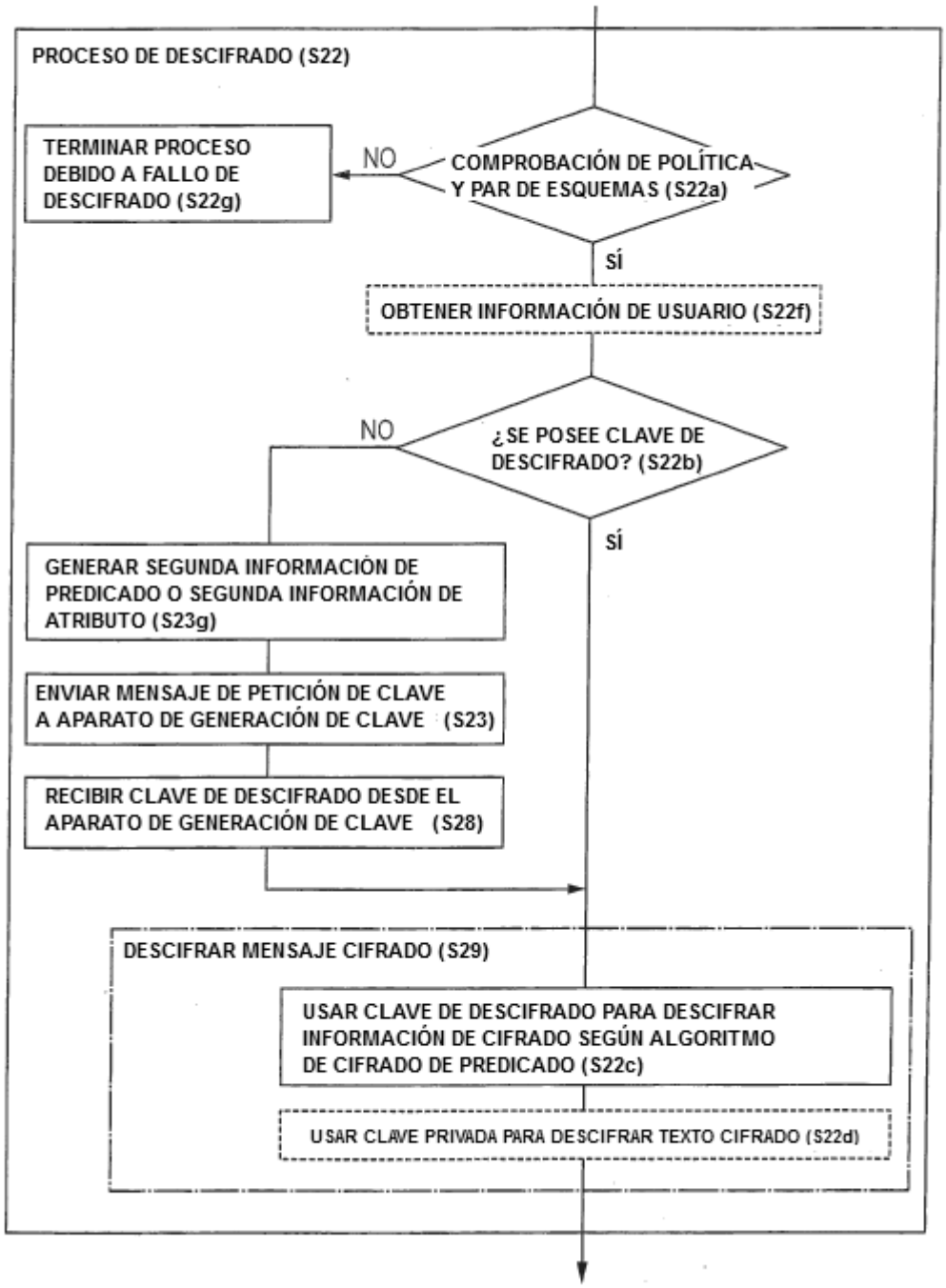

PROCESO DE DESCIFRADO (S22)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S22g)
NO
COMPROBACIÓN DE POLÍTICA Y PAR DE ESQUEMAS (S22a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S22f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S22b)
SÍ
GENERAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO (S23g)
ENVIAR MENSAJE DE PETICIÓN DE CLAVE A APARATO DE GENERACIÓN DE CLAVE (S23)
RECIBIR CLAVE DE DESCIFRADO DESDE EL APARATO DE GENERACIÓN DE CLAVE (S28)
DESCIFRAR MENSAJE CIFRADO (S29)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGÚN ALGORITMO DE CIFRADO DE PREDICADO (S22c)
USAR CLAVE PRIVADA PARA DESCIFRAR TEXTO CIFRADO (S22d)

FIG.44

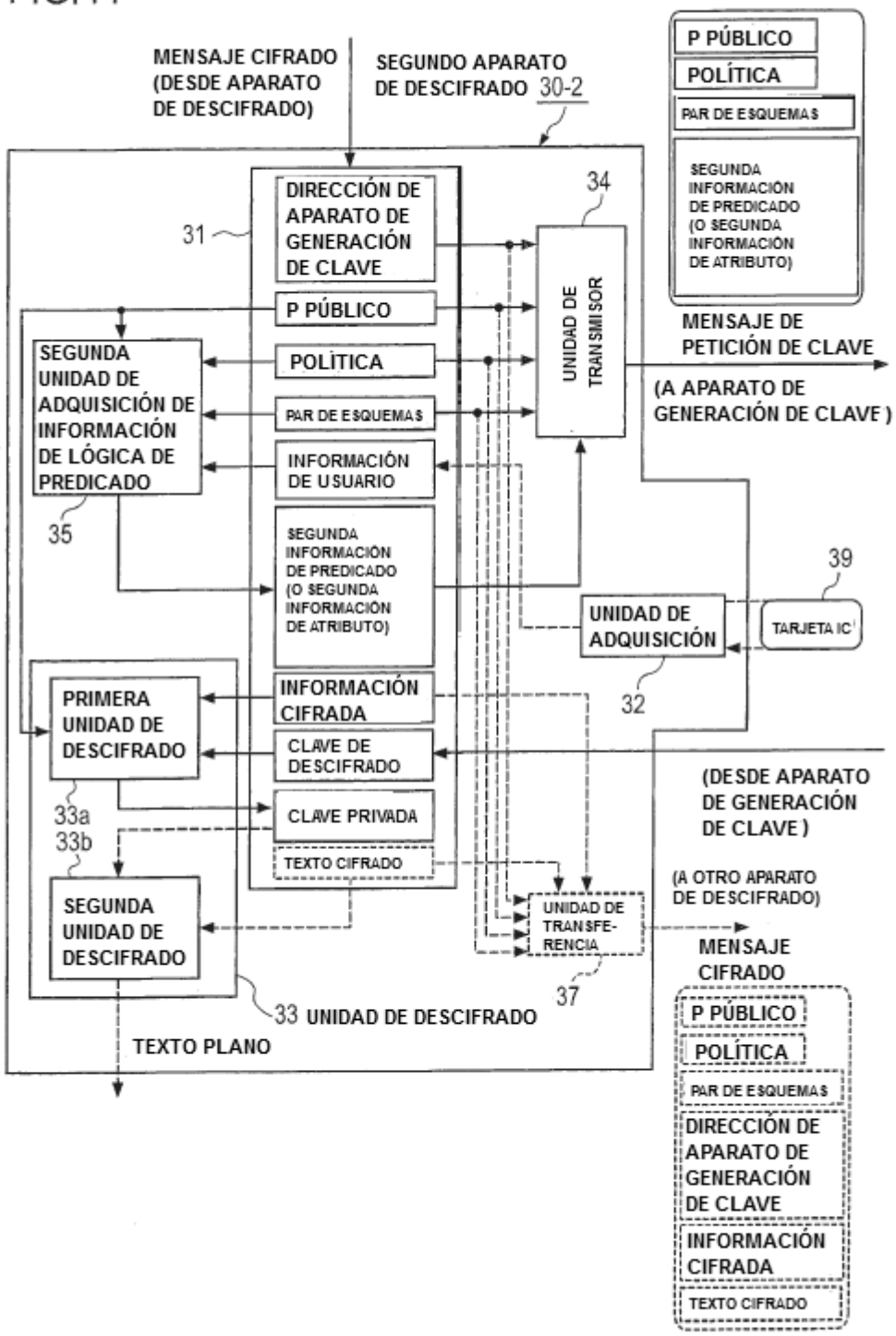

MENSAJE CIFRADO (DESDE APARATO DE DESCIFRADO)
SEGUNDO APARATO DE DESCIFRADO 30-2
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
34
31
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
INFORMACIÓN DE USUARIO
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
INFORMACIÓN CIFRADA
CLAVE DE DESCIFRADO
CLAVE PRIVADA
TEXTO CIFRADO
UNIDAD DE TRANSMISOR
MENSAJE DE PETICIÓN DE CLAVE
(A APARATO DE GENERACIÓN DE CLAVE)
SEGUNDA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
35
39
UNIDAD DE ADQUISICIÓN
TARJETA IC
32
PRIMERA UNIDAD DE DESCIFRADO
33a
33b
SEGUNDA UNIDAD DE DESCIFRADO
(DESDE APARATO DE GENERACIÓN DE CLAVE)
(A OTRO APARATO DE DESCIFRADO)
UNIDAD DE TRANSFERENCIA
37
MENSAJE CIFRADO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
INFORMACIÓN CIFRADA
TEXTO CIFRADO
33 UNIDAD DE DESCIFRADO
TEXTO PLANO

FIG.45

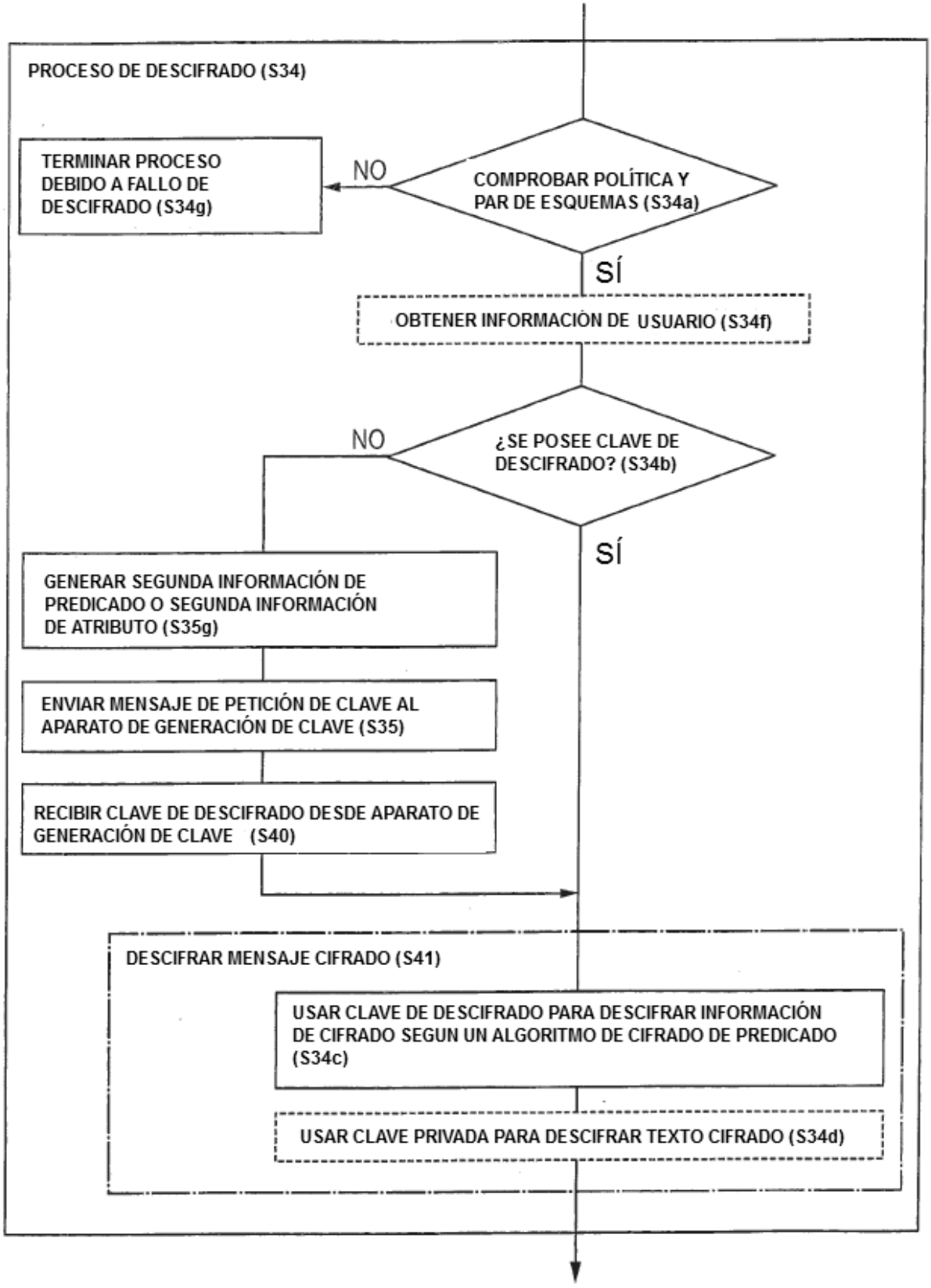

PROCESO DE DESCIFRADO (S34)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S34g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S34a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S34f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S34b)
SÍ
GENERAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO (S35g)
ENVIAR MENSAJE DE PETICIÓN DE CLAVE AL APARATO DE GENERACIÓN DE CLAVE (S35)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACIÓN DE CLAVE (S40)
DESCIFRAR MENSAJE CIFRADO (S41)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGUN UN ALGORITMO DE CIFRADO DE PREDICADO (S34c)
USAR CLAVE PRIVADA PARA DESCIFRAR TEXTO CIFRADO (S34d)

FIG.46

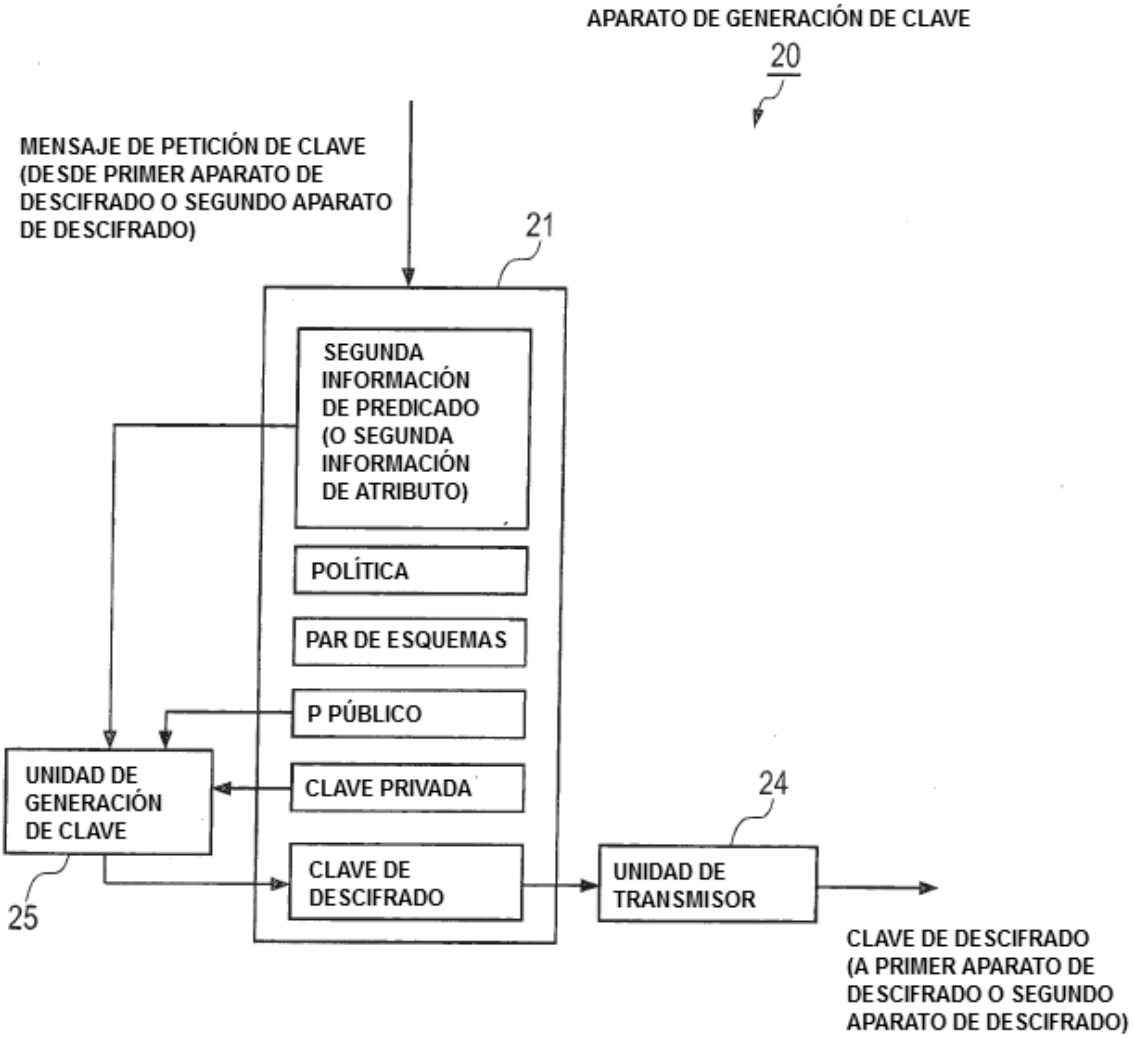

APARATO DE GENERACIÓN DE CLAVE
20
MENSAJE DE PETICIÓN DE CLAVE (DESDE PRIMER APARATO DE DESCIFRADO O SEGUNDO APARATO DE DESCIFRADO)
21
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
POLÍTICA
PAR DE ESQUEMAS
P PÚBLICO
CLAVE PRIVADA
CLAVE DE DESCIFRADO
UNIDAD DE GENERACIÓN DE CLAVE
25
24
UNIDAD DE TRANSMISOR
CLAVE DE DESCIFRADO (A PRIMER APARATO DE DESCIFRADO O SEGUNDO APARATO DE DESCIFRADO)

FIG.47

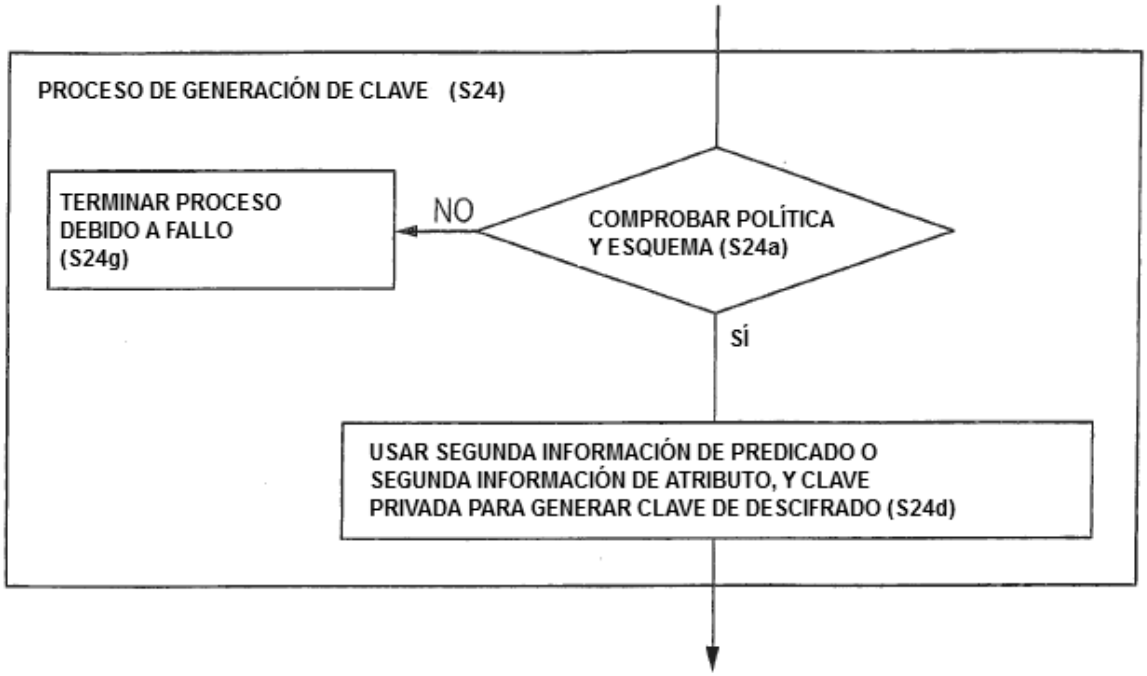

PROCESO DE GENERACIÓN DE CLAVE (S24)
TERMINAR PROCESO DEBIDO A FALLO (S24g)
NO
COMPROBAR POLÍTICA Y ESQUEMA (S24a)
SÍ
USAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO, Y CLAVE PRIVADA PARA GENERAR CLAVE DE DESCIFRADO (S24d)

