(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 307 734**

(51) Int. Cl.:
H04L 9/08 (2006.01)
G09C 1/00 (2006.01)
G06Q 10/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02711464 .4**
(96) Fecha de presentación : **12.02.2002**
(97) Número de publicación de la solicitud: **1361693**
(97) Fecha de publicación de la solicitud: **12.11.2003**

(54) Título: **Sistema de descifre de órdenes y método de descifre de órdenes y programa.**

(30) Prioridad: **13.02.2001 JP 2001-35030**

(45) Fecha de publicación de la mención BOPI:
01.12.2008

(45) Fecha de la publicación del folleto de la patente:
01.12.2008

(73) Titular/es: **NEC CORPORATION**
7-1, Shiba 5-chome
Minato-ku, Tokyo 108-8001, JP

(72) Inventor/es: **Sako, Kazue y**
Mori, Kengo

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Sistema de descifre de órdenes y método de descifre de órdenes y programa.

Campo técnico

La presente invención se refiera a una tecnología de desencriptación anónima y, más en particular, a una tecnología de desencriptación anónima para suministrar resultados de desencriptación manteniendo confidencial la correspondencia con los datos encriptados.

Técnica anterior

El documento US-A-6 049 613 describe un aparato para encriptar, desencriptar y proporcionar reserva de valores de datos, aparato que comprende un duplicador y un primer y un segundo módulo operativos. Cada uno de los módulos operativos primero y segundo comprende un primer y un segundo procesador. Cada procesador comprende un dispositivo operativo parcial. Preferiblemente, el duplicador duplica un vector de entradas encriptadas y proporciona los vectores duplicados sustancialmente similares primero y segundo a los módulos operativos primero y segundo, respectivamente. El dispositivo operativo parcial del primer procesador del primer módulo operativo actúa parcialmente sobre el primer vector duplicado, luego suministra el resultado al dispositivo operativo parcial del segundo procesador del primer módulo operativo que actúa parcialmente sobre él para proporcionar uno totalmente tratado en el primer vector duplicado. Análogamente, el segundo módulo operativo proporciona uno totalmente tratado en el segundo vector duplicado. Un medio para comparar el totalmente tratado en el primer vector duplicado con el totalmente tratado en el segundo vector duplicado.

El documento EP 1 054 527 A2 describe un canal anónimo verificable. En el mencionado canal, dos cifratextos El Gamal, que son entrada a dos puertos de conexión de una unidad de dos entradas dos salidas que forman una red de permutación, están dispuestos al azar con un número aleatorio y permutados al azar, y una prueba de conocimiento cero, que comprueba la correspondencia entre las entradas y salidas de los puertos de conexión, es salida a un verificador sin revelar el número aleatorio ni la permutación al azar. Una unidad de desencriptación desencripta los cifratextos de un puerto de conexión de una unidad en la última columna mediante el uso de una clave secreta, y comprueba en el conocimiento cero la validez de la desencriptación sin revelar la clave secreta. Una unidad de verificación verifica la prueba de cada puerto de conexión de una unidad y la prueba de la unidad de desencriptación.

Yi Mu y otros (*Anonymous secure ε-voting over a network*, Actas de la Computer Security Applications Conference, 1998, 14ª anual, Phoenix, AZ, USA, 7 a 11 de diciembre de 1998, Los Alamitos, CA, USA, IEEE Comp. Soc., US, 7 de diciembre de 1998) proponen dos nuevos esquemas de votación electrónicos de seguridad anónimos en una red que protege la reserva de los votantes para impedir una doble votación. Estos esquemas no requieren un canal especial de votación y las comunicaciones se pueden establecer enteramente en redes existentes tales como Internet. Los esquemas propuestos están basados en el algoritmo de signatura digital El Gamal y se pueden aplicar a elecciones en una variedad de situaciones que van desde elecciones en una organización pequeña a elecciones en un país.

El sistema descrito en la publicación de patente japonesa abierta a conocimiento público nº. H08-263575 (JP-A-263575) es un ejemplo conocido de un sistema de desencriptación anónimo de este tipo de la técnica anterior. El sistema de desencriptación anónimo descrito en este documento está basado en el procedimiento Mix-Net, representado en la Fig. 10, y está compuesto por: una pluralidad de centros mezcladores de desencriptación datos 100-1 a 100-n y un sistema de pantalla electrónica 200 anunciadora que está situado en una red tal como Internet y al que se puede acceder desde el exterior.

Cada uno de los centros mezcladores de desencriptación 100-1 a 100-n está provisto de un elemento 101 de desencriptación parcial, elemento mezclador 102 y el elemento de certificación 103. Además, cada uno de los centros mezcladores de desencriptación 100-1 a 100-n tiene una clave pública para encriptación que se genera de acuerdo con parámetros de seguridad determinados separadamente y una clave de desencriptación para la desencriptación. El sistema anónimo de desencriptación que se presenta en la Fig. 10 emplea una clave que se combina desde la clave pública de cada uno de los centros mezcladores de desencriptación 100-1 a 100-n como una clave pública de encriptación para encriptar datos.

Cuando una pluralidad de emisores (no representados) escribe datos encriptados que se han encriptado usando la clave pública de encriptación al sistema de pantalla electrónica 200 anunciadora, el centro mezclador de desencriptación 100-1, que es el primero en prioridad de procesamiento, admite los datos encriptados descritos antes que han sido escritos por la pluralidad de emisores como lista 201 de datos encriptados y realiza el procesamiento siguiente.