FIG.48

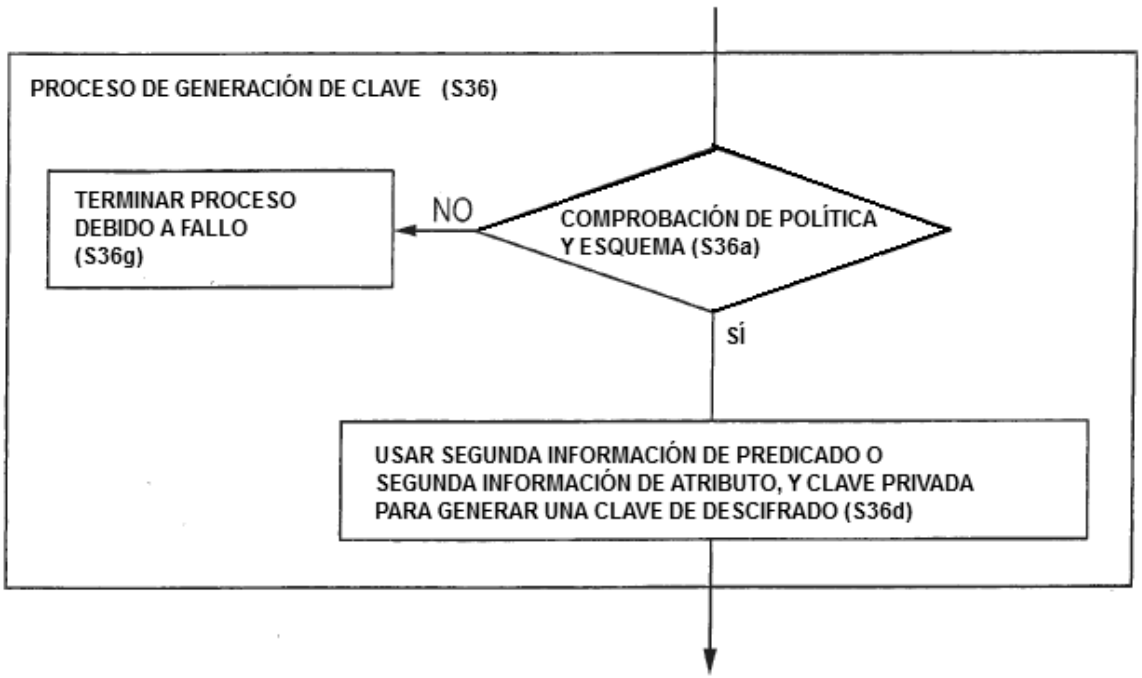

PROCESO DE GENERACIÓN DE CLAVE (S36)
TERMINAR PROCESO DEBIDO A FALLO (S36g)
NO
COMPROBACIÓN DE POLÍTICA Y ESQUEMA (S36a)
SÍ
USAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO, Y CLAVE PRIVADA PARA GENERAR UNA CLAVE DE DESCIFRADO (S36d)

FIG.49

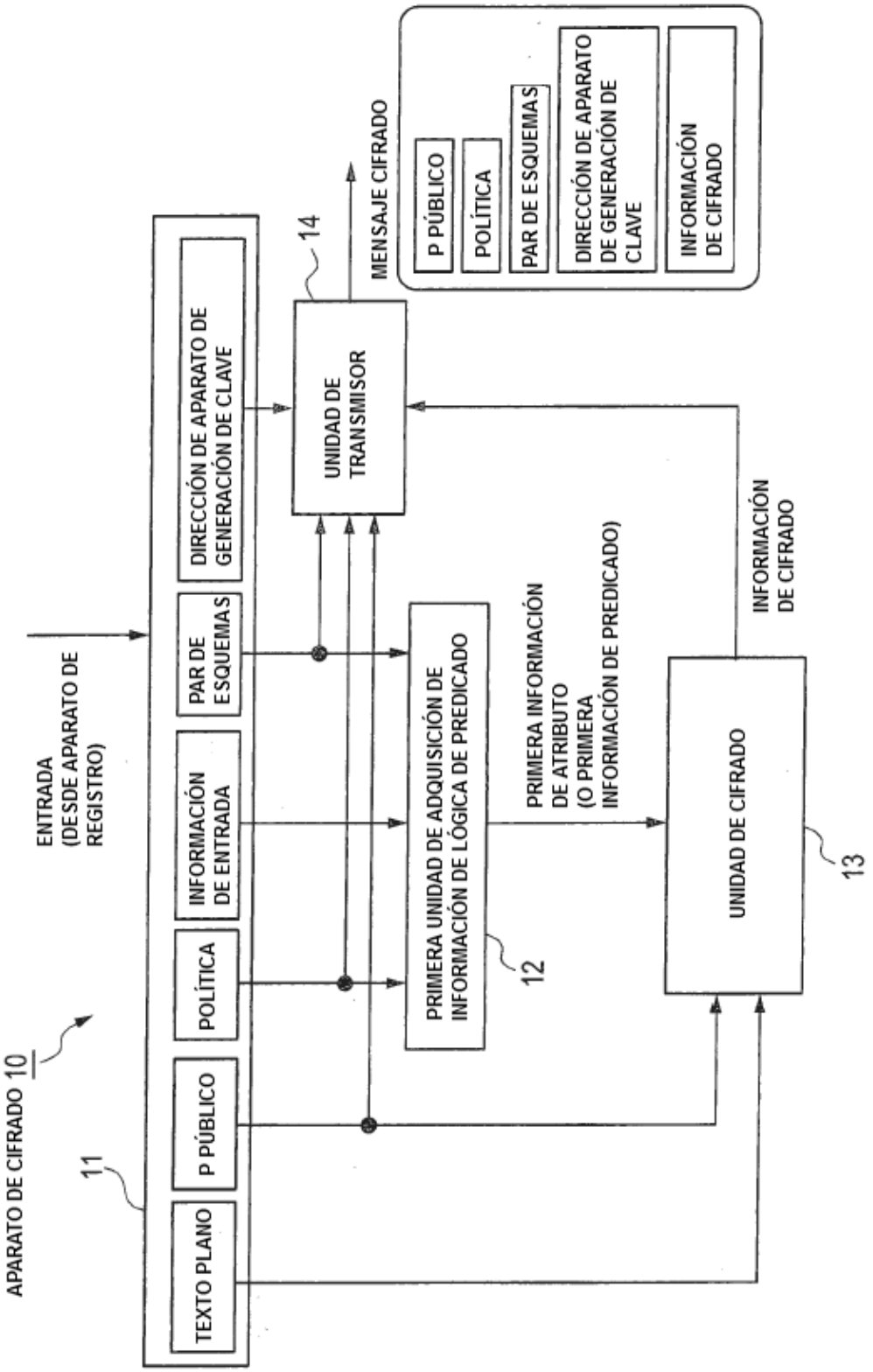

APARATO DE CIFRADO 10
11
ENTRADA
(DESDE APARATO DE
REGISTRO)
TEXTO PLANO
P PÚBLICO
POLÍTICA
INFORMACIÓN
DE ENTRADA
PAR DE
ESQUEMAS
DIRECCIÓN DE APARATO DE
GENERACIÓN DE CLAVE
PRIMERA UNIDAD DE ADQUISICIÓN DE
INFORMACIÓN DE LÓGICA DE PREDICADO
12
PRIMERA INFORMACIÓN
DE ATRIBUTO
(O PRIMERA
INFORMACIÓN DE PREDICADO)
UNIDAD DE CIFRADO
13
INFORMACIÓN
DE CIFRADO
UNIDAD DE
TRANSMISOR
14
MENSAJE CIFRADO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO
DE GENERACIÓN DE
CLAVE
INFORMACIÓN
DE CIFRADO

FIG.50

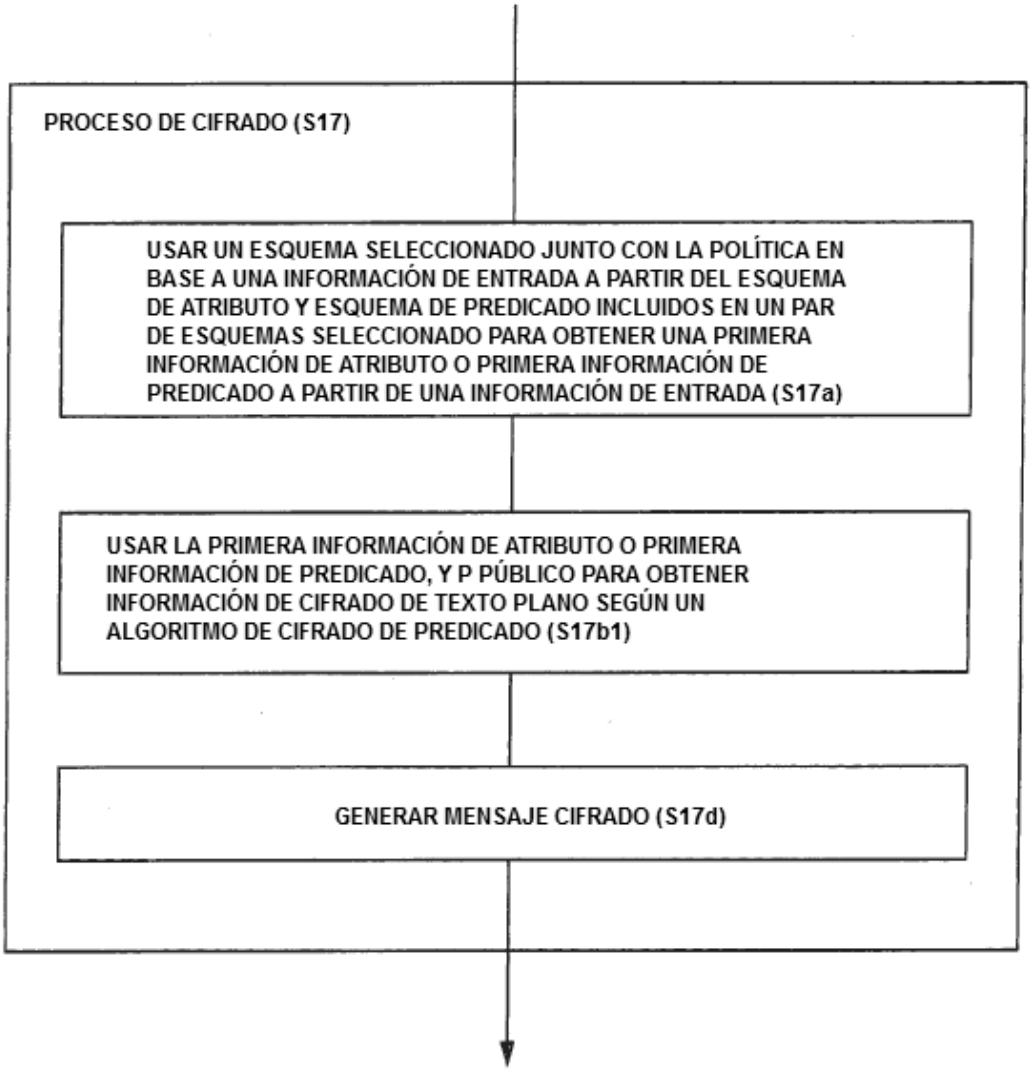

PROCESO DE CIFRADO (S17)
USAR UN ESQUEMA SELECCIONADO JUNTO CON LA POLÍTICA EN BASE A UNA INFORMACIÓN DE ENTRADA A PARTIR DEL ESQUEMA DE ATRIBUTO Y ESQUEMA DE PREDICADO INCLUIDOS EN UN PAR DE ESQUEMAS SELECCIONADO PARA OBTENER UNA PRIMERA INFORMACIÓN DE ATRIBUTO O PRIMERA INFORMACIÓN DE PREDICADO A PARTIR DE UNA INFORMACIÓN DE ENTRADA (S17a)
USAR LA PRIMERA INFORMACIÓN DE ATRIBUTO O PRIMERA INFORMACIÓN DE PREDICADO, Y P PÚBLICO PARA OBTENER INFORMACIÓN DE CIFRADO DE TEXTO PLANO SEGÚN UN ALGORITMO DE CIFRADO DE PREDICADO (S17b1)
GENERAR MENSAJE CIFRADO (S17d)

FIG.51

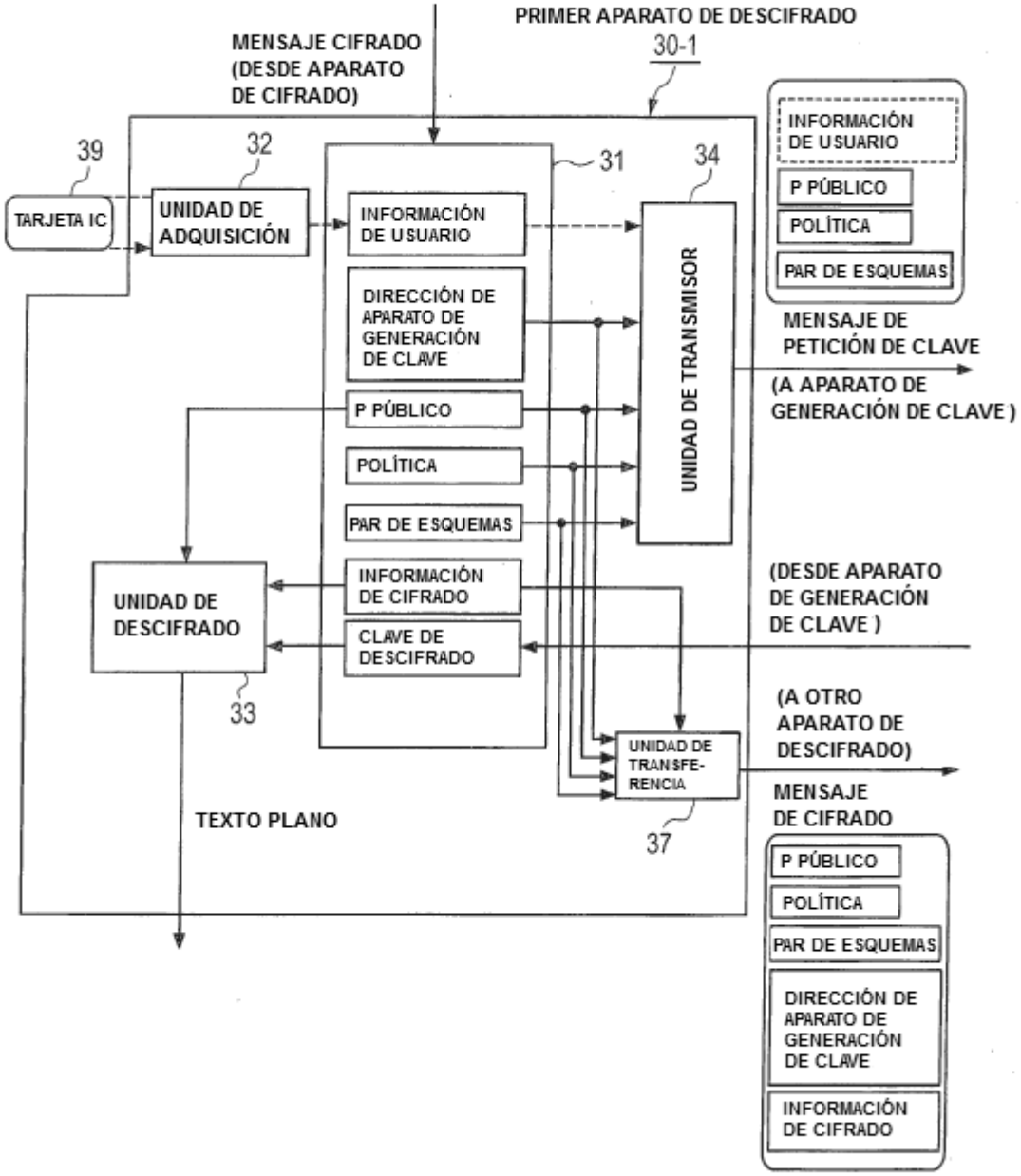

PRIMER APARATO DE DESCIFRADO
30-1
MENSAJE CIFRADO (DESDE APARATO DE CIFRADO)
39
32
31
34
TARJETA IC
UNIDAD DE ADQUISICIÓN
INFORMACIÓN DE USUARIO
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
UNIDAD DE TRANSMISOR
INFORMACIÓN DE USUARIO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
MENSAJE DE PETICIÓN DE CLAVE
(A APARATO DE GENERACIÓN DE CLAVE)
(DESDE APARATO DE GENERACIÓN DE CLAVE)
UNIDAD DE DESCIFRADO
INFORMACIÓN DE CIFRADO
CLAVE DE DESCIFRADO
33
UNIDAD DE TRANSFE-RENCIA
37
(A OTRO APARATO DE DESCIFRADO)
MENSAJE DE CIFRADO
TEXTO PLANO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
INFORMACIÓN DE CIFRADO

FIG.52

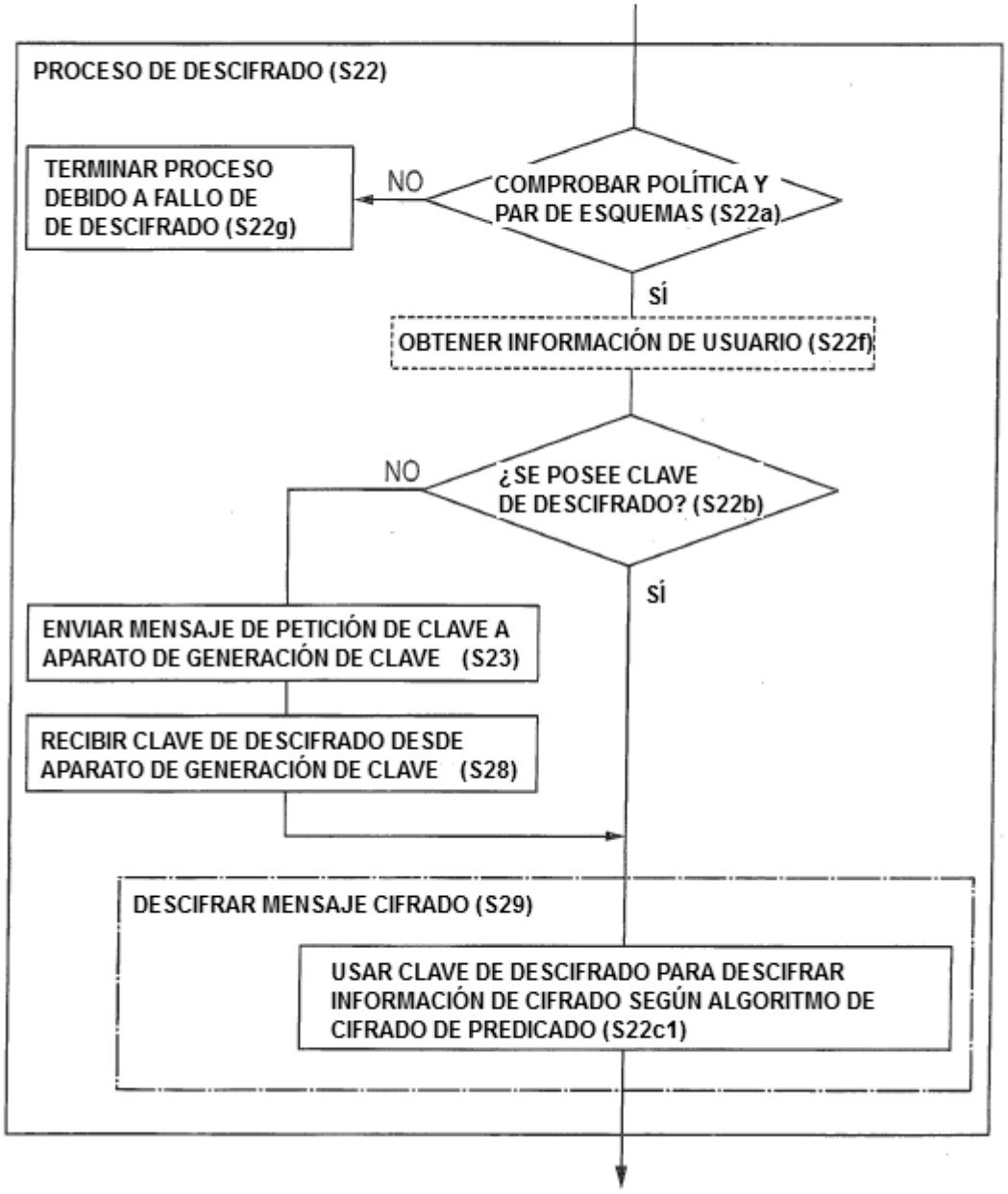

PROCESO DE DESCIFRADO (S22)
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S22a)
NO
TERMINAR PROCESO DEBIDO A FALLO DE DE DESCIFRADO (S22g)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S22f)
¿SE POSEE CLAVE DE DESCIFRADO? (S22b)
NO
SÍ
ENVIAR MENSAJE DE PETICIÓN DE CLAVE A APARATO DE GENERACIÓN DE CLAVE (S23)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACIÓN DE CLAVE (S28)
DESCIFRAR MENSAJE CIFRADO (S29)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGÚN ALGORITMO DE CIFRADO DE PREDICADO (S22c1)