El centro mezclador de desencriptación 100-1 usa primeramente el elemento de desencriptación 101 para someter la lista 201 de datos encriptados a un proceso de desencriptación parcial. En este momento, el elemento 101 de desencriptación parcial usa la clave de desencriptación que está soportado por el centro mezclador de desencriptación 100-1. El centro mezclador de desencriptación 100-1 usa seguidamente el elemento mezclador 102 para someter la lista de datos encriptados que se han desencriptado parcialmente a un proceso de conexión de órdenes.

El centro 100-1 mezclador de desencriptación usa luego el elemento 103 para generar datos de certificación para certificar que el proceso de desencriptación parcial y el proceso de conexión de órdenes se han realizado correctamente. Finalmente, el centro mezclador de desencriptación 100-1 escribe los datos 202-1 que incluye la lista de datos encriptados (esto la lista de datos) que han sido sometidos al proceso de desencriptación parcial y al proceso de conexión de órdenes y los datos de certificación al sistema 200 de pantalla electrónica anunciadora.

Cuando los datos 202-1 se han escrito al sistema de pantalla electrónica anunciadora 200, el centro mezclador de desencriptación 100-2, que es el segundo en prioridad de procesamiento, lleva a cabo los mismos procesos en la lista de datos de los datos 202-1 que los procesos realizados por el centro mezclador de desencriptación 101 y escribe los datos 200-2 que incluyen la lista de datos y los datos de certificación al sistema de pantalla electrónica anunciadora 200.

La misma operación se realiza sucesivamente hasta que se escriben al sistema electrónico de pantalla anunciadores 200 el último centro mezclador de desencriptación 100-n y los datos 203 que incluyen la lista resultado de la desencriptación y los datos de certificación.

El sistema de desencriptación anónimo de la técnica anterior usa un sistema de pantalla electrónica anunciadora y, por tanto, acarrea varios problemas como se indica seguidamente. Para que cada centro mezclador de desencriptación realice el proceso de desencriptación parcial y el proceso de conexión de órdenes, así como para que cada emisor pueda verificar los datos de certificación, cada centro mezclador de desencriptación y cada emisor debe ser capaz de acceder libremente y al sistema de pantalla electrónica anunciadora y leerlo. Además, para prevenir acciones ilegitimadas, la escritura de los datos al sistema electrónico de pantalla anunciadora debe estar restringida a datos de emisores autorizados y el centro mezclador de desencriptación. Por tanto, un sistema de desencriptación anónimo de la técnica anterior debe permitir que cada centro mezclador de desencriptación y cada emisor lean libremente una pantalla electrónica anunciadora y, además, debe restringir la escritura de datos a una pantalla electrónica anunciadora sólo a datos autorizados de emisores autorizados y centros mezcladores de desencriptación, y estos requerimientos complican la gestión.

Además, desde el punto de vista de protección del anonimato, en operaciones reales, cada uno de los centros mezcladores de desencriptación que conforman un sistema anónimo de desencriptación es operado por organizaciones separadas. Sin embargo, el que diferentes organizaciones operen el sistema presenta el problema de complicar la tarea de hacer los ajustes iniciales que determinan los diversos parámetros importantes (tales como claves usadas por los usuarios para encriptar mensajes) que son necesarios para el sistema.

Consecuentemente, hay peligro de que no estén claros los detalles de determinar los parámetros importantes y, como resultado de ello, hay la posibilidad de problemas en el funcionamiento normal del sistema.

Por tanto, es objeto de la presente invención eliminar la necesidad de procedimientos de gestión complicados y facilitar y hacer más fiable la tarea de los ajustes iniciales.

Descripción de la invención

El sistema anónimo de desencriptación de la presente invención está constituido por una pluralidad de centros mezclador de desencriptación y un centro de gestión de mezcla. Si sólo hay un centro mezclador de desencriptación, el centro de gestión de mezcla transfiere una lista de datos encriptada que se recibe como entrada desde el exterior al centro mezclador de desencriptación y luego suministra la lista de datos (una lista de datos encriptada que ha experimentado un proceso de desencriptación parcial y un proceso de conexión de órdenes en el centro mezclador de desencriptación antes descrito) que vuelve del centro mezclador de desencriptación como lista resultado de la desencriptación.

Si hay una pluralidad de centros mezcladores de desencriptación, el centro de gestión de mezcla transfiere una lista de datos encriptada que se recibe como entrada del exterior al centro mezclador de desencriptación que es el primero en prioridad de procesamiento y, cuando la lista de datos retorna del centro mezclador de desencriptación antes descrito, transfiere esta lista como lista de datos encriptados al centro mezclador de desencriptación que es el segundo en prioridad de procesamiento. Posteriormente, el centro de gestión de mezcla repite el proceso de transferir la lista de datos que retorna de un centro mezclador de desencriptación particular al centro mezclador de desencriptación que es el siguiente en prioridad de procesamiento como lista de datos encriptados y, cuando la lista de datos retorna desde el centro mezclador de desencriptación que es el último en prioridad de procesamiento, suministra esta lista como lista de resultados de desencriptación. El sistema de desencriptación anónimo de la presente invención es así capaz de desencriptar una lista de datos encriptados simplemente intercambiando datos entre un centro de gestión de mezcla y centros de mezcladores de desencriptación, con lo que se elimina sí la necesidad de un proceso de gestión complicado tal como el del sistema anónimo de desencriptación de la técnica anterior que usa el sistema de pantalla electrónica anunciadora.

Además, a causa de que el centro de gestión de mezcla y cada uno de los centros mezcladores de desencriptación juntos generan información pública que incluye claves públicas de encriptación cuando un parámetro de seguridad entra como entrada, el sistema anónimo de desencriptación de la presente invención puede facilitar la tarea de los ajustes iniciales y hacerla más fiable.

Breve descripción de los dibujos

La Fig. 1 es un diagrama de bloque que representa un ejemplo de la construcción de la primera realización de la presente invención.