FIG.53

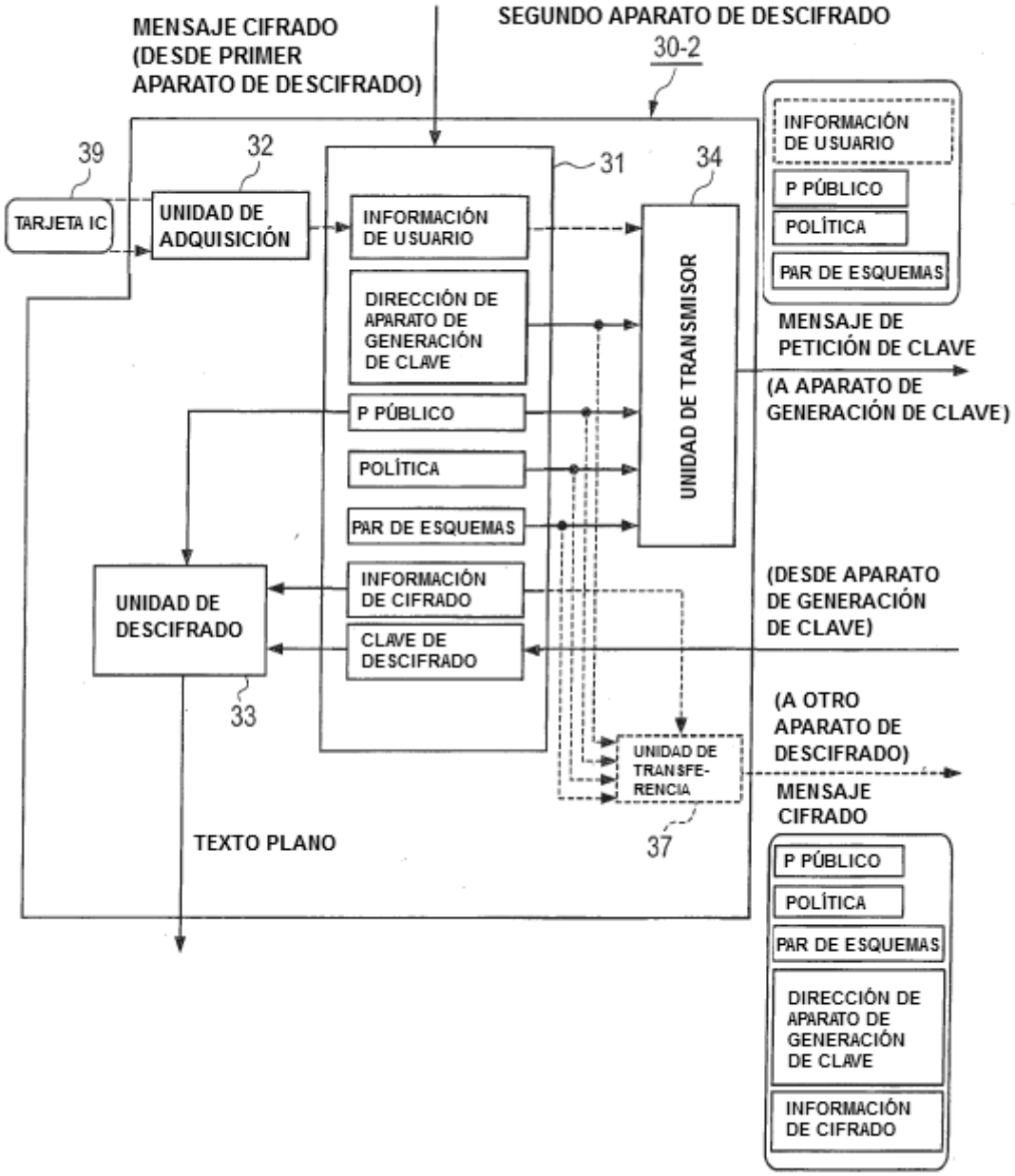

MENSAJE CIFRADO
(DESDE PRIMER
APARATO DE DESCIFRADO)
SEGUNDO APARATO DE DESCIFRADO
30-2
39
32
31
34
TARJETA IC
UNIDAD DE
ADQUISICIÓN
INFORMACIÓN
DE USUARIO
DIRECCIÓN DE
APARATO DE
GENERACIÓN
DE CLAVE
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
UNIDAD DE TRANSMISOR
INFORMACIÓN
DE USUARIO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
MENSAJE DE
PETICIÓN DE CLAVE
(A APARATO DE
GENERACIÓN DE CLAVE)
UNIDAD DE
DESCIFRADO
INFORMACIÓN
DE CIFRADO
CLAVE DE
DESCIFRADO
(DESDE APARATO
DE GENERACIÓN
DE CLAVE)
33
UNIDAD DE
TRANSFE-
RENCIA
(A OTRO
APARATO DE
DESCIFRADO)
MENSAJE
CIFRADO
37
TEXTO PLANO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE
APARATO DE
GENERACIÓN
DE CLAVE
INFORMACIÓN
DE CIFRADO

FIG.54

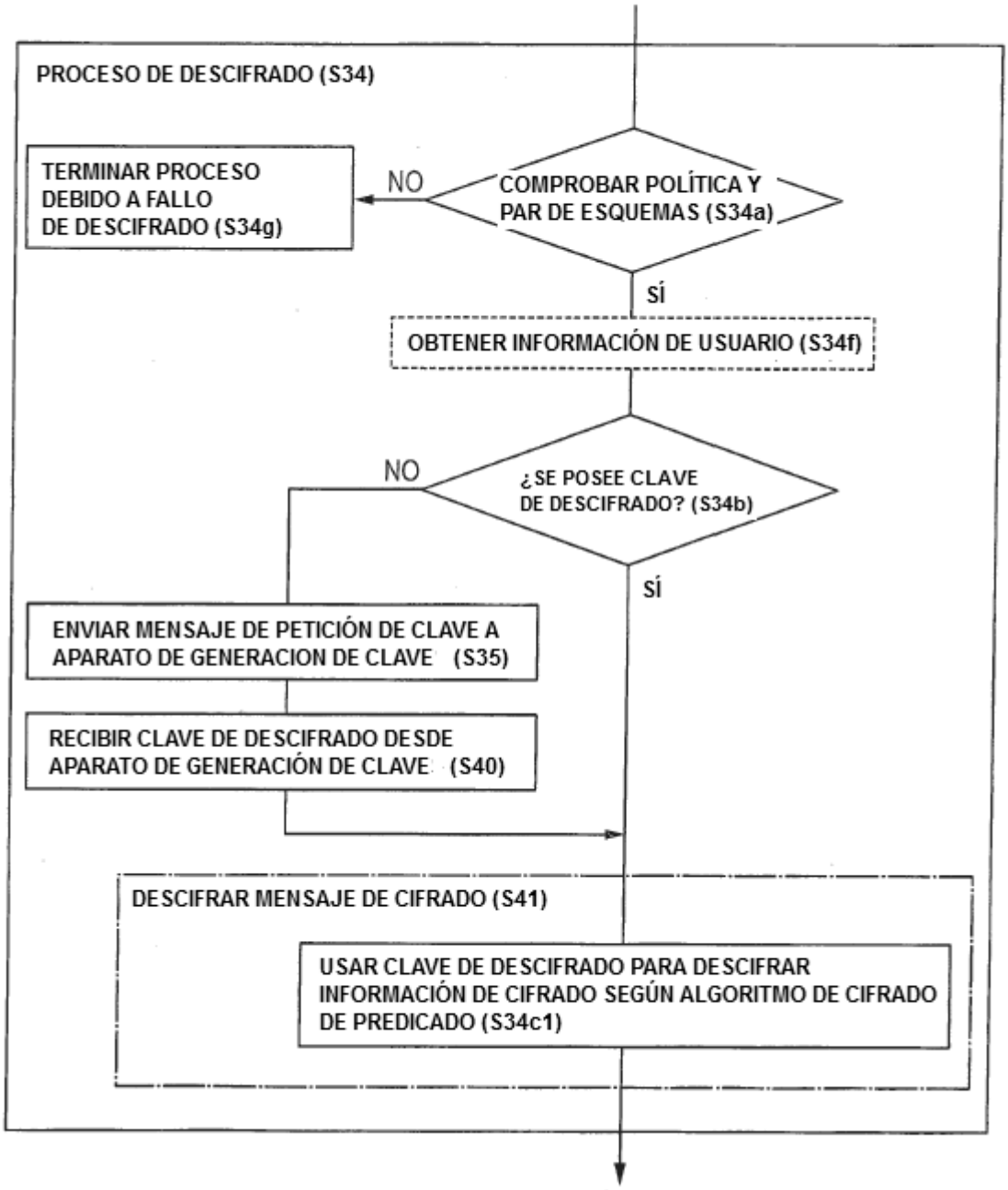

PROCESO DE DESCIFRADO (S34)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S34g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S34a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S34f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S34b)
SÍ
ENVIAR MENSAJE DE PETICIÓN DE CLAVE A APARATO DE GENERACION DE CLAVE (S35)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACIÓN DE CLAVE (S40)
DESCIFRAR MENSAJE DE CIFRADO (S41)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGÚN ALGORITMO DE CIFRADO DE PREDICADO (S34c1)

FIG.55

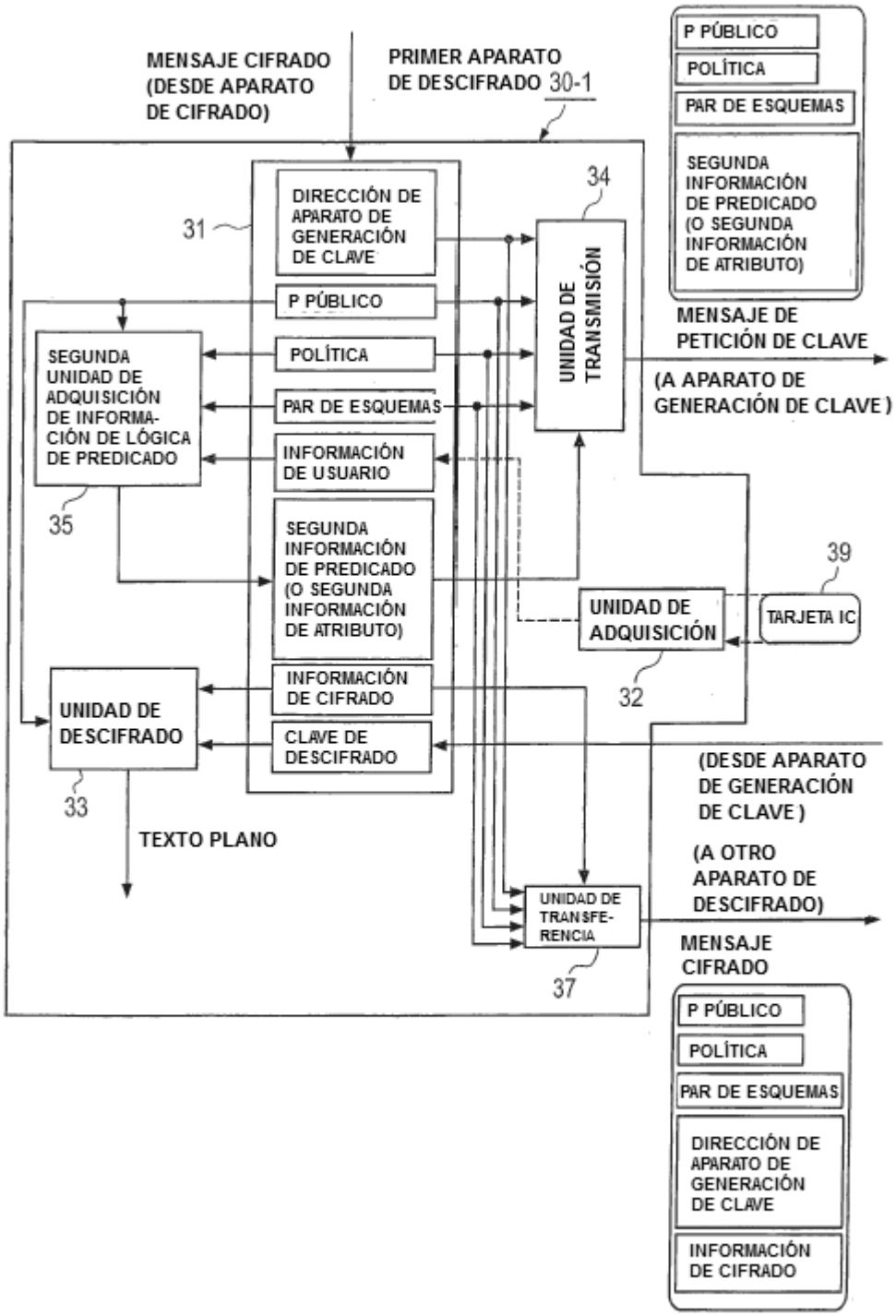

MENSAJE CIFRADO (DESDE APARATO DE CIFRADO)
PRIMER APARATO DE DESCIFRADO 30-1
31
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
INFORMACIÓN DE USUARIO
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
INFORMACIÓN DE CIFRADO
CLAVE DE DESCIFRADO
34
UNIDAD DE TRANSMISIÓN
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
MENSAJE DE PETICIÓN DE CLAVE
(A APARATO DE GENERACIÓN DE CLAVE)
SEGUNDA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
35
39
UNIDAD DE ADQUISICIÓN
TARJETA IC
32
UNIDAD DE DESCIFRADO
33
TEXTO PLANO
(DESDE APARATO DE GENERACIÓN DE CLAVE)
(A OTRO APARATO DE DESCIFRADO)
UNIDAD DE TRANSFERENCIA
37
MENSAJE CIFRADO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
INFORMACIÓN DE CIFRADO

FIG.56

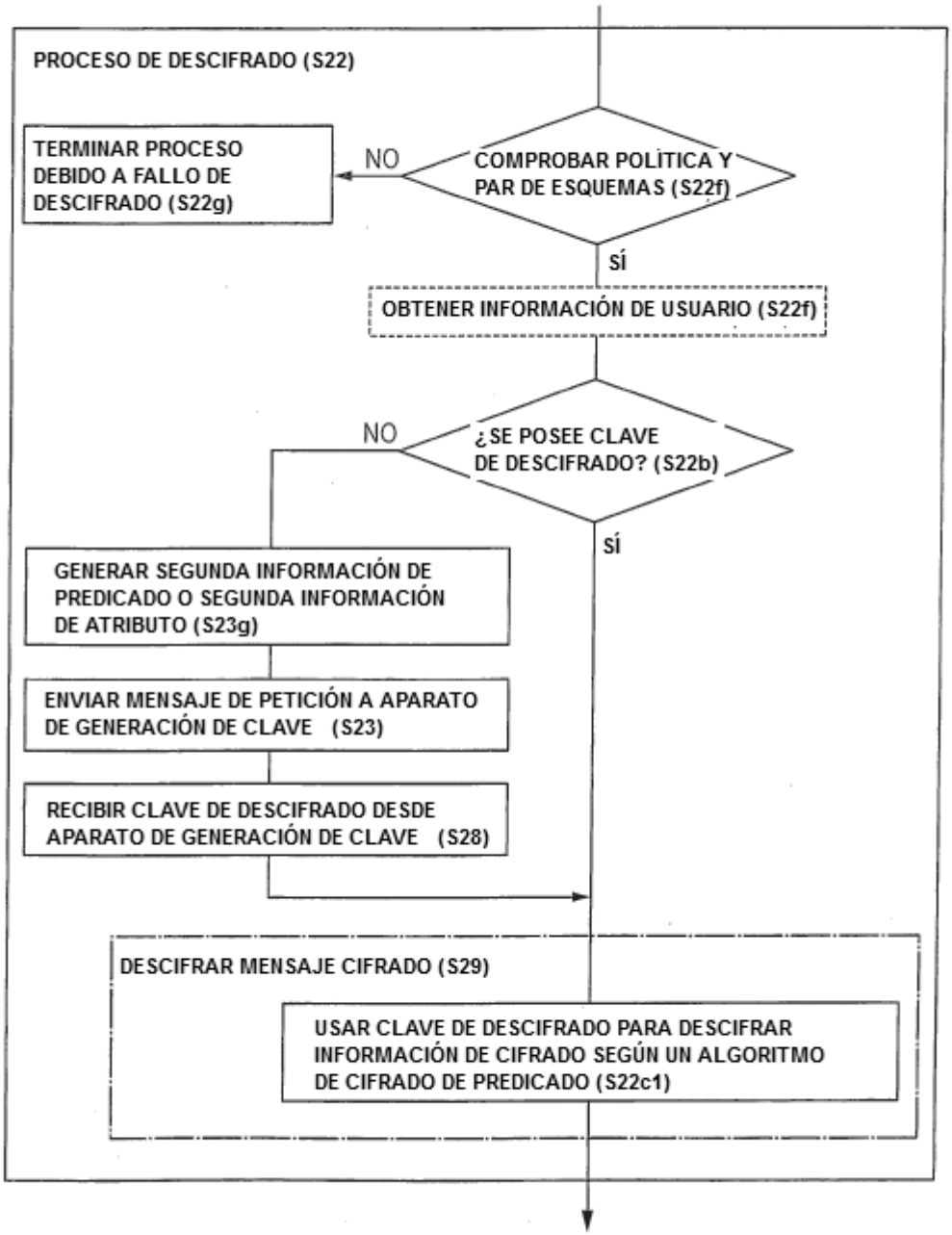

PROCESO DE DESCIFRADO (S22)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S22g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S22f)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S22f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S22b)
SÍ
GENERAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO (S23g)
ENVIAR MENSAJE DE PETICIÓN A APARATO DE GENERACIÓN DE CLAVE (S23)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACIÓN DE CLAVE (S28)
DESCIFRAR MENSAJE CIFRADO (S29)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGÚN UN ALGORITMO DE CIFRADO DE PREDICADO (S22c1)

FIG.57

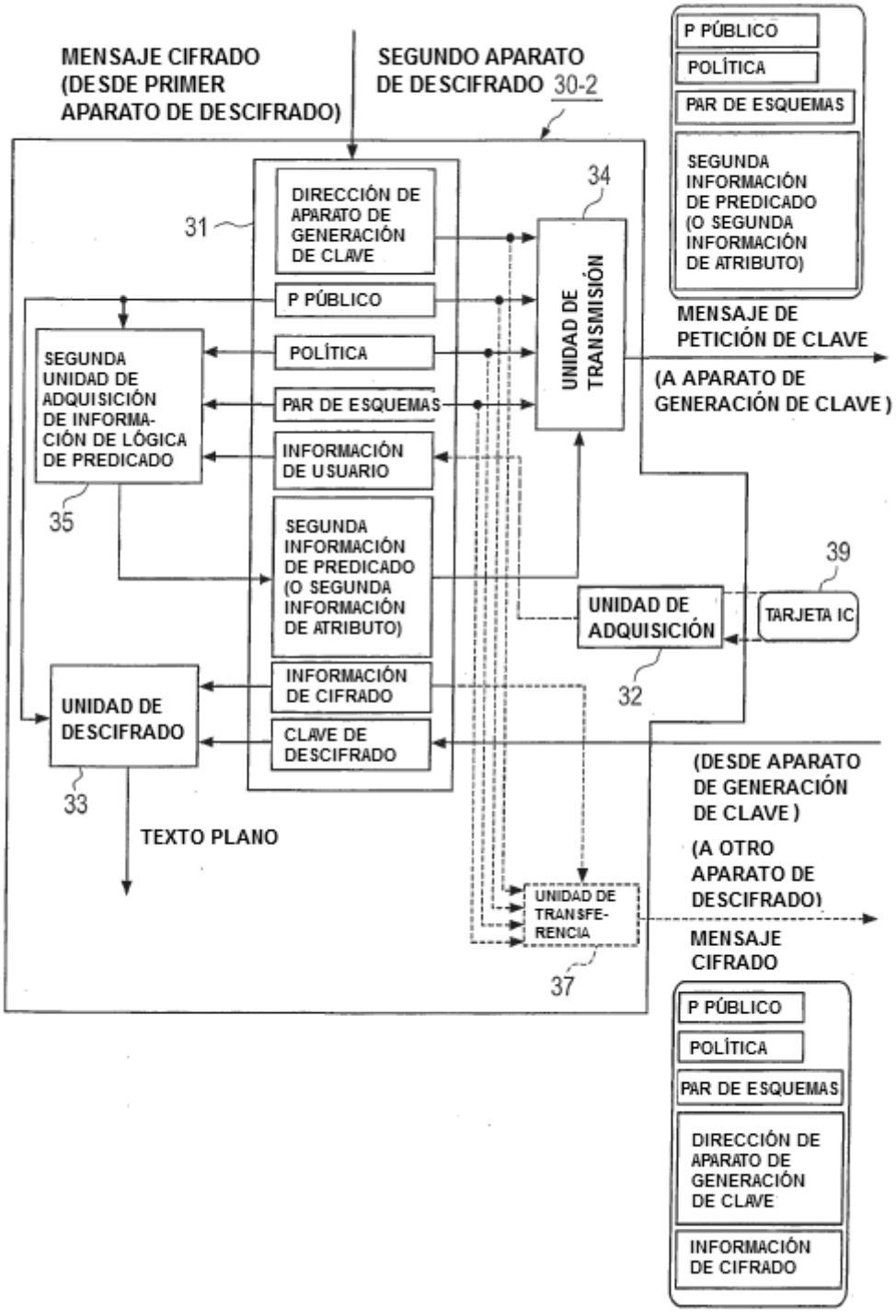

MENSAJE CIFRADO (DESDE PRIMER APARATO DE DESCIFRADO)
SEGUNDO APARATO DE DESCIFRADO 30-2
31
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
INFORMACIÓN DE USUARIO
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
INFORMACIÓN DE CIFRADO
CLAVE DE DESCIFRADO
34
UNIDAD DE TRANSMISIÓN
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
MENSAJE DE PETICIÓN DE CLAVE
(A APARATO DE GENERACIÓN DE CLAVE)
SEGUNDA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
35
39
UNIDAD DE ADQUISICIÓN
TARJETA IC
32
UNIDAD DE DESCIFRADO
33
TEXTO PLANO
(DESDE APARATO DE GENERACIÓN DE CLAVE)
(A OTRO APARATO DE DESCIFRADO)
UNIDAD DE TRANSFERENCIA
37
MENSAJE CIFRADO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
INFORMACIÓN DE CIFRADO