La Fig. 2 es un diagrama de bloque que representa un ejemplo de la construcción del centro 10 de gestión de mezcla.

La Fig. 3 es un diagrama de bloque que representa un ejemplo de la construcción del centro 20-j mezclador de desencriptación.

La Fig. 4 es un diagrama de flujo que presenta un ejemplo del procesamiento cuando se hacen los ajustes iniciales.

La Fig. 5 es un diagrama de flujo que presenta un ejemplo del procesamiento del elemento 12 de control de la desencriptación.

La Fig. 6 es un diagrama de flujo que presenta un ejemplo del procesamiento del elemento 12 de control de la desencriptación de los centros 20-1 a 20-m mezcladores de la desencriptación.

La Fig. 7 es un diagrama de bloque que presenta un ejemplo de la construcción de la segunda realización de la presente invención.

La Fig. 8 es un diagrama de bloque que presenta un ejemplo de la construcción de la tercera realización de la presente invención.

La Fig. 9 es un diagrama de bloque que presenta un ejemplo de la construcción de la cuarta realización de la presente invención y

La Fig. 10 es un diagrama de bloque para explicar la técnica anterior.

Modo óptimo para realizar la presente invención

La siguiente explicación considera cada una de las realizaciones de la presente invención con referencia a las figuras que se acompañan.

Se considera primeramente la Fig. 1, en la que se presenta un sistema anónimo de desencriptación como primera realización de la presente invención. Este sistema anónimo de desencriptación está constituido por un centro 10 de gestión de mezcla y una pluralidad (m) de centros mezcladores de desencriptación 20-1 a 20-m.

El centro 10 de gestión de mezcla está constituido por un ordenador y tiene las funciones de, por ejemplo, actuar concertadamente con cada uno de los centros mezcladores 20-1 a 20-m para realizar un proceso de ajuste inicial y generar información pública que incluye, por ejemplo, claves públicas de encriptación cuando se reciben parámetros de seguridad como entradas desde el exterior; y, cuando se recibe una lista de datos encriptados como entrada desde el exterior que incluye una pluralidad de asuntos de datos de encriptación que se han encriptado mediante claves de encriptación públicas, usar los centros 21-1 a 20-m mezcladores de desencriptación en un orden prescrito (por ejemplo, en un orden que se ha instruido desde el exterior) para desencriptar la lista de datos encriptados antes descrita.

Como se representa en la Fig. 2, el centro 10 de gestión de mezcla que tiene estas funciones dispone del elemento 11 de ajuste inicial de la parte de gestión y el elemento 12 de control de la desencriptación.

El elemento 11 de ajuste inicial de la parte de gestión tiene funciones tales como la de generar y publicar información pública que incluye, por ejemplo, claves públicas de encriptación concertadamente con cada uno de los centros 20-1 a 20-m mezcladores de desencriptación, cuando se reciben parámetros de seguridad como entrada desde el exterior. El elementos 12 de control de la desencriptación tiene la función de, cuando se recibe una lista de datos encriptados como entrada desde el exterior, usar sucesivamente cada uno de los centros 20-1 a 20-m mezcladores de desencriptación para desencriptar la lista de datos encriptados y publicar una lista de desencriptación resultante, que es el resultado de la desencriptación.

El elemento de registro K10, que está conectado al centro de gestión 10 de mezcla, es un disco, una memoria de semiconductor u otro tipo de elemento de registro, y graba un programa para hacer que el centro 10 de gestión de mezcla, que está constituido por un ordenador, opere como parte del sistema anónimo de desencriptación. Este programa lo lee el centro de gestión 10 de mezcla que está constituido por un ordenador, y, mediante el control de las operaciones del centro de gestión 10 de mezcla, verifica el elemento 11 de ajuste inicial de la parte de gestión y el elemento 12 de control de la desencriptación.

Los centros 20-1 a 20-m mezcladores de señales están constituidos por ordenadores y están conectados al centro de gestión 10 de mezcla mediante, por ejemplo, un circuito dedicado. Cada uno de los centros 20-1 a 20-m mezcladores de desencriptación tiene las funciones de, por ejemplo, funcionar concertadamente con el centro de gestión 10 de

mezcla para realizar un proceso inicial de ajuste y subsiguientemente realizar un proceso de conexión de órdenes, y un proceso de desencriptación parcial en la lista de datos encriptados que se transmite desde el centro de gestión 10 de mezcla de señales y devolver el resultado del procesamiento al centro de gestión 10 de mezcla.

Cada uno de los centros 20-1 a 20-m mezcladores de señales de desencriptación que tienen estas funciones está provisto de, por ejemplo, elemento 21 de ajuste inicial de la parte de mezcla, el elemento 23 de desencriptación parcial y el elemento de certificación 24, como se representa en la Fig. 3.

El elemento 21 de ajuste inicial de la parte de mezcla tiene las funciones de realizar un proceso inicial de ajuste concertadamente con el elemento 11 de ajuste del lado de la gestión. En este proceso de ajuste inicial, el elemento 21 de ajuste inicial de la parte de mezcla genera claves públicas y claves de desencriptación. El elemento mezclador 22 tiene la función de someter listas de datos encriptados que se transmiten desde el centro de gestión 10 de mezcla a un proceso de conexión de órdenes. El elemento 23 de desencriptación parcial tiene la función de someter las listas de datos encriptados a un proceso parcial de desencriptación después de que el elemento 22 mezclador ha realizado el proceso de conexión de órdenes. El elemento de certificación 24 tiene las funciones de generar datos de certificación para certificar que el procesamiento del elemento 22 mezclador es correcto y generar datos de certificación para certificar que el procesamiento del elemento 23 de desencriptación parcial es correcto.

El elemento de registro K20-j, que está conectado al centro 20-j mezclador de desencriptación, es un disco, una memoria de semiconductor u otros tipo de elemento de registro, y graba un programa para causar que el centro 20-j mezclador de desencriptación, que está constituido por un ordenador, funcione como parte del sistema anónimo de desencriptación. Este programa lo lee el centro de gestión 20-j mezclador de desencriptación que está constituido por un ordenador, y, mediante el control de las operaciones del centro 20-j mezclador de desencriptación, verifica el elemento 21 de ajuste inicial de la parte de mezcla, el elemento 22 mezclador, el elemento 23 de desencriptación parcial y el elemento de certificación 24 en el centro 20-j mezclador de señales de desencriptación.

La siguiente explicación se refiere a los detalles operativos de esta realización.

Proceso inicial de ajuste

Primeramente, en cuanto al proceso de ajuste inicial, cuando se reciben parámetros de seguridad (*pL, qL, t*) a los que se ha añadido un ID de sesión, como entrada desde el exterior, el elemento 11 de ajuste inicial del lado de gestión en el centro de gestión 10 de mezcla genera información pública común (*p, q, g*) (Fig. 4, A1). Aquí, *p* y *q* son parámetros de un criptosistema de El Gamal y son dos números primos en una relación tal que $p = kq + 1$, siendo *k* un número entero particular. La variable *g* es un generador de subgrupos de orden *q* en el módulo *p*. Además, *pL* y *qL* son las longitudes de los números primos *p* y *q*, respectivamente y *t* es el número de repeticiones usado cuando se generan datos de certificación para certificar que un proceso de conexión de órdenes (a explicar) es correcto y cuando se verifican los datos de certificación antes descritos. El ID de sesión es un identificador para especificar el objeto de procesamiento, y el objeto de procesamiento es, por ejemplo, la elección de un gobernador de una prefectura o la elección de los miembros de una organización ciudadana.

El elemento de ajuste inicial 11 del lado de gestión produce luego una declaración de requerimiento para generar una clave pública que incluye información pública común (*p, q, g*), une la signatura digital del centro de gestión 10 de mezcla y el ID de sesión ID a esta declaración de requerimiento y luego transfiere la declaración a todos los centros 20-1 a 20-m (A2) mezcladores de desencriptación.

El elemento 21 de ajuste inicial del lado de mezclador de señales de cada centro 20-1 a 20-m mezclador de desencriptación realiza la autentificación mediante verificación de la signatura digital que está unida a la declaración de requerimiento para la generación de una clave pública (A3). Si la signatura no es correcta, el elemento 21 de ajuste inicial del lado del mezclador actúa terminando el proceso. Por otra parte, si la signatura es correcta, el elemento 21 de ajuste inicial del lado del mezclador autentifica la corrección de la información pública común (*p, q, g*). Con otras palabras, el elemento 21 de ajuste inicial del lado del mezclador investiga si (*p, q, g*) satisfacen la relación que está descrita en el párrafo [0026]. Si no se puede confirmar la corrección, el elemento 21 de ajuste inicial del lado del mezclador actúa terminando el proceso. Por otra parte, si el elemento 21 de ajuste inicial del lado del mezclador puede confirmar la corrección, el elemento 21 de ajuste inicial del lado del mezclador genera un clave pública y una clave de desencriptación (clave privada) basadas en información pública común (*p, q, g*) y almacena estas claves en correspondencia con el ID de sesión dentro de su propio centro mezclador de desencriptación (A4). Por ejemplo, un centro 20-j mezclador de señales de desencriptación que tiene la prioridad j^{ava} en la prioridad de procesamiento selecciona al azar x_i mod *q* y toma este valor como clave de desencriptación. La clave pública y_j de este centro 20-j mezclador de desencriptación se genera a partir de:

$$y_j = g^{xi} \bmod p$$

Los elementos 21 de ajuste inicial del lado del mezclador de en cada uno de los centros 20-1 a 20-m mezcladores de desencriptación generan luego datos de certificación de forma que cada centro mezclador de desencriptación conoce

la clave de desencriptación para la clave pública que se generó en la Etapa A4 (A5). Por ejemplo, el medio 21 de ajuste inicial del lado del mezclador en el centro 20-j mezclador de desencriptación, que tiene la prioridad j^{ava} en prioridad de procesamiento, genera los datos de certificación y_j, r_j certificando que la clave de desencriptación para la clave pública x_j para la clave pública y_j

$$y'_j = g^{\beta_j} \bmod p$$

$$c_j = Hash(p, q, g, y_j, y'_j)$$

$$r_j = c_j x_j + \beta_j \bmod q$$

en la que *Hash* es una función Hash segura y β_j es un número al azar. Cuando el proceso de la Etapa A5 se ha completado, el elemento 21 de ajuste inicial del lado del mezclador de señales en cada uno de los centros 20-1 a 20-m mezcladores de desencriptación produce una declaración de requerimiento de registro de clave pública que incluye la clave pública que se generó en la Etapa A4 y los datos de certificación que se generaron en la Etapa A5, une la signatura digital de su propio centro mezclador de desencriptación y un ID de sesión a esta declaración de requerimiento y devuelve la declaración a al centro 10 de gestión del mezclar (A6).