FIG.58

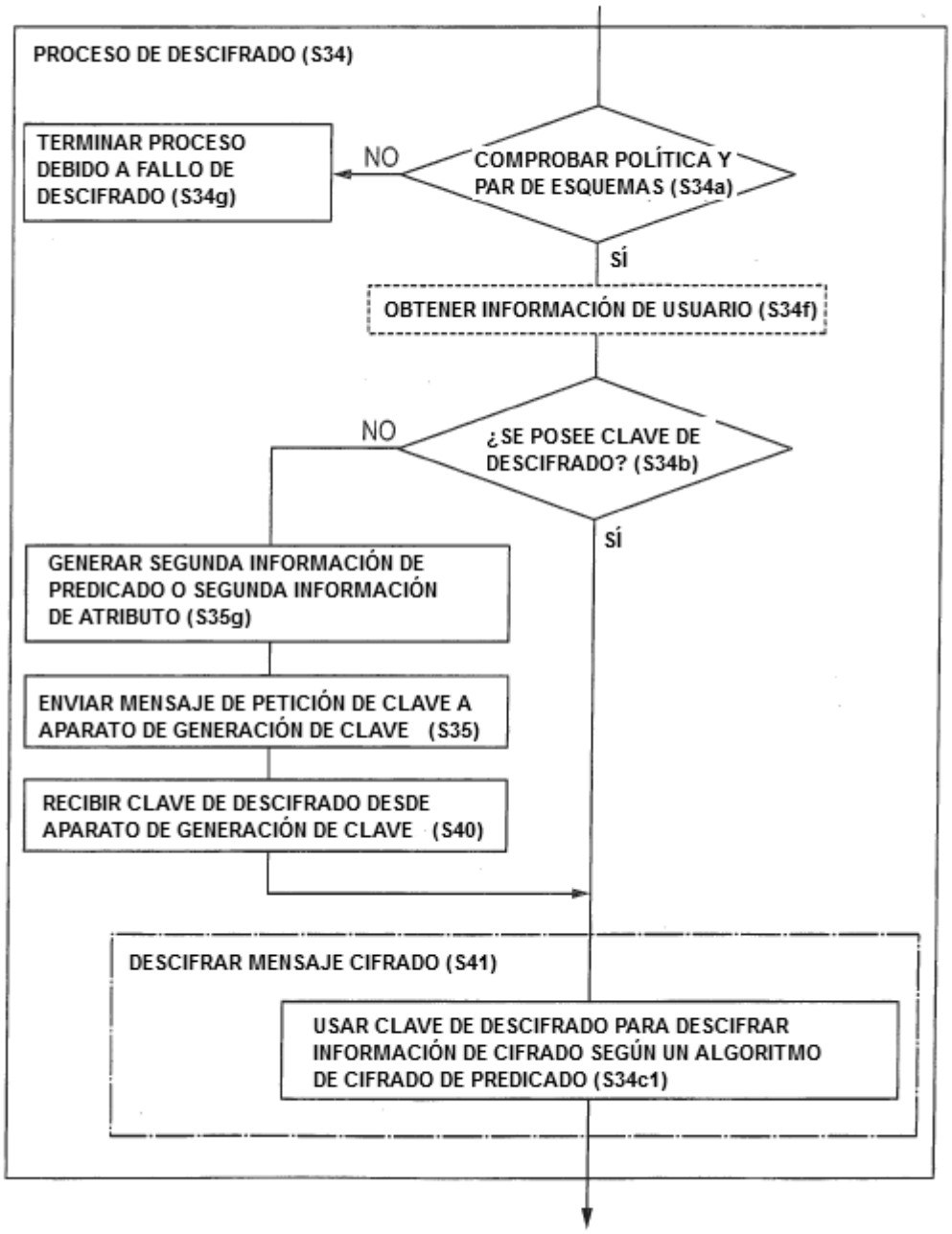

PROCESO DE DESCIFRADO (S34)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S34g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S34a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S34f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S34b)
SÍ
GENERAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO (S35g)
ENVIAR MENSAJE DE PETICIÓN DE CLAVE A APARATO DE GENERACIÓN DE CLAVE (S35)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACIÓN DE CLAVE (S40)
DESCIFRAR MENSAJE CIFRADO (S41)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGÚN UN ALGORITMO DE CIFRADO DE PREDICADO (S34c1)

FIG.59

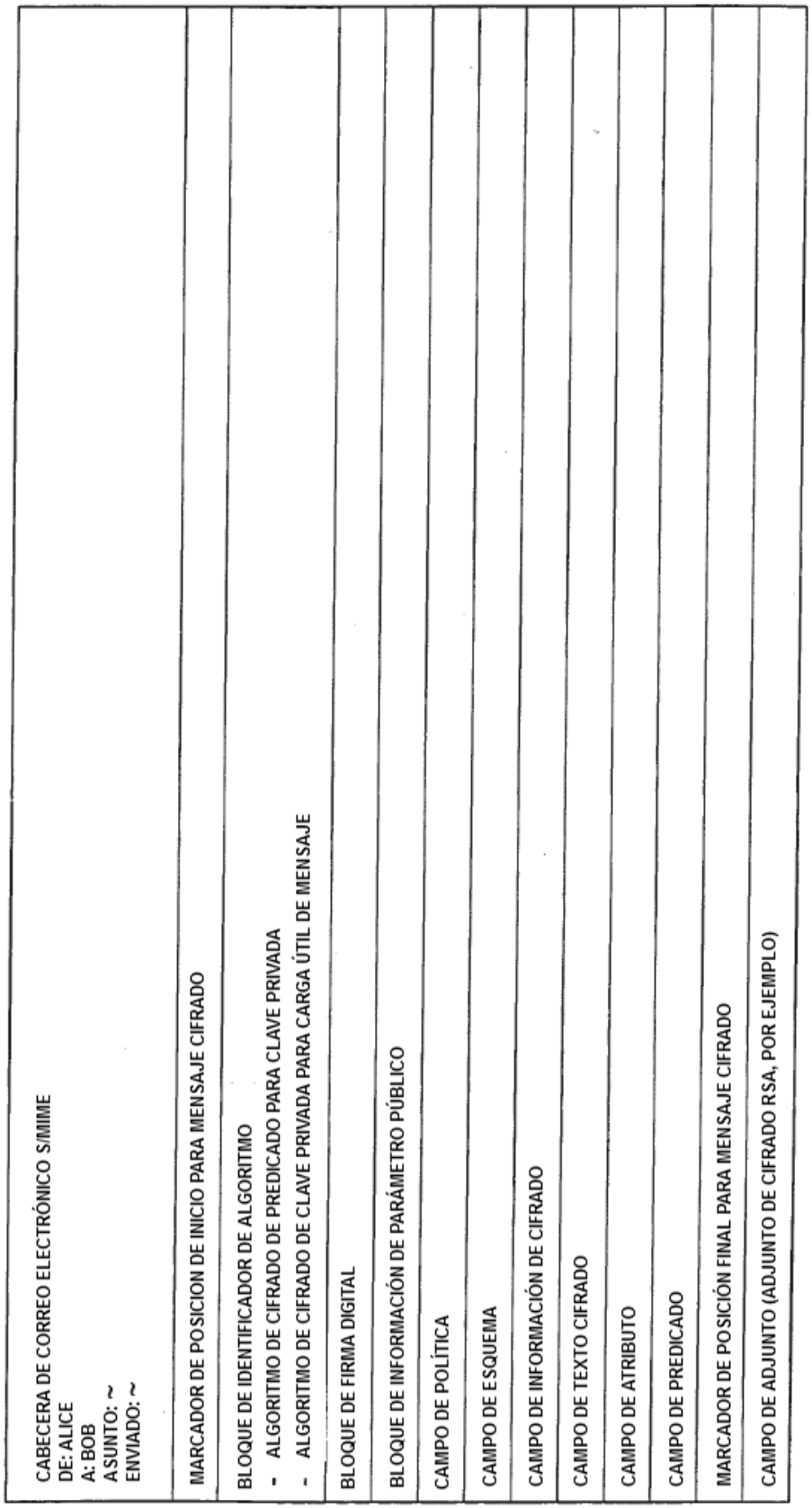

CABECERA DE CORREO ELECTRÓNICO S/MIME
DE: ALICE
A: BOB
ASUNTO: ~
ENVIADO: ~
MARCADOR DE POSICION DE INICIO PARA MENSAJE CIFRADO
BLOQUE DE IDENTIFICADOR DE ALGORITMO
- ALGORITMO DE CIFRADO DE PREDICADO PARA CLAVE PRIVADA
- ALGORITMO DE CIFRADO DE CLAVE PRIVADA PARA CARGA ÚTIL DE MENSAJE
BLOQUE DE FIRMA DIGITAL
BLOQUE DE INFORMACIÓN DE PARÁMETRO PÚBLICO
CAMPO DE POLÍTICA
CAMPO DE ESQUEMA
CAMPO DE INFORMACIÓN DE CIFRADO
CAMPO DE TEXTO CIFRADO
CAMPO DE ATRIBUTO
CAMPO DE PREDICADO
MARCADOR DE POSICIÓN FINAL PARA MENSAJE CIFRADO
CAMPO DE ADJUNTO (ADJUNTO DE CIFRADO RSA, POR EJEMPLO)

FIG.60

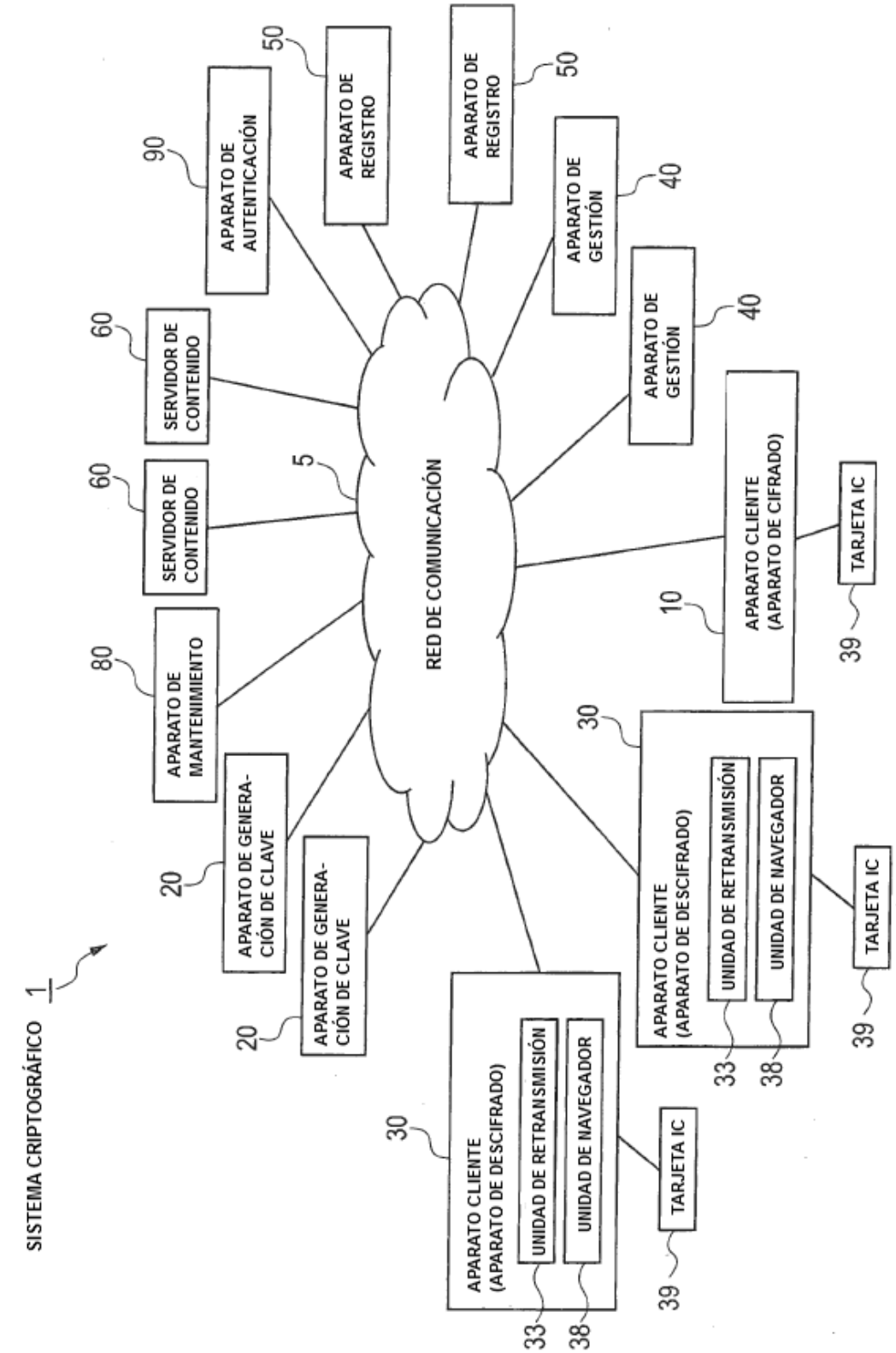

SISTEMA CRIPTOGRÁFICO 1
RED DE COMUNICACIÓN 5
APARATO DE AUTENTICACIÓN 90
APARATO DE REGISTRO 50
APARATO DE REGISTRO 50
APARATO DE GESTIÓN 40
APARATO DE GESTIÓN 40
SERVIDOR DE CONTENIDO 60
SERVIDOR DE CONTENIDO 60
APARATO DE MANTENIMIENTO 80
APARATO DE GENERACIÓN DE CLAVE 20
APARATO DE GENERACIÓN DE CLAVE 20
APARATO CLIENTE (APARATO DE CIFRADO) 10
TARJETA IC 39
APARATO CLIENTE (APARATO DE DESCIFRADO) 30
UNIDAD DE RETRANSMISIÓN 33
UNIDAD DE NAVEGADOR 38
TARJETA IC 39
APARATO CLIENTE (APARATO DE DESCIFRADO) 30
UNIDAD DE RETRANSMISIÓN 33
UNIDAD DE NAVEGADOR 38
TARJETA IC 39

FIG.61

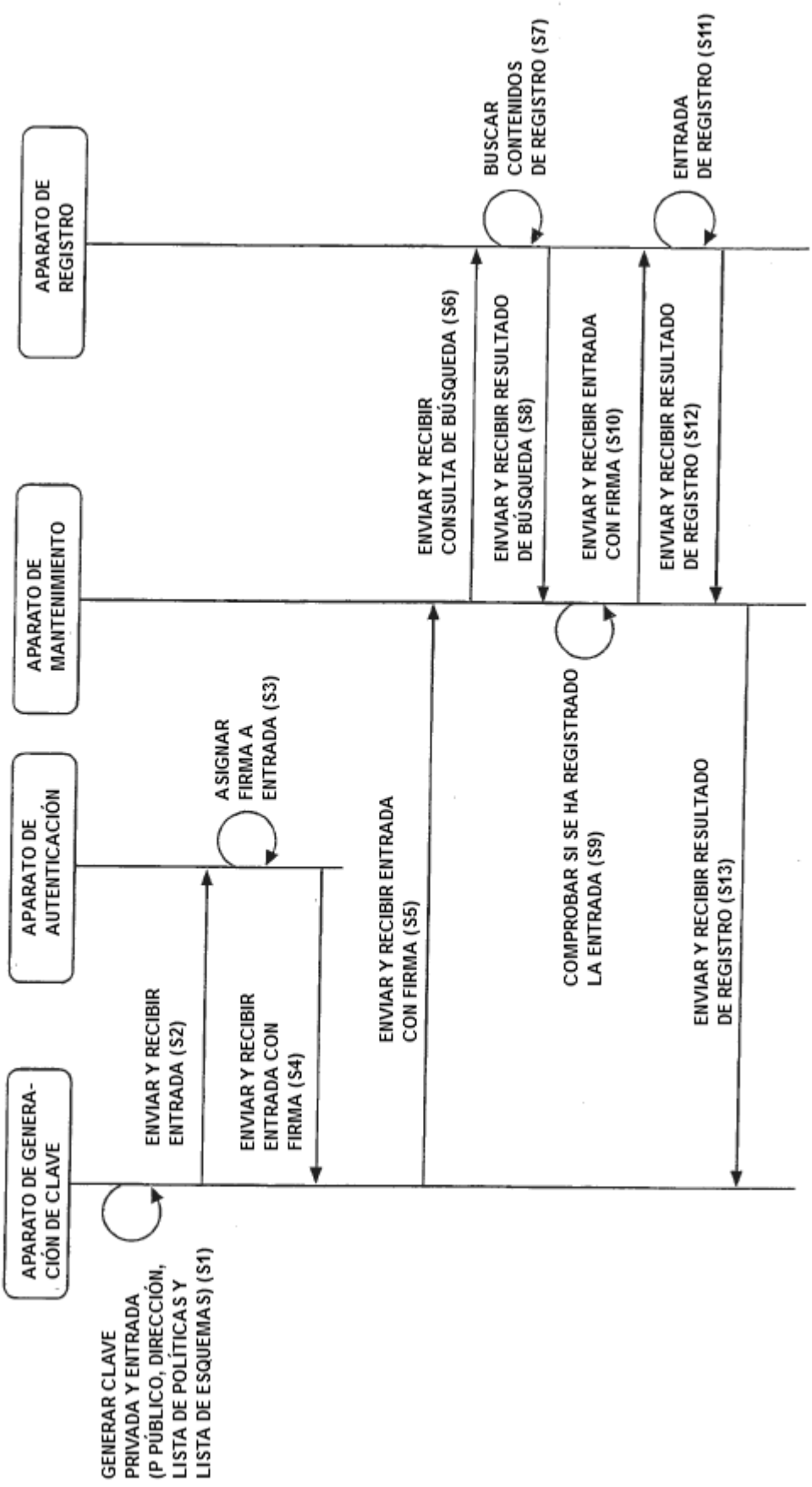

APARATO DE GENERACIÓN DE CLAVE
APARATO DE AUTENTICACIÓN
APARATO DE MANTENIMIENTO
APARATO DE REGISTRO
GENERAR CLAVE PRIVADA Y ENTRADA (P PÚBLICO, DIRECCIÓN, LISTA DE POLÍTICAS Y LISTA DE ESQUEMAS) (S1)
ENVIAR Y RECIBIR ENTRADA (S2)
ASIGNAR FIRMA A ENTRADA (S3)
ENVIAR Y RECIBIR ENTRADA CON FIRMA (S4)
ENVIAR Y RECIBIR ENTRADA CON FIRMA (S5)
ENVIAR Y RECIBIR CONSULTA DE BÚSQUEDA (S6)
BUSCAR CONTENIDOS DE REGISTRO (S7)
ENVIAR Y RECIBIR RESULTADO DE BÚSQUEDA (S8)
COMPROBAR SI SE HA REGISTRADO LA ENTRADA (S9)
ENVIAR Y RECIBIR ENTRADA CON FIRMA (S10)
ENTRADA DE REGISTRO (S11)
ENVIAR Y RECIBIR RESULTADO DE REGISTRO (S12)
ENVIAR Y RECIBIR RESULTADO DE REGISTRO (S13)

FIG.62

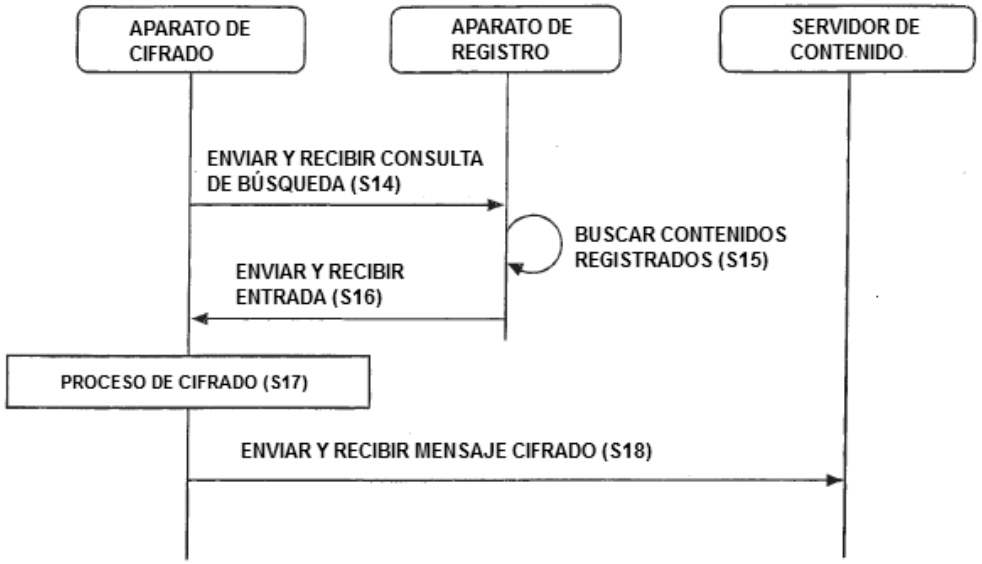
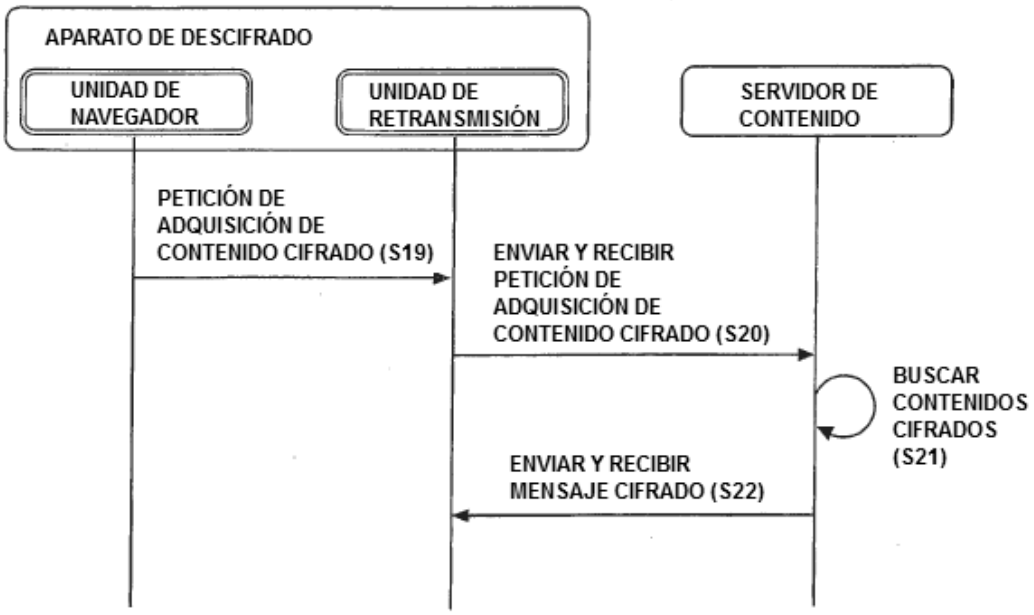