El elemento 11 de ajuste inicial del lado de gestión del centro 10 de gestión de mezcla realiza la autentificación del emisor mediante verificación de la signatura digital que está unida a la declaración de requerimiento de registro de la clave pública que se devuelve de cada uno de los centros 20-1 a 20-m mezcladores (A7) y, además, verifica la corrección de las claves públicas que se devuelven de cada uno de los centros 20-1 a 20-m mezcladores de señales de desencriptación (A7) mediante las siguientes ecuaciones (AB):

$$c_j = Hash(p, q, g, y_j, y'_j)$$

$$g^{r_j} y_j^{-c_j} = y'_j \bmod p$$

$$y_j^{q} = 1 \bmod p$$

$$y_j \neq 1 \bmod p$$

Cuando todas las declaraciones de requerimiento de registro de claves públicas que se han devuelto desde centros 20-1 a 20-m mezcladores de desencriptación han pasado la verificación de las Etapas A7 y A8, las claves públicas y_1 a y_m que se han devuelto desde cada uno de los centros 20-1 a 20-m mezcladores de desencriptación se combinan mediante:

$$Y = \prod_{j=1}^{m} y_j \bmod p$$

para generar la clave *Y* de encriptación pública que se usa cuando los usuarios del sistema encriptan datos (A9).

El elemento 11 de ajuste inicial del lado de gestión genera luego información pública que incluye la clave pública *Y* de encriptación, las claves públicas y_1 a y_m de cada uno de los centros 20-1 a 20-m mezcladores de desencriptación, información pública común(*p, q, g*) y los ID de centros mezcladores de desencriptación de cada uno de los centros 20-1 a 20-m mezcladores de desencriptación (para informar a los usuarios de la organización que está encargada de la desencriptación) y publica esta información pública en correspondencia con el ID de sesión ID (A10). Esto completa el proceso de ajuste inicial.

La explicación siguiente concierne al proceso de desencriptación

La lista de datos encriptados $\{(G_i, M_i)\}_{(i=1,2...n)}$ que contiene n materias de datos encriptados se aplica como entrada desde el exterior al elemento 12 de control de la desencriptación en el centro 10 de gestión de mezcla de señales. El ID de sesión ID para especificar el objeto del procesamiento para el que son relevantes estos datos está unido a esta lista de datos encriptados.

Los datos encriptados (G_i,M_1) son datos encriptados que corresponden a datos m_i y se obtienen de:

$$(G_i, M_i) = (g^{ri}, m_i Y^{ri}) \bmod p$$

en la que los datos m_i se seleccionan de manera que el orden es q. Además, r_i es un número al azar seleccionado arbitrariamente para los datos m_i.

Cuando la lista de datos encriptados $\{(G_i, M_i)\}_{(i=1,2,n)}$ se recibe como entrada, el elemento 12 de control de la desencriptación en el centro 10 de gestión de mezcla confirma primeramente que el orden de G_1 y M_1 es q para todos los i y luego une el ID de sesión y la signatura digital del centro 10 de gestión de mezcla a la lista de datos encriptados y transfiere la lista de datos encriptados al centro 20-1 mezclador de desencriptación, que es el primero en la prioridad de procesamiento (B1 y B2 en la Fig. 5). La lista de datos encriptados que se transfiere al centro 20-j mezclador de desencriptación, que es el j.^{avo} en la prioridad de procesamiento, está representada por $\{(G^{(j)}{}_i, M^{(j)}{}_i)\}_{(n=12,2,...n)}$.

El centro 20-1 mezclador de desencriptación realiza la autentificación del emisor verificando la signatura digital que está unida a la lista de datos encriptados $\{(G^{(1)}{}_i, M^{(1)}{}_i)\}_{(i=1,2...n)}$. (C1 en la Fig. 6).Si la signatura digital es correcta, el elemento 22 mezclador y el elemento 23 de desencriptación parcial se usan para someter la lista de datos encriptados descrita antes a un proceso de conexión de órdenes y un proceso de desencriptación parcial para obtener una lista de datos que es el resultado del procesamiento (C2 y C3). Los detalles del proceso de conexión de órdenes y el proceso de desencriptación parcial se explicarán más adelante. El elemento de certificación 24 se usa luego para generar datos de certificación que indican que los procesos realizados por el elemento 22 mezclador y el elemento 23 de desencriptación parcial son correctos (C4). La signatura digital y el ID de sesión se unen luego a la lista de datos y los datos de certificación y retornan al centro 10 de gestión de mezcla de señales (C5). Los datos de certificación se pueden unir a la lista de datos y restituir al centro 10 de gestión de la mezcla de señales, o se puede devolver primeramente sólo la lista de datos y separadamente, más tarde, los datos de certificación. Más adelante se explicarán detalles del procedimiento para generar los datos de certificación.

Cuando los datos de certificación y la lista de datos unidos con la signatura y el ID de sesión vuelven desde el centro 20-1 mezclador, el elemento 12 de control de la desencriptación en el centro 10 gestión de mezcla realiza la autentificación del emisor y verifica los datos de certificación basados en la signatura digital (B3 en la Fig. 5). Se explicarán más adelante detalles referentes al procedimiento de verificación de los datos de certificación. Si la signatura digital y los datos de certificación son correctos, la lista de datos que se ha devuelto desde el centro 20-1 mezclador de desencriptación, que es el primero en prioridad de procesamiento, se transfiere como lista de datos encriptados al centro 20-2 mezclador de desencriptación, que es el segundo en prioridad de procesamiento (B4 a B6). En este momento, el elemento 12 de control de la desencriptación añade el ID de sesión a la lista de datos encriptados.

En el centro 20-2 mezclador de desencriptación se realizan los mismos procedimientos realizados en el centro 20-1 mezclador de desencriptación (C1 a C5 en la Fig. 6) y se devuelven al centro 10 de gestión de mezcla los datos de certificación y la lista de datos a que se han unido la signatura digital y ID el de sesión.

De esta manera, el elemento 12 de control de la desencriptación del centro 10 de gestión de mezcla realiza los procesos iguales a los descritos previamente (B3 a B6 en la Fig. 5).El procesamiento descrito antes es realiza repetidamente hasta que la lista de certificación y la lista de datos a las que se han unido la signatura digital y la sesión ID han vuelto del centro 20-m mezclador de desencriptación, que es el último en la prioridad de procesamiento, después de lo cual, el elemento 20 de control de la desencriptación publica la lista de datos antes descrita como lista resultado de la desencriptación (B7). En este momento se publican los ID de los centros mezcladores de desencriptación de los centros 20-1 a 20-m mezcladores de desencriptación, el ID del centro de gestión de mezcla del centro 10 de gestión de la mezcla, los ID de sesión y cada uno de los asuntos de los datos de certificación que han vuelto de cada uno de los centros 20-1 a 20-m mezcladores de desencriptación.

La siguiente explicación considera los detalles del proceso de conexión de órdenes que realiza el elemento mezclador, el procedimiento de desencriptación parcial realizado por el elemento 23 de desencriptación parcial, el procedimiento de generación de datos de certificación que realiza el elemento 24 de certificación y el procedimiento de verificación que realiza el elemento 12 de control de la desencriptación.

Procedimiento de conexión de órdenes

La explicación considera el proceso de conexión de órdenes que realiza el elemento 22 mezclador de señales del centro 20-j mezclador de desencriptación, que es el j^{avo} en cuanto a prioridad de procesamiento. El proceso de conexión de órdenes se hace por un procedimiento de mezcla y un procedimiento de reencriptación que se describen seguidamente.

El elemento 22 mezclador realiza primeramente un proceso de mezcla. En el procedimiento de mezcla de señales, el elemento mezclador 22 determina aleatoriamente un mapeo $\pi^{(j)}$ para datos encriptados $(G^{(j)}{}_i, M^{(j)}{}_i)_{(i\ =\ 1,2.....n)}$ en la lista de datos encriptados $\{(G^{(j)}{}_i, M^{(j)}{}_i)\}_{(i\ =\ 1,2.....n)}$ que han sido transmitidos desde el centro 10 de gestión de mezcla, conecta el orden de $(G^{(j)}{}_i, M^{(j)}{}_i)_{(i\ =\ 1,2.....n)}$ sobre la base del mapeo de permutación y obtiene luego:

$$\{(\overline{G}_i^{(j)}, \overline{M}_i^{(j)})\}_{(i=1,2,\ldots,n)}$$

Éste es el proceso de mezcla

$$\{(\overline{G}_i^{(j)}, \overline{M}_i^{(j)})\} = \{(G_{\pi(j)(i)}^{(j)}, M_{\pi(j)(i)}^{(j)})\}_{(i=1,2,\ldots,n)}$$

que se realiza ahora.

El procedimiento de reencriptación se realiza después de haber finalizado el proceso de mezcla. La reencriptación implica cambiar el aspecto de los datos encriptados sin cambiar el contenido de los datos encriptados. La reencriptación es necesaria porque el mero cambio de las posiciones permite la posibilidad de rastrear los datos encriptados desde la configuración bit de los datos encriptados.

El elemento 22 mezclador de desencriptación del centro 20-j mezclador de desencriptación, que es el $j^{avo.}$ en prioridad de procesamiento, combina las claves públicas de los centros mezcladores de desencriptación que vienen después del centro 20-j de mezcla de señales de desencriptación para encontrar:

$$Y = \prod_{j=1}^{m} y_j \bmod p$$

Se genera un número al azar $s^{(j)}{}_i \bmod q$ para

$$\{(\overline{G}_i^{(j)}, \overline{M}_i^{(j)})\}_{(i=1,2,\ldots,n)}$$

que ha experimentado el proceso de mezcla por lo que $\{(G^{(j)}{}_i, M^{(j)}{}_i)\}_{(n=1,2..n)}$ se encuentra mediante

$$G_i'^{(j)} = \overline{G}_i^{(j)} \cdot g^{s_i^{(j)}} \bmod p$$

$$M_i'^{(j)} = \overline{M}_i^{(j)} \cdot Y^{s_i^{(j)}} \bmod p$$

La generación de Y_j y el número al azar $s^{(j)}{}_i$ y el cálculo de $g^{si(i)}, Y^{si(i)}$ se puede hacer por cálculo antes de recibir la lista de datos encriptados. Si se almacenan los valores que se han calculado previamente, el procedimiento de encriptación se puede realizar por un procedimiento de multiplicación individual para cada componente de los datos.

Procedimiento de desencriptación parcial

La explicación siguiente considera el procedimiento de desencriptación parcial que es realizado por el elemento 23 de desencriptación parcial en el centro 20-j mezclador de desencriptación.

El elemento 23 de desencriptación parcial usa una clave x_j de desencriptación (una clave de desencriptación que corresponde al ID de sesión que está unida a la lista de datos encriptados) que tiene su propio centro 20-j mezclador de desencriptación en $\{(G(j)_i, M^{(j)}{}_i)\}_{(i=1,2..n)}$ que ha experimentado un proceso de conexión de órdenes por el elemento 22 mezclador para calcular

$$M_i''^{(j)} = M_i'^{(j)} / (G_i'^{(j)})^{x_j} \bmod p$$

$$G_i''^{(j)} = G_i'^{(j)}$$

Seguidamente se devuelve $\{(G(j)_i, M^{(j)}{}_i)\}_{(i=1,2..n)}$ al centro 10 de gestión de mezcla como lista de datos.

Procedimiento de generación de datos de certificación

La explicación siguiente considera el procedimiento de generar datos de certificación por el elemento de certificación 24. En la explicación siguiente se omite la notación (*j*) para identificar el centro mezclador de desencriptación.