APARATO DE CIFRADO
APARATO DE REGISTRO
SERVIDOR DE CONTENIDO
ENVIAR Y RECIBIR CONSULTA DE BÚSQUEDA (S14)
BUSCAR CONTENIDOS REGISTRADOS (S15)
ENVIAR Y RECIBIR ENTRADA (S16)
PROCESO DE CIFRADO (S17)
ENVIAR Y RECIBIR MENSAJE CIFRADO (S18)

FIG.63


APARATO DE DESCIFRADO
UNIDAD DE NAVEGADOR
UNIDAD DE RETRANSMISIÓN
SERVIDOR DE CONTENIDO
PETICIÓN DE ADQUISICIÓN DE CONTENIDO CIFRADO (S19)
ENVIAR Y RECIBIR PETICIÓN DE ADQUISICIÓN DE CONTENIDO CIFRADO (S20)
BUSCAR CONTENIDOS CIFRADOS (S21)
ENVIAR Y RECIBIR MENSAJE CIFRADO (S22)

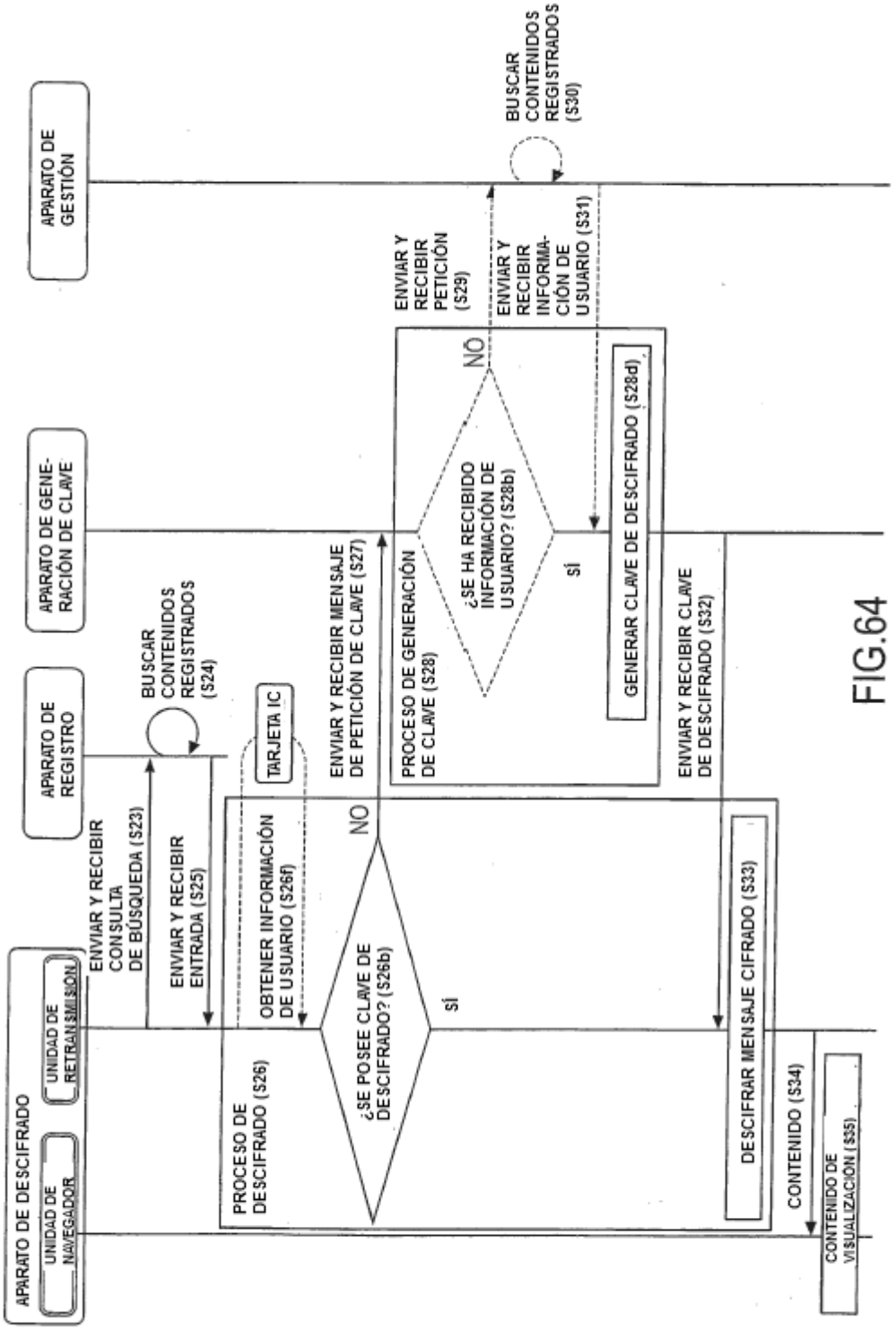

APARATO DE DESCIFRADO
UNIDAD DE NAVEGADOR
UNIDAD DE RETRANSMISIÓN
APARATO DE REGISTRO
APARATO DE GENERACIÓN DE CLAVE
APARATO DE GESTIÓN
ENVIAR Y RECIBIR CONSULTA DE BÚSQUEDA (S23)
BUSCAR CONTENIDOS REGISTRADOS (S24)
ENVIAR Y RECIBIR ENTRADA (S25)
PROCESO DE DESCIFRADO (S26)
OBTENER INFORMACIÓN DE USUARIO (S26f)
TARJETA IC
¿SE POSEE CLAVE DE DESCIFRADO? (S26b)
NO
SÍ
ENVIAR Y RECIBIR MENSAJE DE PETICIÓN DE CLAVE (S27)
PROCESO DE GENERACIÓN DE CLAVE (S28)
¿SE HA RECIBIDO INFORMACIÓN DE USUARIO? (S28b)
NO
SÍ
ENVIAR Y RECIBIR PETICIÓN (S29)
BUSCAR CONTENIDOS REGISTRADOS (S30)
ENVIAR Y RECIBIR INFORMACIÓN DE USUARIO (S31)
GENERAR CLAVE DE DESCIFRADO (S28d)
ENVIAR Y RECIBIR CLAVE DE DESCIFRADO (S32)
DESCIFRAR MENSAJE CIFRADO (S33)
CONTENIDO (S34)
CONTENIDO DE VISUALIZACIÓN (S35)

FIG.64

FIG.65

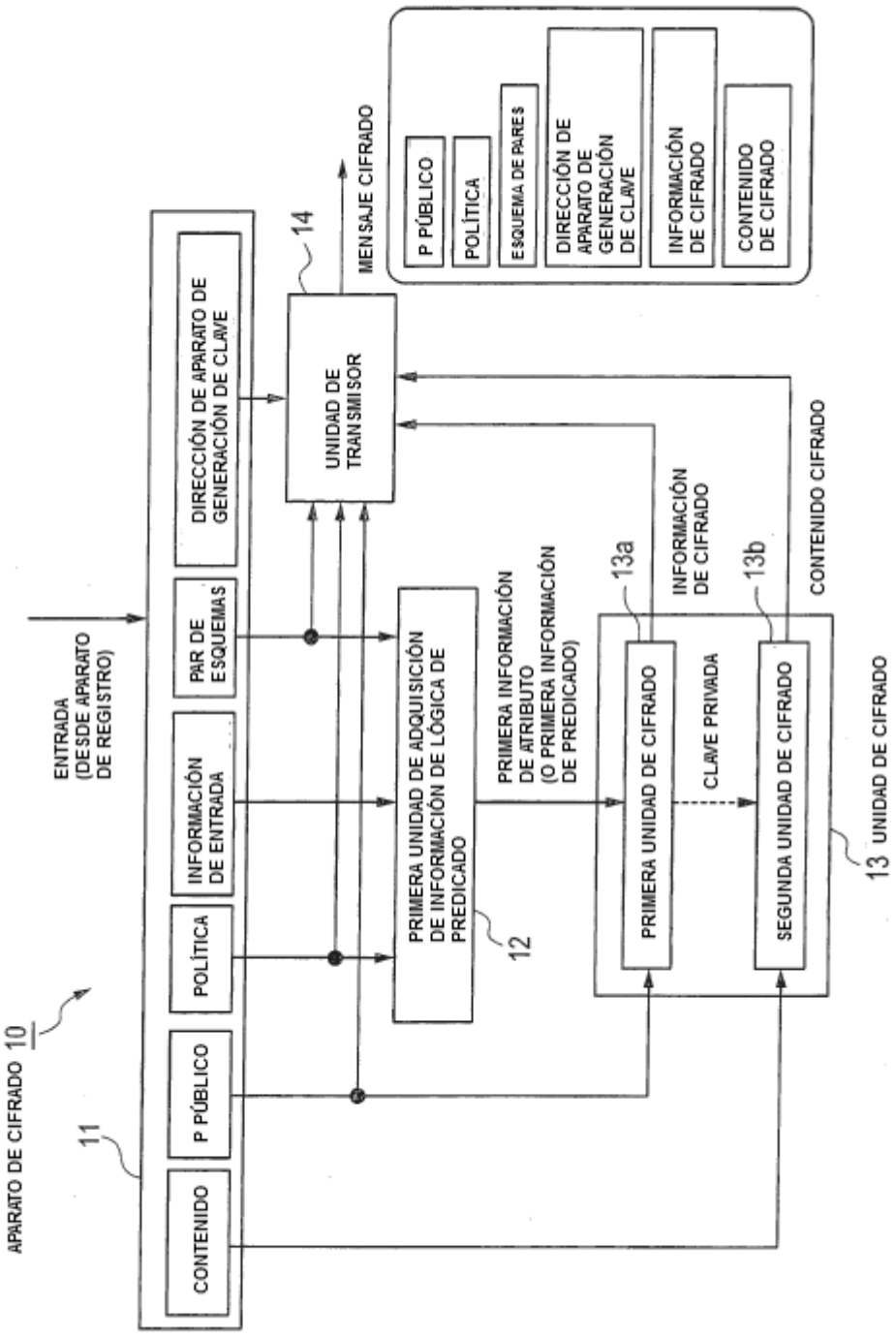

APARATO DE CIFRADO 10
11
CONTENIDO
P PÚBLICO
POLÍTICA
INFORMACIÓN DE ENTRADA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
ENTRADA (DESDE APARATO DE REGISTRO)
PRIMERA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
12
PRIMERA INFORMACIÓN DE ATRIBUTO (O PRIMERA INFORMACIÓN DE PREDICADO)
UNIDAD DE TRANSMISOR
14
MENSAJE CIFRADO
P PÚBLICO
POLÍTICA
ESQUEMA DE PARES
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
INFORMACIÓN DE CIFRADO
CONTENIDO DE CIFRADO
13a
PRIMERA UNIDAD DE CIFRADO
CLAVE PRIVADA
13b
SEGUNDA UNIDAD DE CIFRADO
INFORMACIÓN DE CIFRADO
CONTENIDO CIFRADO
13 UNIDAD DE CIFRADO

FIG.66

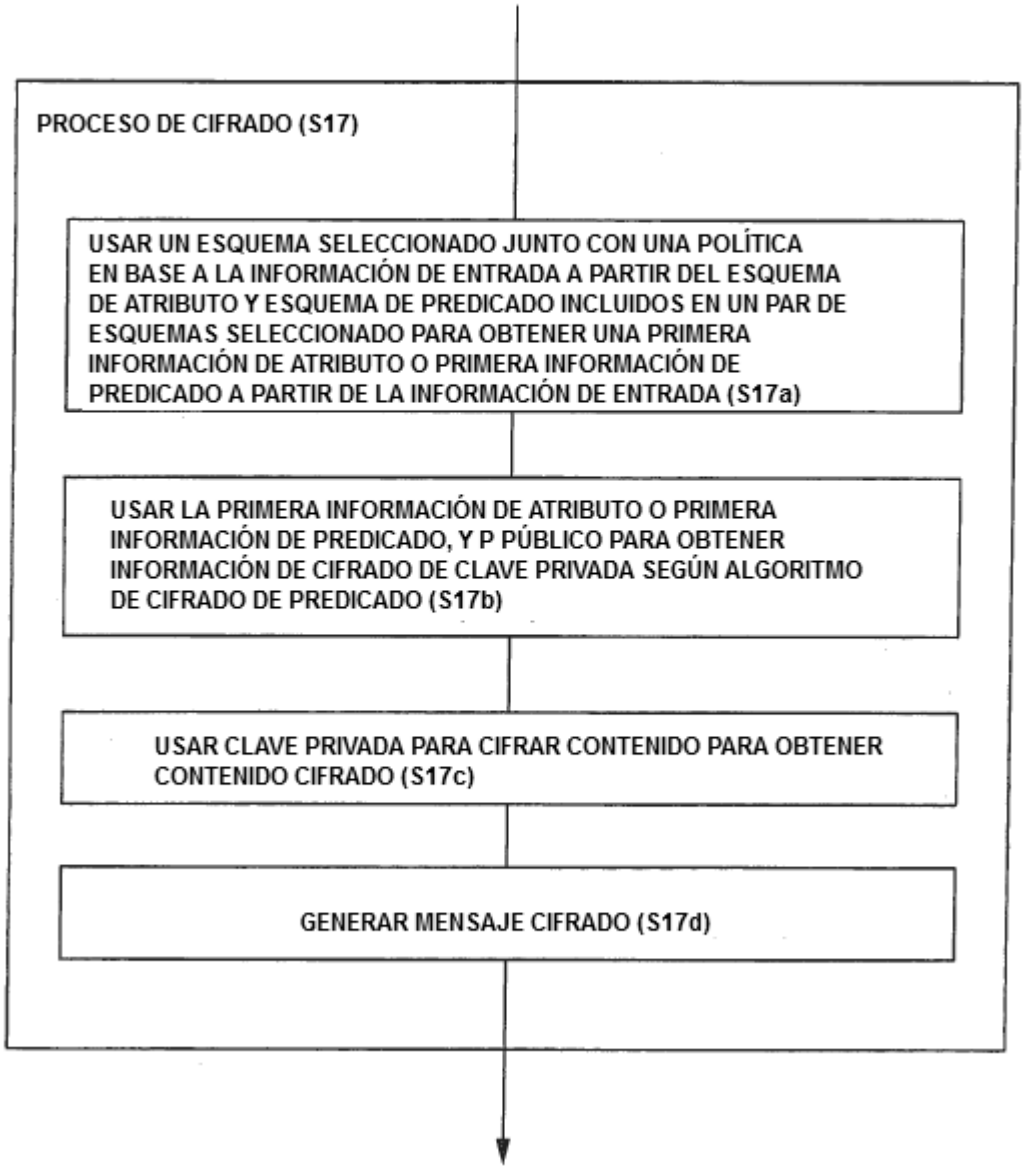

PROCESO DE CIFRADO (S17)
USAR UN ESQUEMA SELECCIONADO JUNTO CON UNA POLÍTICA EN BASE A LA INFORMACIÓN DE ENTRADA A PARTIR DEL ESQUEMA DE ATRIBUTO Y ESQUEMA DE PREDICADO INCLUIDOS EN UN PAR DE ESQUEMAS SELECCIONADO PARA OBTENER UNA PRIMERA INFORMACIÓN DE ATRIBUTO O PRIMERA INFORMACIÓN DE PREDICADO A PARTIR DE LA INFORMACIÓN DE ENTRADA (S17a)
USAR LA PRIMERA INFORMACIÓN DE ATRIBUTO O PRIMERA INFORMACIÓN DE PREDICADO, Y P PÚBLICO PARA OBTENER INFORMACIÓN DE CIFRADO DE CLAVE PRIVADA SEGÚN ALGORITMO DE CIFRADO DE PREDICADO (S17b)
USAR CLAVE PRIVADA PARA CIFRAR CONTENIDO PARA OBTENER CONTENIDO CIFRADO (S17c)
GENERAR MENSAJE CIFRADO (S17d)

FIG.67

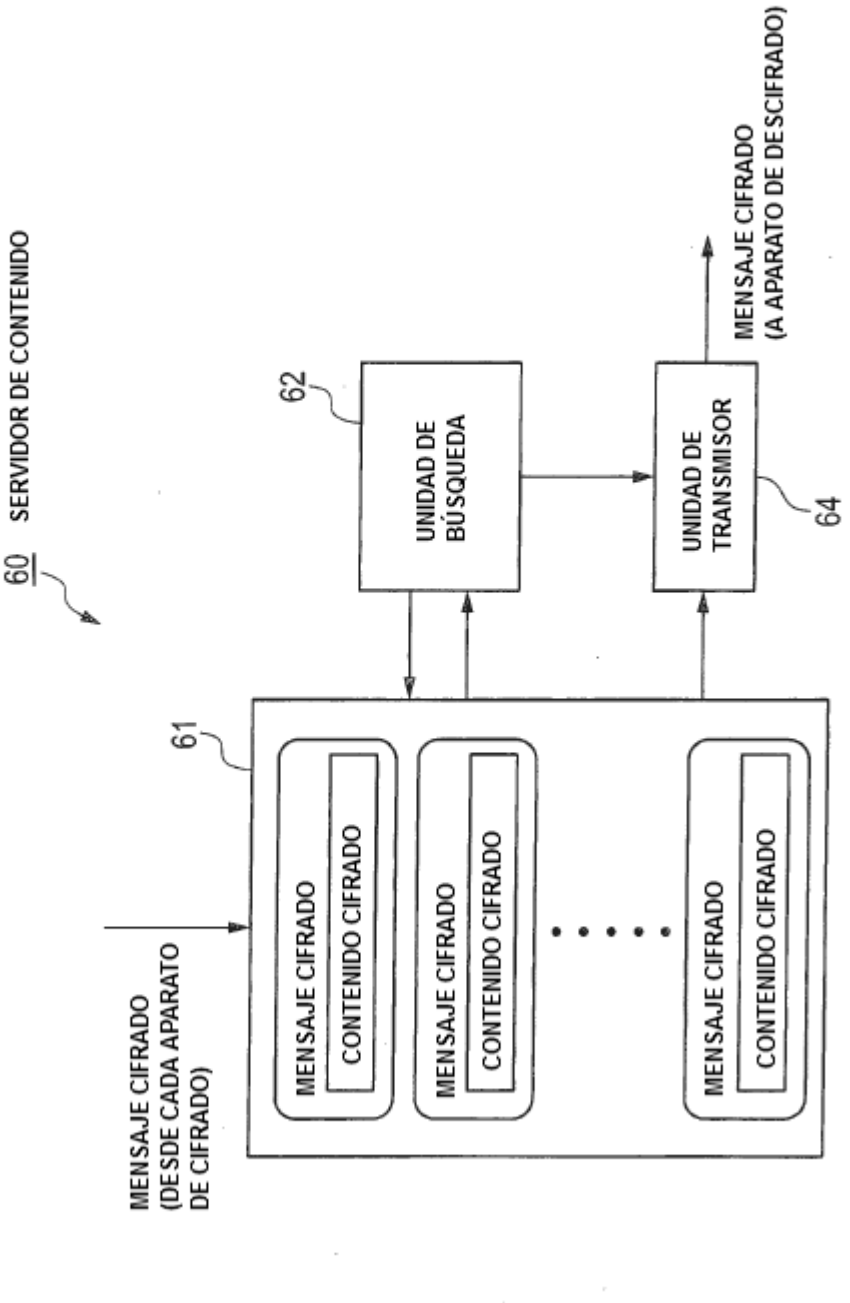

60
SERVIDOR DE CONTENIDO
61
62
UNIDAD DE BÚSQUEDA
UNIDAD DE TRANSMISOR
64
MENSAJE CIFRADO (DESDE CADA APARATO DE CIFRADO)
MENSAJE CIFRADO
CONTENIDO CIFRADO
MENSAJE CIFRADO
CONTENIDO CIFRADO
MENSAJE CIFRADO
CONTENIDO CIFRADO
MENSAJE CIFRADO (A APARATO DE DESCIFRADO)

FIG.68

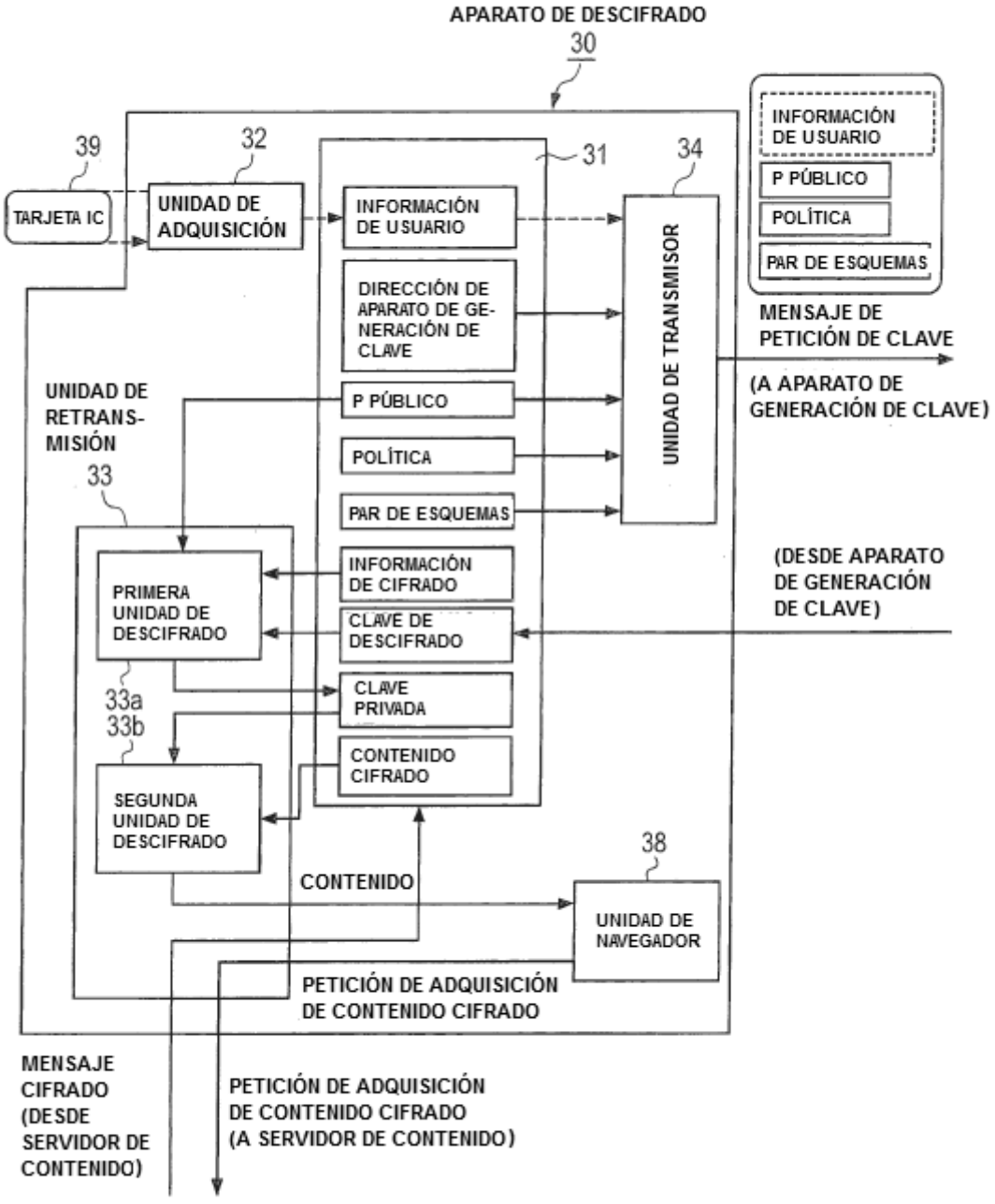

APARATO DE DESCIFRADO
30
39
32
31
34
TARJETA IC
UNIDAD DE ADQUISICIÓN
INFORMACIÓN DE USUARIO
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
UNIDAD DE TRANSMISOR
INFORMACIÓN DE USUARIO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
MENSAJE DE PETICIÓN DE CLAVE
(A APARATO DE GENERACIÓN DE CLAVE)
UNIDAD DE RETRANSMISIÓN
33
PRIMERA UNIDAD DE DESCIFRADO
INFORMACIÓN DE CIFRADO
CLAVE DE DESCIFRADO
(DESDE APARATO DE GENERACIÓN DE CLAVE)
33a
33b
CLAVE PRIVADA
CONTENIDO CIFRADO
SEGUNDA UNIDAD DE DESCIFRADO
38
CONTENIDO
UNIDAD DE NAVEGADOR
PETICIÓN DE ADQUISICIÓN DE CONTENIDO CIFRADO
MENSAJE CIFRADO (DESDE SERVIDOR DE CONTENIDO)
PETICIÓN DE ADQUISICIÓN DE CONTENIDO CIFRADO (A SERVIDOR DE CONTENIDO)

FIG.69

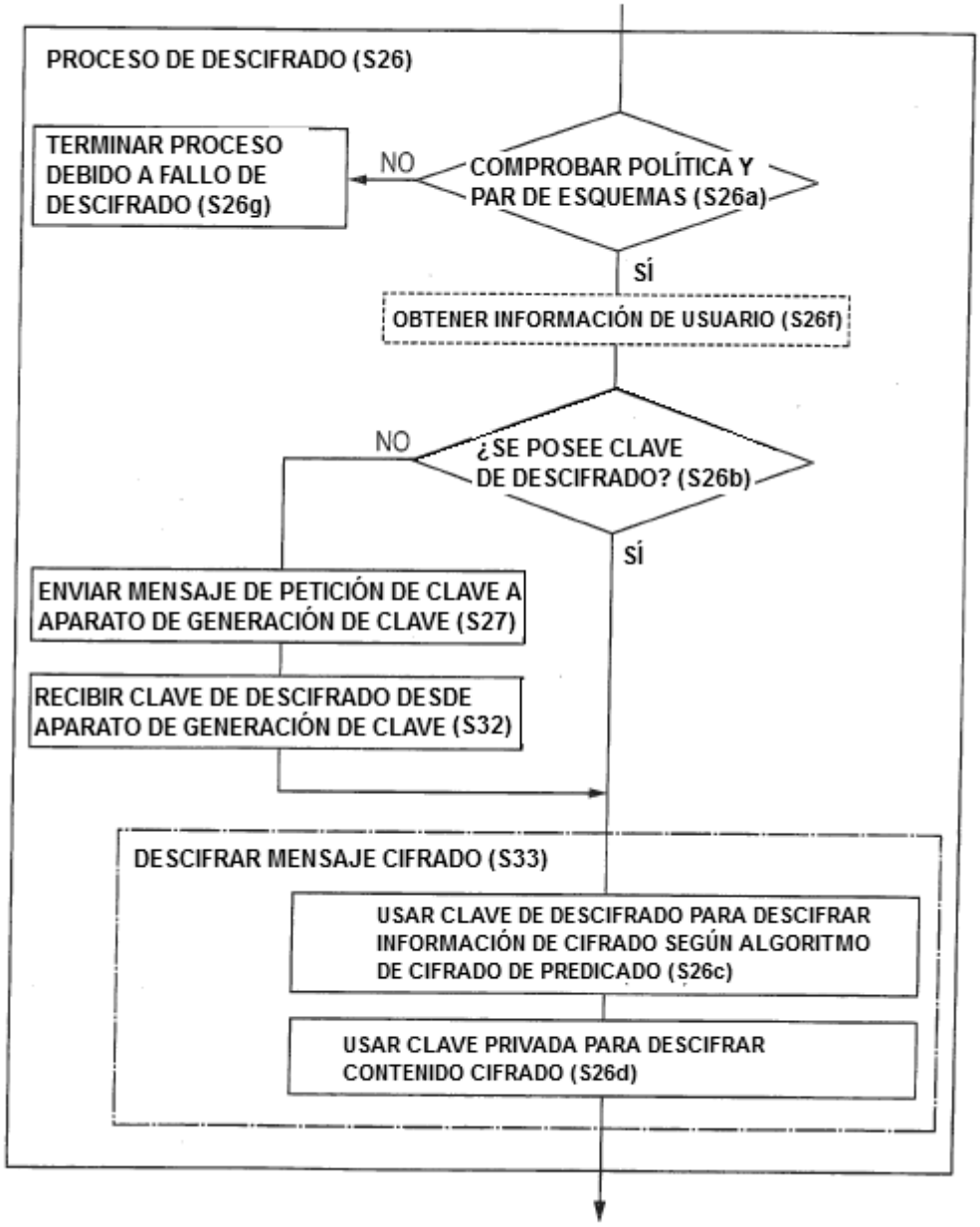

PROCESO DE DESCIFRADO (S26)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S26g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S26a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S26f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S26b)
SÍ
ENVIAR MENSAJE DE PETICIÓN DE CLAVE A APARATO DE GENERACIÓN DE CLAVE (S27)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACIÓN DE CLAVE (S32)
DESCIFRAR MENSAJE CIFRADO (S33)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGÚN ALGORITMO DE CIFRADO DE PREDICADO (S26c)
USAR CLAVE PRIVADA PARA DESCIFRAR CONTENIDO CIFRADO (S26d)

FIG.70

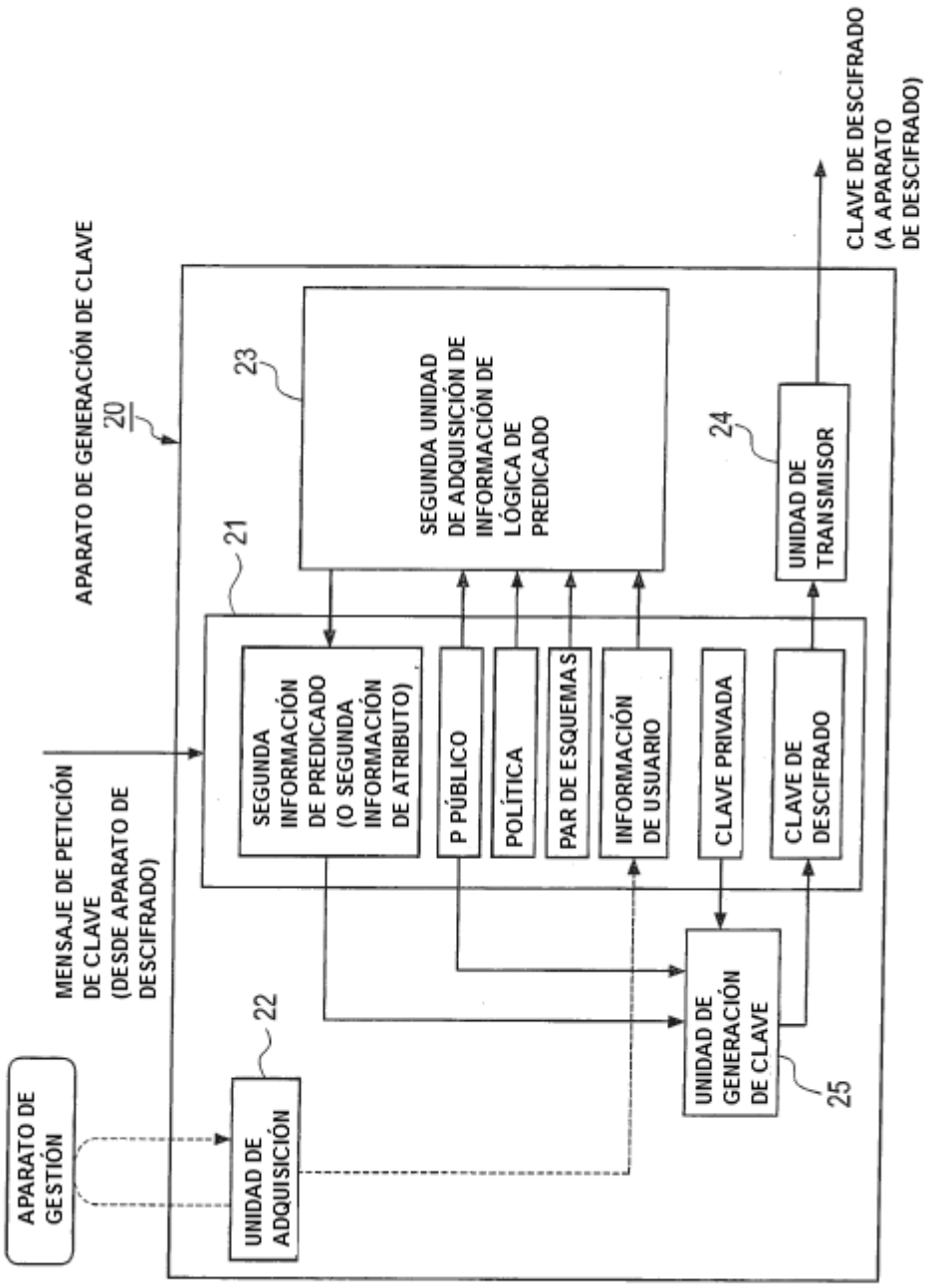

APARATO DE GESTIÓN
MENSAJE DE PETICIÓN DE CLAVE (DESDE APARATO DE DESCIFRADO)
APARATO DE GENERACIÓN DE CLAVE
20
UNIDAD DE ADQUISICIÓN
22
21
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
INFORMACIÓN DE USUARIO
CLAVE PRIVADA
CLAVE DE DESCIFRADO
23
SEGUNDA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
UNIDAD DE GENERACIÓN DE CLAVE
25
24
UNIDAD DE TRANSMISOR
CLAVE DE DESCIFRADO (A APARATO DE DESCIFRADO)

FIG.71

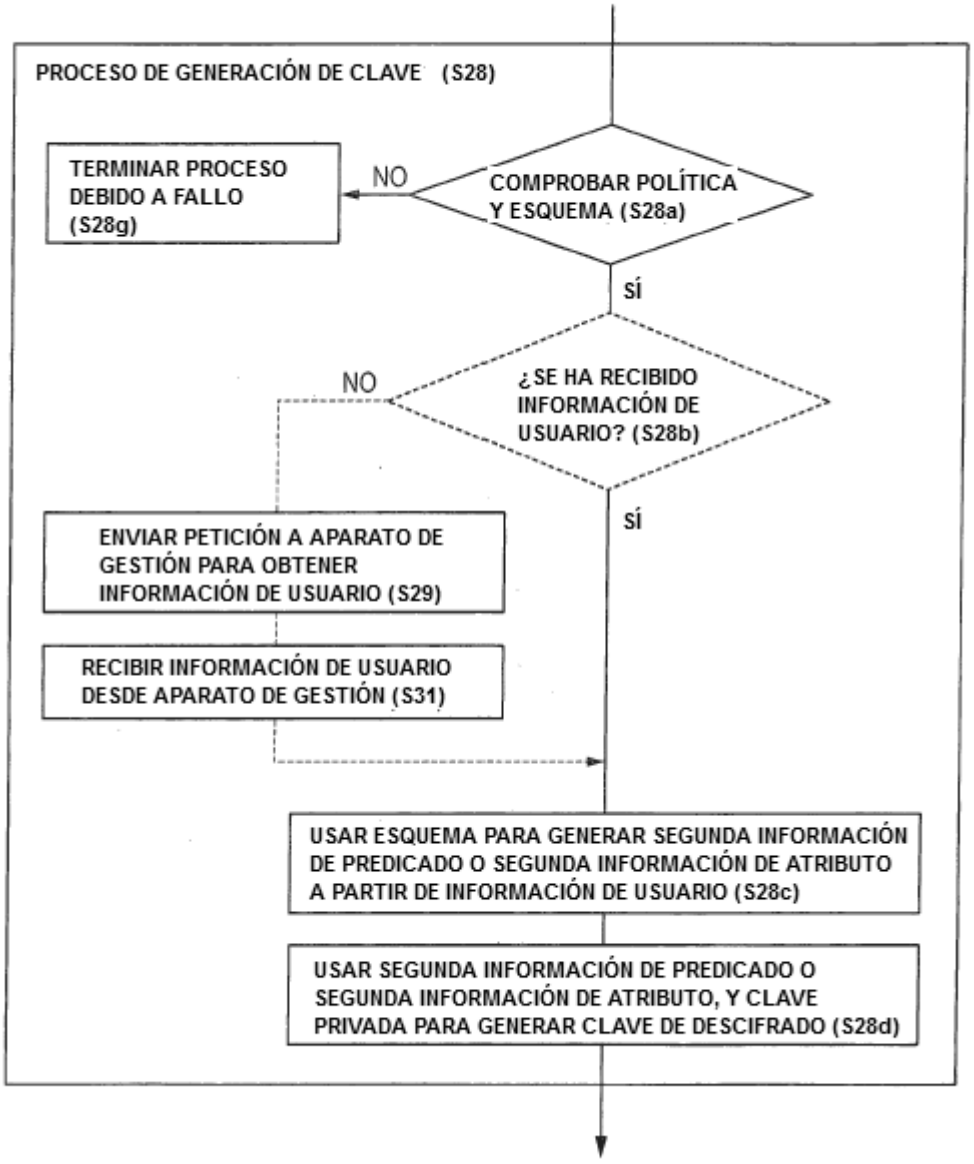

PROCESO DE GENERACIÓN DE CLAVE (S28)
COMPROBAR POLÍTICA Y ESQUEMA (S28a)
NO
TERMINAR PROCESO DEBIDO A FALLO (S28g)
SÍ
¿SE HA RECIBIDO INFORMACIÓN DE USUARIO? (S28b)
NO
SÍ
ENVIAR PETICIÓN A APARATO DE GESTIÓN PARA OBTENER INFORMACIÓN DE USUARIO (S29)
RECIBIR INFORMACIÓN DE USUARIO DESDE APARATO DE GESTIÓN (S31)
USAR ESQUEMA PARA GENERAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO A PARTIR DE INFORMACIÓN DE USUARIO (S28c)
USAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO, Y CLAVE PRIVADA PARA GENERAR CLAVE DE DESCIFRADO (S28d)

FIG.72

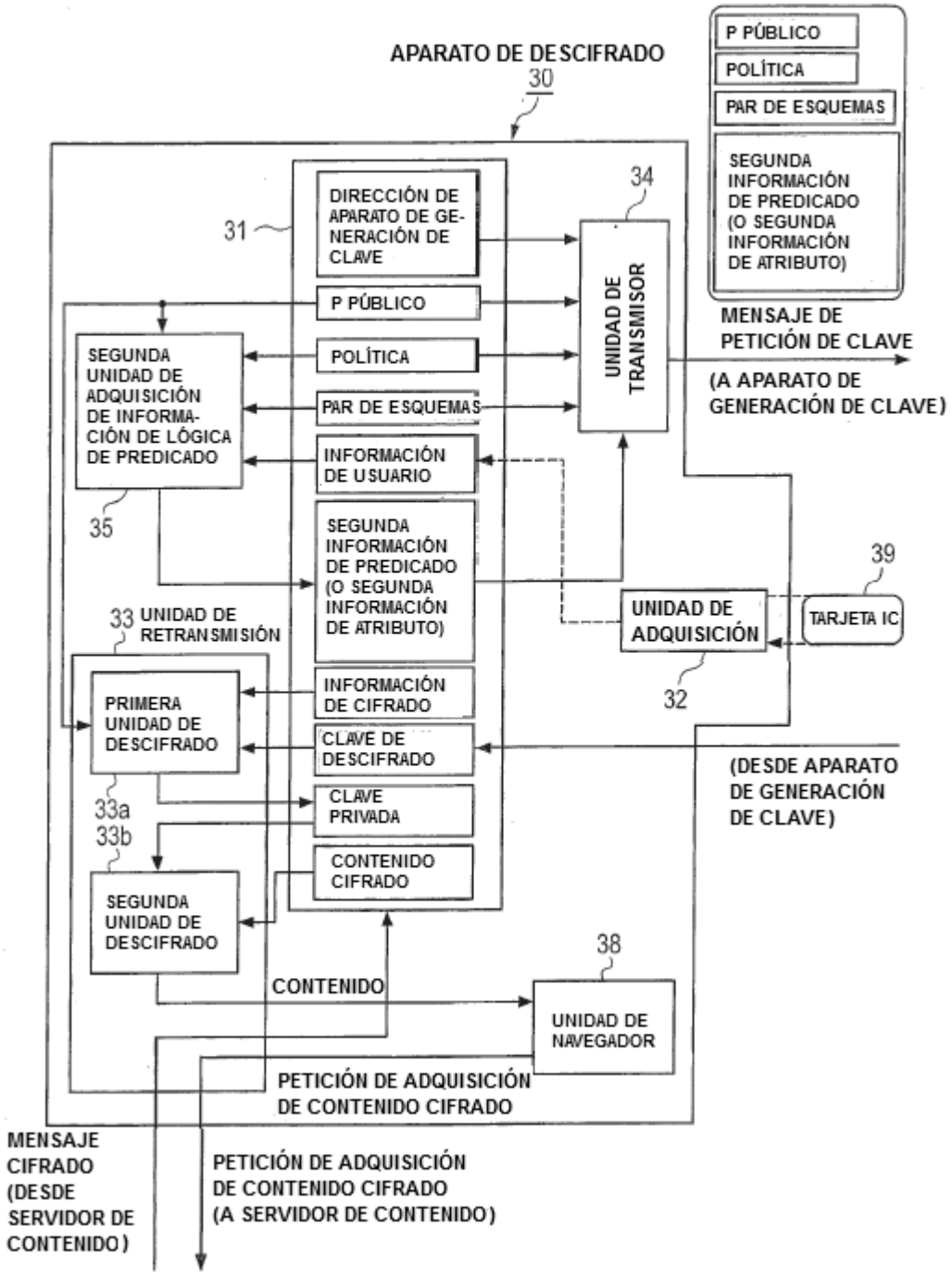

APARATO DE DESCIFRADO
30
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
31
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
34
UNIDAD DE TRANSMISOR
MENSAJE DE PETICIÓN DE CLAVE
(A APARATO DE GENERACIÓN DE CLAVE)
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
INFORMACIÓN DE USUARIO
SEGUNDA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
35
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
39
UNIDAD DE ADQUISICIÓN
TARJETA IC
32
33 UNIDAD DE RETRANSMISIÓN
PRIMERA UNIDAD DE DESCIFRADO
INFORMACIÓN DE CIFRADO
CLAVE DE DESCIFRADO
(DESDE APARATO DE GENERACIÓN DE CLAVE)
CLAVE PRIVADA
33a
33b
CONTENIDO CIFRADO
SEGUNDA UNIDAD DE DESCIFRADO
38
CONTENIDO
UNIDAD DE NAVEGADOR
PETICIÓN DE ADQUISICIÓN DE CONTENIDO CIFRADO
MENSAJE CIFRADO (DESDE SERVIDOR DE CONTENIDO)
PETICIÓN DE ADQUISICIÓN DE CONTENIDO CIFRADO (A SERVIDOR DE CONTENIDO)