La explicación considera primeramente el procedimiento para generar datos para la generación de $\{(G(j)_i, M^{(j)}_i)\}_{(i=1,2..n)}$ mientras que se mantiene el π del mapeo de permutación y la secuencia (s_i) de número al azar. Aquí $\{(G(j)_i, M^{(j)}_i)\}_{(i=1,2..n)}$ es generado por los elementos mezcladores que realizan el proceso de mezclar para la lista de datos $\{(G^{(j)}_i, M^{(j)}_i)\}_{(i=1,2..n)}$ usando π de mapeo de permutación y usan la información de clave pública (*p, q, g*) y la secuencia de número al azar $\{s_j\}_{(i\ =\ 1,2...n)}$. En lo que sigue, *t* representa un parámetro de seguridad (número de repetición).

1. Se generan *t* piezas de mapeos de permutación al azar π'_u y *t x n* piezas de números al azar $\{s'_{(u,v)}\}$ para calcular:

$$A_{u,v} = G_{\pi'_u(v)} \cdot g^{s'(u,v)} \bmod p$$

$$B_{u,v} = M_{\pi'_u(v)} \cdot Y_j^{s'(u,v)} \bmod p$$

para $u = 1, 2, \ldots, t$ y $v = 1, 2, \ldots, n$.

2. Se realiza el siguiente cálculo:

$$c = \text{Hash}(p||q||g||Y_j||\{(G_i, M_i)\}_{(i\ =\ 1,\ 2,\ \ldots,\ n)}||\{(G'_i, M'_i)\}_{(i\ =\ 1,\ 2,\ \ldots,}$$

$$\{(A_{(u,v)}, B_{(u,v)})\}_{(u\ =\ 1,\ 2,\ \ldots,\ t,\ v\ =\ 1,\ 2,\ \ldots,\ n)})$$

Aquí, || representa conexión.

3. Representando $u^{avo} = u = s'_{(u,v)}$), bit de *c* como *c*[u], se realiza el cálculo siguiente:

$$\alpha_u = \pi'_u \text{ y } \beta_{(u,v)} = s'_{(u,v)} \text{ cuando } c[u] = 0; \text{ y}$$

$$\alpha_u = \pi^{-1} o \pi'_u \text{ y } \beta_{(u,v)} = s'_{(u,v)} - s_{(u,v)} - s_{(\pi^{-1} on' v(u)}, \text{ cuando } c[u] = 1.$$

La generación de los mapeos de permutación π'_u y los números al azar $\{s'_{(u,v)}\}$ y el cálculo de $g^{s'(u,v)}$, $Y_j^{s'(u,v)}$ se puede hacer por cálculo antes de recibir la lista de datos encriptados. Si se almacenan los datos que se han calculado antes, se puede reducir el tiempo de procesamiento.

La explicación siguiente considera el procedimiento de generación de datos de certificación para certificar que $\{[G''_i, M''_i)\}_{(i=1,2,\ldots,n),}$ que se ha calculado correctamente usando la clave privada *x* que corresponde a una clave pública propia *y* en el $\{[G''_i, M''_i)\}_{(i=1,2,\ldots,n)}$ antes descrito, se ha remitido al centro 10 de gestión de mezcla sin revelar la clave privada x.

1. Se genera el número al azar *r* mod *q*.

2. Se realiza el cálculo siguiente:

$$c = \text{Hash}(p||q||g||y||\{G'_i\}_{(i\ =\ 1,\ 2,\ \ldots,\ n)}||\{(M'_i/M''_i)\}_{(i\ =\ 1,\ 2,\ \ldots,\ n)}||$$

$$g^r||\{G'_i\}_{(i\ =\ 1,\ 2,\ \ldots,\ n)})$$

3. Se calcula α=r-*cx* mod *q*. c y α que se han encontrado como se ha señalado antes son los datos de certificación.

Procedimiento de verificación

La explicación considera el procedimiento de verificación realizado por el elemento 12 de control de desencriptación. La explicación considera primeramente la verificación de datos de certificación para certificar que el proceso del elemento 22 mezclador es correcto.

Los cálculos siguientes se realizan basándose en la información publicada y los datos de certificación:

$$c = \text{Hash}(p||q||g||Y_j||\{(G_i, M_i)\}_{(i = 1, 2, \ldots, n)}||\{(G'_i, M'_i)\}_{(i = 1, 2, \ldots, n)}||$$
$$\{(A_{(u,v)}, B_{(u,v)})\}_{(u = 1, 2, \ldots, t,\ v = 1, 2, \ldots, n)})$$

2. Si el bit u^{avo} (en el que $u = 1,2,...t$) de c es c[u], se comprueba si se cumple la relación siguiente cuando c[u] = 0

$$A_{U,V} = G_{\alpha_u(v)} \cdot g^{\beta_{(u,v)}} \bmod p$$

$$B_{U,V} = M_{\alpha_u(v)} \cdot Y_j^{\beta_{(u,v)}} \bmod p$$

Se comprueba si se cumple la relación siguiente cuando c[u] = 1,

$$A_{U,V} = G'_{\alpha_u(v)} \cdot g^{\beta_{(u,v)}} \bmod p$$

$$B_{U,V} = M'_{\alpha_u(v)} \cdot Y_j^{\beta_{(u,v)}} \bmod p$$

3. Se comprueba si el orden de G'$_1$,M_i es q. Cuando se han confirmado toda las relaciones, se considera que los daos de certificación son correctos.

La explicación siguiente considera la verificación de los datos de certificación que certifican que el proceso realizado por el elemento 23 de desencriptación parcial es correcto.

1. Se comprueba primeramente si $G'_{1=}$ G'$_i$ para todos los i.

2. Se comprueba si se cumple

$$c = \text{Hash}(p||q||g||y||\{G'_i\}_{(i = 1, 2, \ldots, n)}||\{(M'_i/M''_i)\}_{(i = 1, 2, \ldots, n)}||$$
$$g^{\alpha} \cdot y^{c}||\{G'^{\alpha}_i \cdot (M'_i/M''_i)^{c}\}_{(i = 1, 2, \ldots, n)})$$

3. Se comprueba luego si $M''^{q}_i = 1$ mod p para todos los i Si se confirman todas las relaciones, se considera que los datos de certificación son correctos.