FIG.73

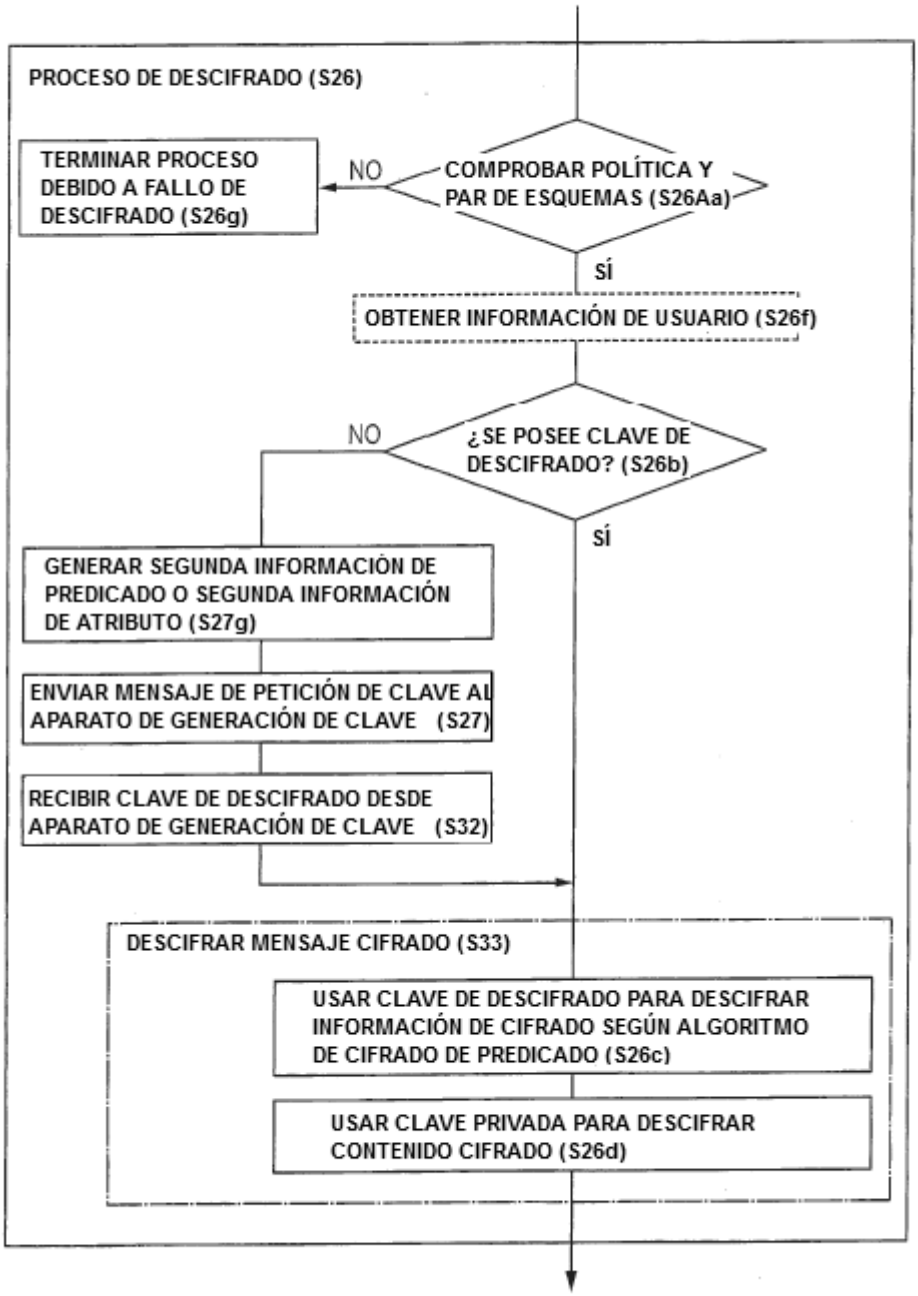

PROCESO DE DESCIFRADO (S26)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S26g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S26Aa)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S26f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S26b)
SÍ
GENERAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO (S27g)
ENVIAR MENSAJE DE PETICIÓN DE CLAVE AL APARATO DE GENERACIÓN DE CLAVE (S27)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACIÓN DE CLAVE (S32)
DESCIFRAR MENSAJE CIFRADO (S33)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR INFORMACIÓN DE CIFRADO SEGÚN ALGORITMO DE CIFRADO DE PREDICADO (S26c)
USAR CLAVE PRIVADA PARA DESCIFRAR CONTENIDO CIFRADO (S26d)

FIG.74

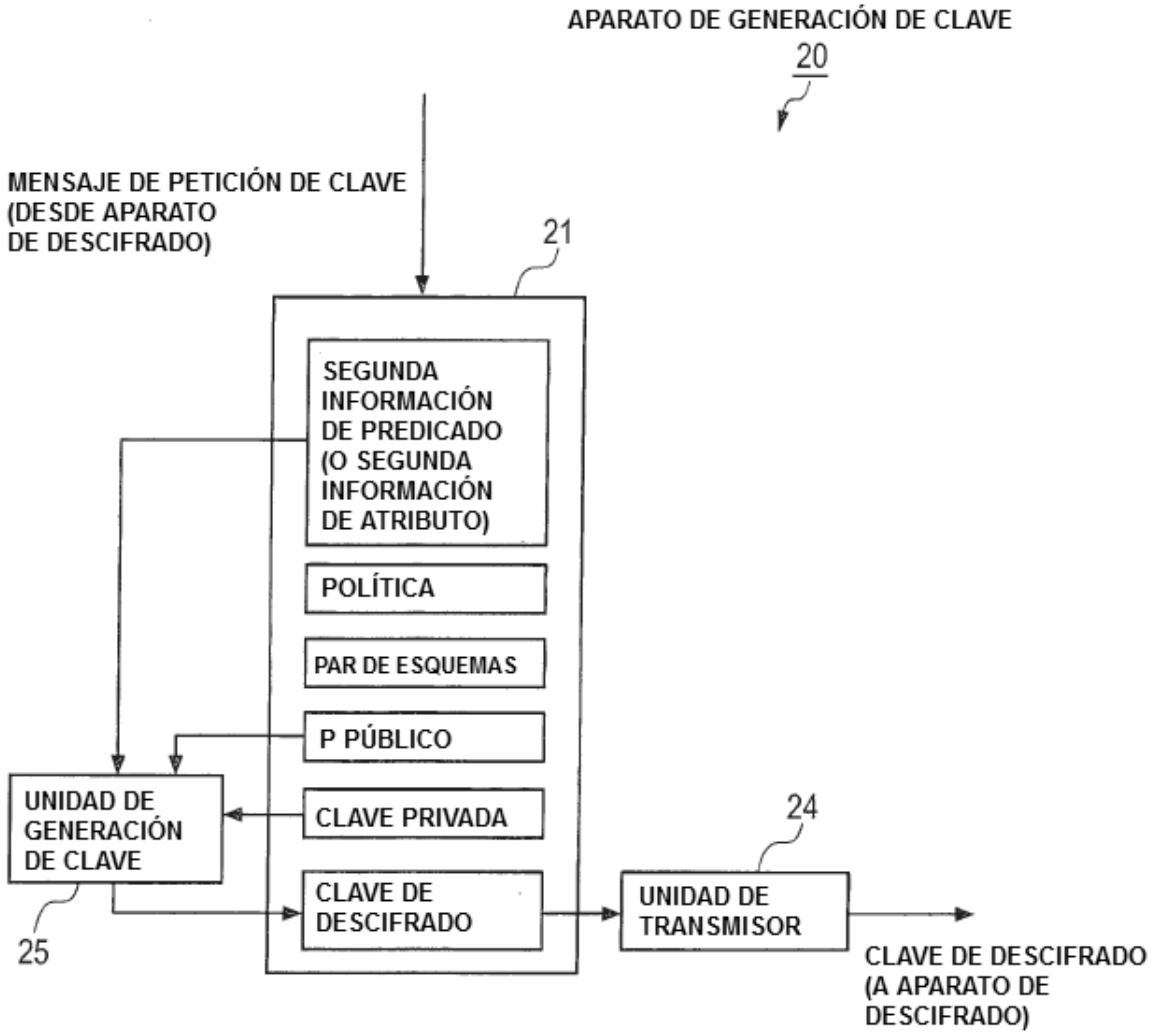

APARATO DE GENERACIÓN DE CLAVE
20
MENSAJE DE PETICIÓN DE CLAVE (DESDE APARATO DE DESCIFRADO)
21
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
POLÍTICA
PAR DE ESQUEMAS
P PÚBLICO
CLAVE PRIVADA
CLAVE DE DESCIFRADO
UNIDAD DE GENERACIÓN DE CLAVE
25
24
UNIDAD DE TRANSMISOR
CLAVE DE DESCIFRADO (A APARATO DE DESCIFRADO)

FIG.75

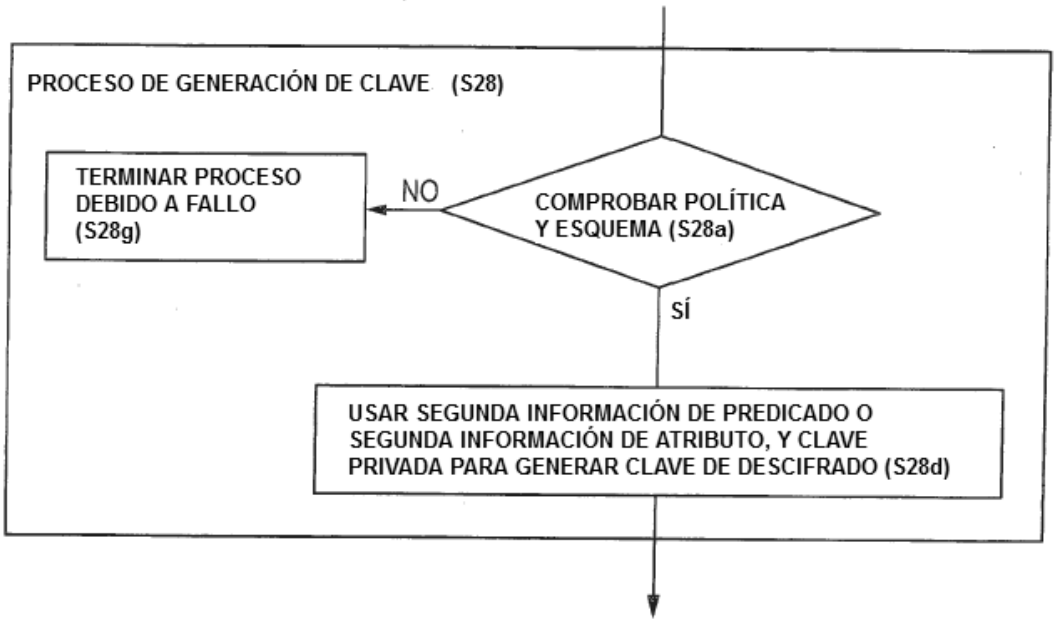

PROCESO DE GENERACIÓN DE CLAVE (S28)
TERMINAR PROCESO DEBIDO A FALLO (S28g)
NO
COMPROBAR POLÍTICA Y ESQUEMA (S28a)
SÍ
USAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO, Y CLAVE PRIVADA PARA GENERAR CLAVE DE DESCIFRADO (S28d)

FIG.76

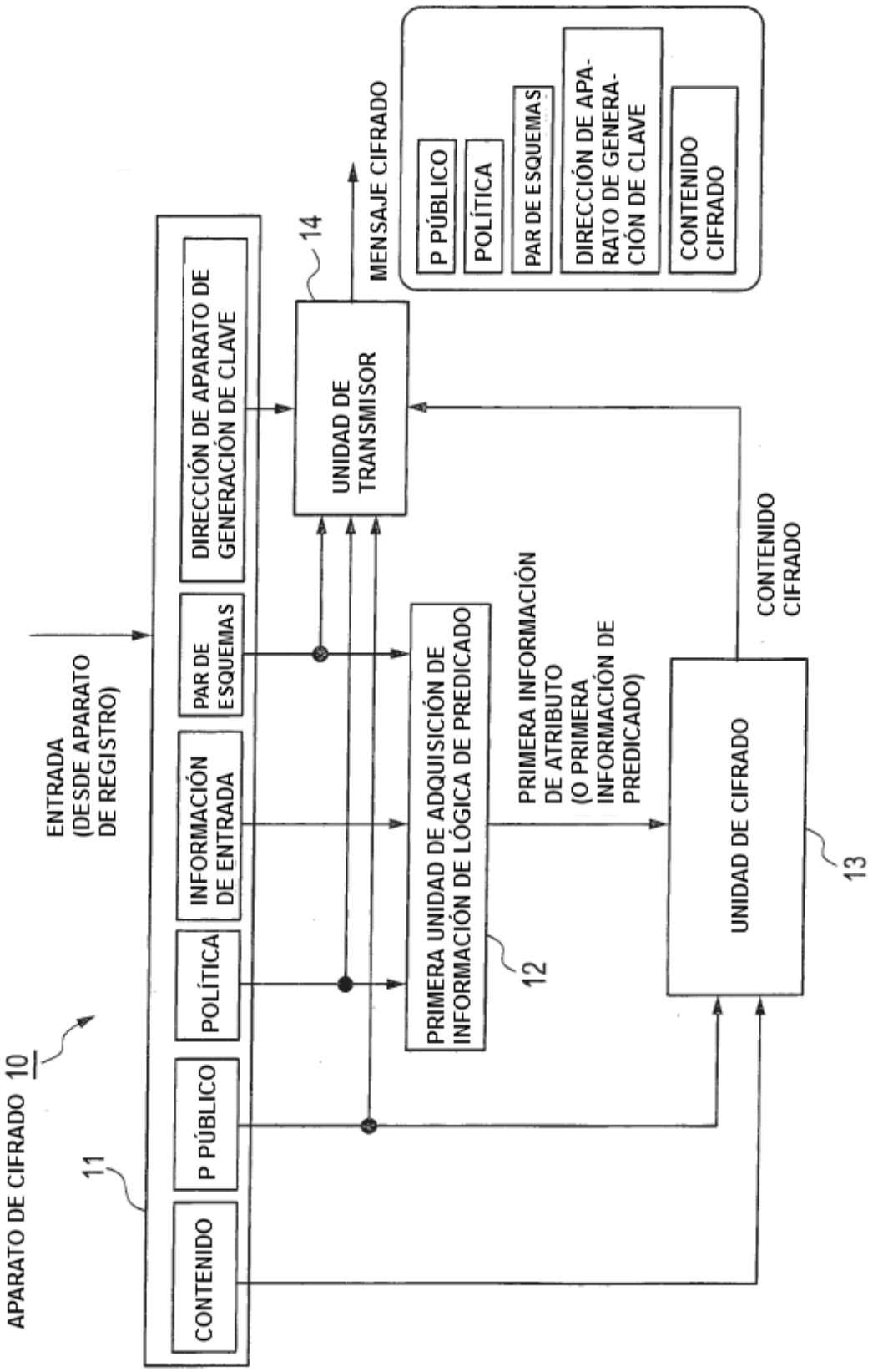

APARATO DE CIFRADO 10
11
CONTENIDO
P PÚBLICO
POLÍTICA
INFORMACIÓN DE ENTRADA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
ENTRADA (DESDE APARATO DE REGISTRO)
UNIDAD DE TRANSMISOR
14
MENSAJE CIFRADO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
CONTENIDO CIFRADO
PRIMERA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
12
PRIMERA INFORMACIÓN DE ATRIBUTO (O PRIMERA INFORMACIÓN DE PREDICADO)
UNIDAD DE CIFRADO
13
CONTENIDO CIFRADO

FIG.77

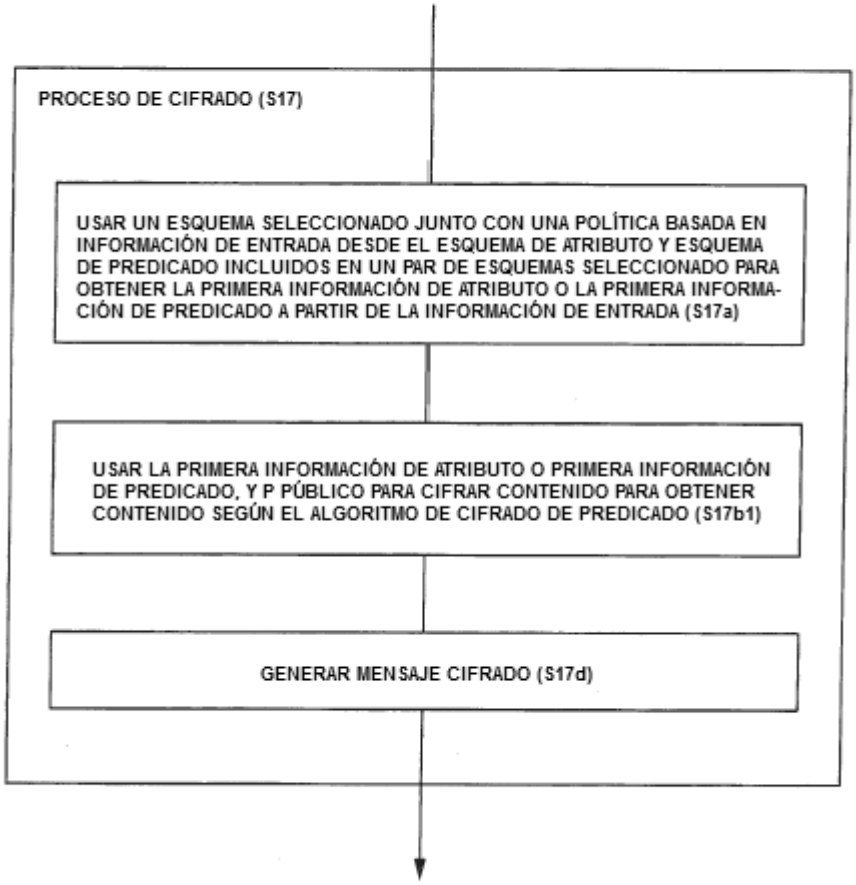

PROCESO DE CIFRADO (S17)
USAR UN ESQUEMA SELECCIONADO JUNTO CON UNA POLÍTICA BASADA EN INFORMACIÓN DE ENTRADA DESDE EL ESQUEMA DE ATRIBUTO Y ESQUEMA DE PREDICADO INCLUIDOS EN UN PAR DE ESQUEMAS SELECCIONADO PARA OBTENER LA PRIMERA INFORMACIÓN DE ATRIBUTO O LA PRIMERA INFORMACIÓN DE PREDICADO A PARTIR DE LA INFORMACIÓN DE ENTRADA (S17a)
USAR LA PRIMERA INFORMACIÓN DE ATRIBUTO O PRIMERA INFORMACIÓN DE PREDICADO, Y P PÚBLICO PARA CIFRAR CONTENIDO PARA OBTENER CONTENIDO SEGÚN EL ALGORITMO DE CIFRADO DE PREDICADO (S17b1)
GENERAR MENSAJE CIFRADO (S17d)

FIG.78

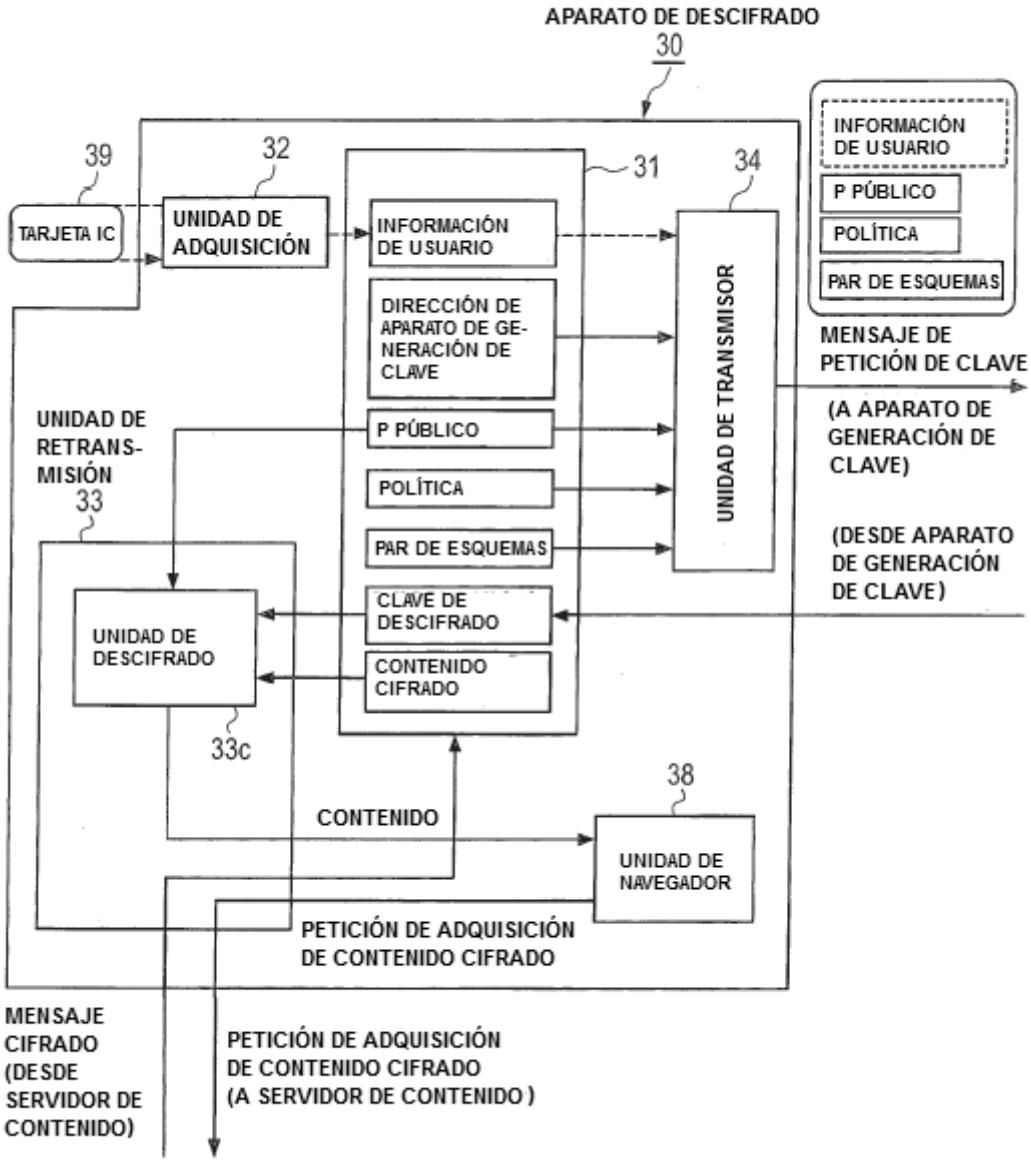

APARATO DE DESCIFRADO
30
INFORMACIÓN DE USUARIO
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
39
32
31
34
TARJETA IC
UNIDAD DE ADQUISICIÓN
INFORMACIÓN DE USUARIO
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
UNIDAD DE TRANSMISOR
MENSAJE DE PETICIÓN DE CLAVE
(A APARATO DE GENERACIÓN DE CLAVE)
UNIDAD DE RETRANSMISIÓN
33
(DESDE APARATO DE GENERACIÓN DE CLAVE)
UNIDAD DE DESCIFRADO
CLAVE DE DESCIFRADO
CONTENIDO CIFRADO
33c
38
CONTENIDO
UNIDAD DE NAVEGADOR
PETICIÓN DE ADQUISICIÓN DE CONTENIDO CIFRADO
MENSAJE CIFRADO (DESDE SERVIDOR DE CONTENIDO)
PETICIÓN DE ADQUISICIÓN DE CONTENIDO CIFRADO (A SERVIDOR DE CONTENIDO)

FIG.79

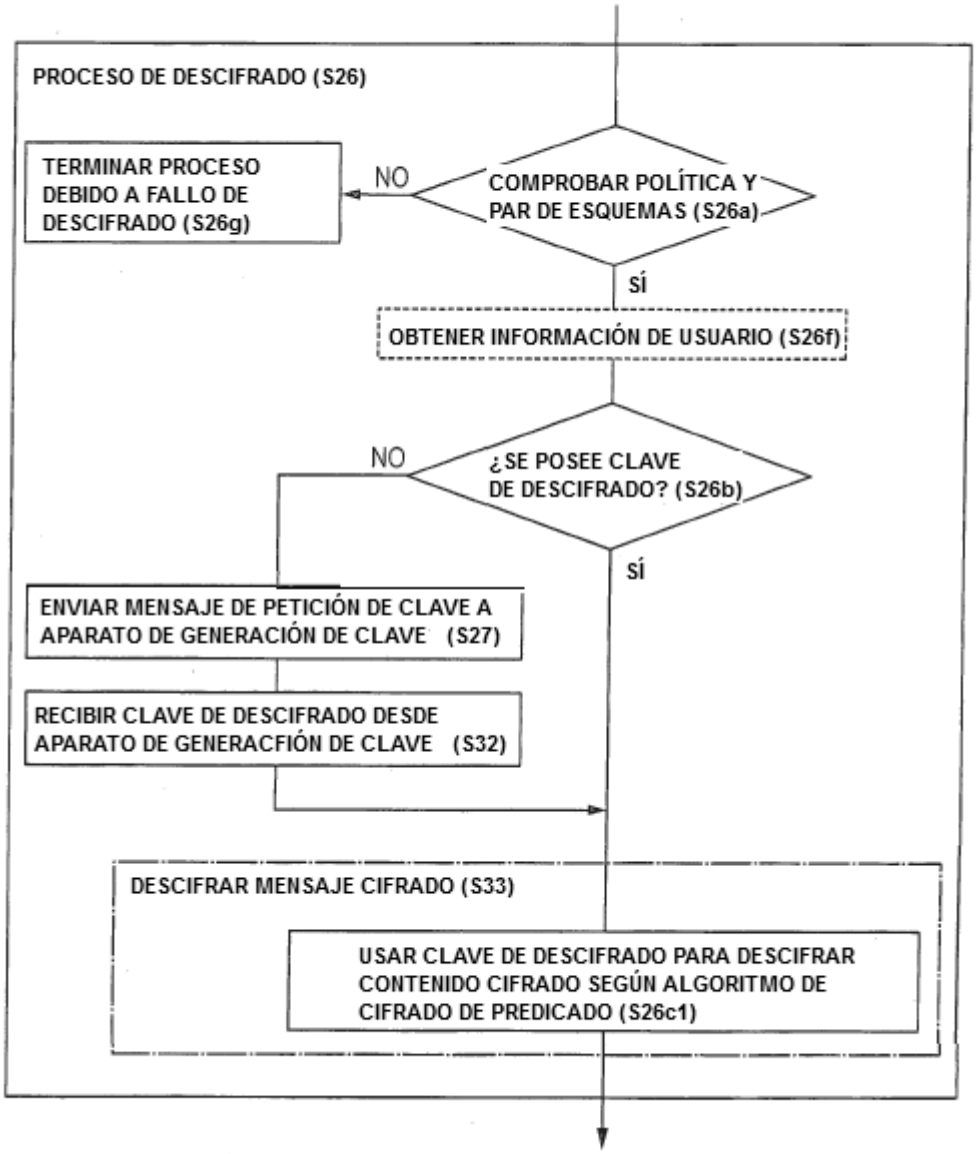

PROCESO DE DESCIFRADO (S26)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S26g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S26a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S26f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S26b)
SÍ
ENVIAR MENSAJE DE PETICIÓN DE CLAVE A APARATO DE GENERACIÓN DE CLAVE (S27)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACFIÓN DE CLAVE (S32)
DESCIFRAR MENSAJE CIFRADO (S33)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR CONTENIDO CIFRADO SEGÚN ALGORITMO DE CIFRADO DE PREDICADO (S26c1)

FIG.80

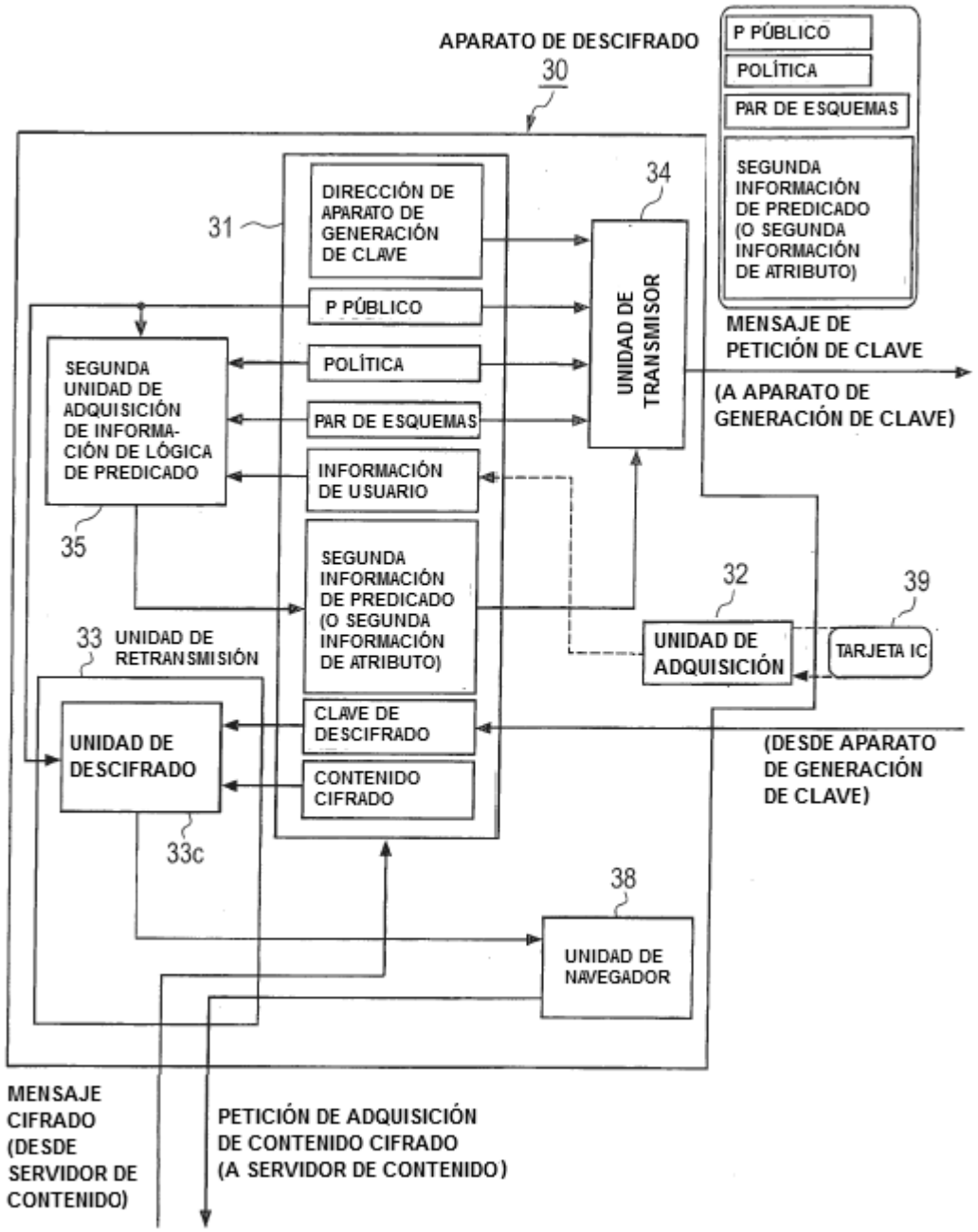

APARATO DE DESCIFRADO
30
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
31
DIRECCIÓN DE APARATO DE GENERACIÓN DE CLAVE
34
UNIDAD DE TRANSMISOR
MENSAJE DE PETICIÓN DE CLAVE
(A APARATO DE GENERACIÓN DE CLAVE)
P PÚBLICO
POLÍTICA
PAR DE ESQUEMAS
INFORMACIÓN DE USUARIO
SEGUNDA UNIDAD DE ADQUISICIÓN DE INFORMACIÓN DE LÓGICA DE PREDICADO
35
SEGUNDA INFORMACIÓN DE PREDICADO (O SEGUNDA INFORMACIÓN DE ATRIBUTO)
32
UNIDAD DE ADQUISICIÓN
39
TARJETA IC
33
UNIDAD DE RETRANSMISIÓN
CLAVE DE DESCIFRADO
(DESDE APARATO DE GENERACIÓN DE CLAVE)
UNIDAD DE DESCIFRADO
CONTENIDO CIFRADO
33c
38
UNIDAD DE NAVEGADOR
MENSAJE CIFRADO (DESDE SERVIDOR DE CONTENIDO)
PETICIÓN DE ADQUISICIÓN DE CONTENIDO CIFRADO (A SERVIDOR DE CONTENIDO)

FIG.81

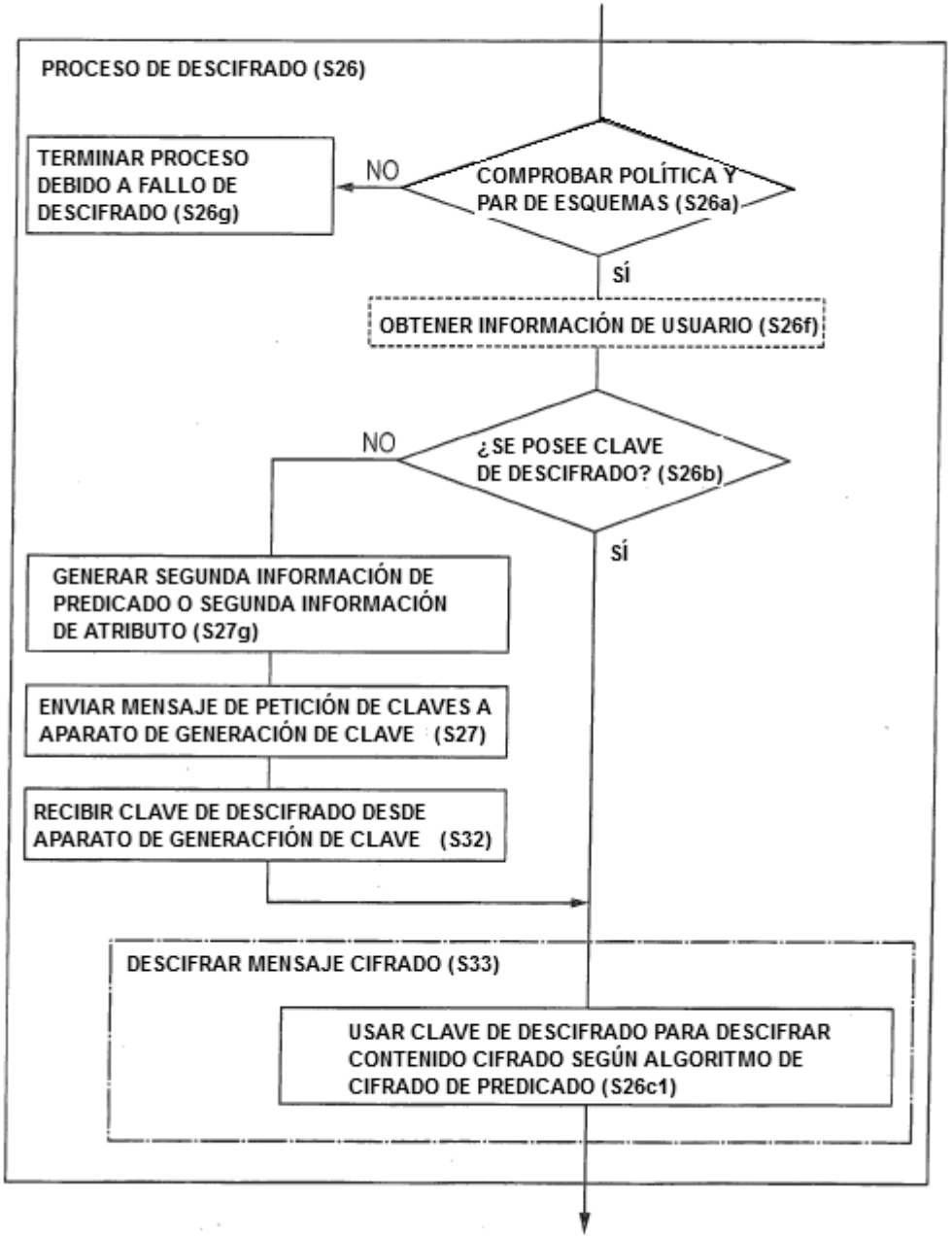
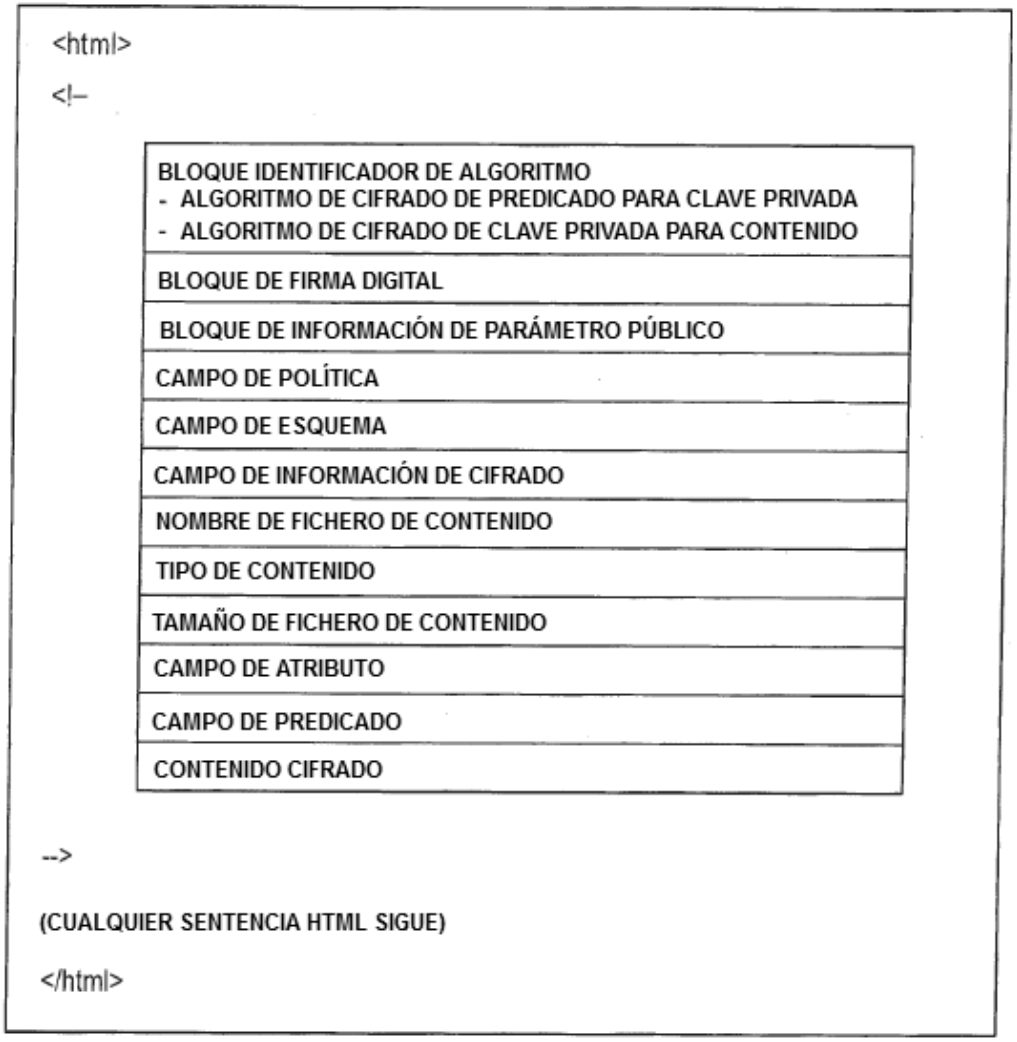

PROCESO DE DESCIFRADO (S26)
TERMINAR PROCESO DEBIDO A FALLO DE DESCIFRADO (S26g)
NO
COMPROBAR POLÍTICA Y PAR DE ESQUEMAS (S26a)
SÍ
OBTENER INFORMACIÓN DE USUARIO (S26f)
NO
¿SE POSEE CLAVE DE DESCIFRADO? (S26b)
SÍ
GENERAR SEGUNDA INFORMACIÓN DE PREDICADO O SEGUNDA INFORMACIÓN DE ATRIBUTO (S27g)
ENVIAR MENSAJE DE PETICIÓN DE CLAVES A APARATO DE GENERACIÓN DE CLAVE (S27)
RECIBIR CLAVE DE DESCIFRADO DESDE APARATO DE GENERACFIÓN DE CLAVE (S32)
DESCIFRAR MENSAJE CIFRADO (S33)
USAR CLAVE DE DESCIFRADO PARA DESCIFRAR CONTENIDO CIFRADO SEGÚN ALGORITMO DE CIFRADO DE PREDICADO (S26c1)

FIG.82


<html>
<!–
BLOQUE IDENTIFICADOR DE ALGORITMO
- ALGORITMO DE CIFRADO DE PREDICADO PARA CLAVE PRIVADA
- ALGORITMO DE CIFRADO DE CLAVE PRIVADA PARA CONTENIDO
BLOQUE DE FIRMA DIGITAL
BLOQUE DE INFORMACIÓN DE PARÁMETRO PÚBLICO
CAMPO DE POLÍTICA
CAMPO DE ESQUEMA
CAMPO DE INFORMACIÓN DE CIFRADO
NOMBRE DE FICHERO DE CONTENIDO
TIPO DE CONTENIDO
TAMAÑO DE FICHERO DE CONTENIDO
CAMPO DE ATRIBUTO
CAMPO DE PREDICADO
CONTENIDO CIFRADO
-->
(CUALQUIER SENTENCIA HTML SIGUE)
</html>