De hecho, la certificación de mezcla y la certificación de la desencriptación se hacen al mismo tiempo y, consecuentemente, no hay necesidad de enviar $\{G'_i\}_{(i=1,2,...n)}$ que ha de ser G'$_i$ = G''_i para $\{G''_i\}_{(i=1,2,...n)}$ que se da como resultado de desencriptación. Así, en el trabajo real sólo se envía $\{M'_i\}_{(i=1,2,...n)}$ cuando se certifica la mezcla.

Aunque se ha omitido en la explicación anterior de operaciones, el ID del centro de gestión de mezcla o centro mezclador de desencriptación que es el destino de la transmisión de datos y el ID del centro de gestión de mezcla o centro mezclador de desencriptación que es la fuente de transmisión se añaden cuando se intercambian datos entre el centro de gestión de mezcla y los centros mezcladores de desencriptación. Por ejemplo, cuando se transfieren datos del centro 10 de gestión de mezcla al centro 20-1 mezclador de desencriptación, los ID del centro 20-1 mezclador de desencriptación y el centro 10 de gestión de mezcla de desencriptación se añaden como destino de la transferencia y fuente de la transferencia, respectivamente. Otro ejemplo, cuando se transmiten datos desde el centro 10 de gestión de mezcla a todos los centros 20-1 a 20-m mezcladores de desencriptación, los ID de los centros 20-1 a 20-m mezcladores de desencriptación y el ID de centro 10 de gestión de mezcla de desencriptación se añaden como destinos de la transferencia y fuente de la transferencia.

Seguidamente se hace referencia a la Fig. 7 para describir la segunda realización de la presente invención. Esta realización e adecuada para uso cundo se depositan papeletas (escrutinios) electrónicas anónimas y se añade un centro

30 de gestión del voto a la construcción que se ha proporcionado para el sistema de desencriptación anónima que se representa en la Fig. 1.

Como entrada, al centro 30 de gestión del voto se proporciona una lista de votantes registrados, parámetros de seguridad, el período de votación de la elección y el ID de sesión. El centro 30 de gestión del voto añade el ID de sesión antes descrito a los parámetros de seguridad antes descritos y los transfiere al centro 10 de gestión de mezcla.

Cuando se envían los parámetros de seguridad con el ID de sesión añadido desde el centro 30 de gestión del voto, el centro 10 de gestión de mezcla realiza el proceso de ajuste inicial descrito previamente (referencia, Fig.4) concertadamente con cada uno de los centros 20-1 a 20-m de mezcla de desencriptación y publica la información pública obtenida (que incluye, por ejemplo, las claves públicas y la información pública *p, q* y *g*). El centro 30 de gestión del voto comprueba si esta información pública es correcta de acuerdo con los parámetros de seguridad y luego la notifica a cada votante.

Cuando comienza el período de votación, los votantes encriptan sus propios datos de votación basándose en la información pública, añaden sus signaturas digitales de votante y envían los datos al centro 30 de gestión del voto. Aquí, el votante i^{avo} (siendo $i = 1,2,...n$) usa la clave pública publicada Y y la información pública común (p, q, g) para encriptar el contenido del voto m_i como se indica seguidamente. En este caso, se supone que el contenido del voto se selecciona de manera que el orden sea q.

Primeramente, el votante soluciona cualquier número al azar r_j mod q. Seguidamente se toman como datos de voto encriptados (G_i,M_i) obtenidos por

$$(G_i, M_i) = (g^{r_i}, m_i Y^{r_i}) \bmod p$$

Estos datos encriptados son remitidos al centro de votos 30 con la signatura digital propia del votante anexa.

Se puede certificar aquí que el votante ha preparado los datos encriptados del voto conociendo el m_i correcto. Por ejemplo, el votante i^{avo} genera el número al azar γ y luego genera los datos de certificación α y t_i mediante

$$\alpha_i = g^{\gamma_i} \bmod p$$

$$c_i = Hash(p, q, g, G_i, \alpha_i)$$

$$t_i = c_i r_i + \gamma_i \bmod q$$

Esta certificación se pude verificar mediante:

$$c_i = Hash(p, q, g, G_i, \alpha_i)$$

$$g^{t_i} G_i^{-c_i} = \alpha_i \bmod p$$

Alternativamente, el votante i^{avo} puede generar también un número al azar γ y generar luego los datos de certificación α y t_i mediante

$$\alpha_i = g^{\gamma_i} \bmod p$$

$$c_i = Hash(p, q, g, G_i, \alpha_i)$$

$$t_i = \gamma_i - c_i r_i \bmod q$$

Esta certificación se puede verificar mediante:

$$c_i = Hash(p, q, g, G_i, \alpha_i)$$

$$g^{t_i} G_i^{c_i} = \alpha_i \bmod p$$

El centro 30 de gestión del voto acepta las papeletas después de verificar las signaturas, confirmar los derechos de voto del votante sobre la base de la lista de votantes registrados y comprobar si hay voto doble. Cuando se han añadido los dato de certificación, el centro 30 de gestión del voto acepta las papeletas después de verificar adicionalmente los datos de certificación. Cuando termina el período de votación, el centro 30 de gestión del voto para la aceptación de papeletas y envía los datos de voto encriptados que se han aceptado como lista de datos encriptados con las signaturas digitales anexas al centro 10 de gestión de mezcla del sistema de desencriptación anónimo. Después de recibir la lista de datos encriptados, el centro 10 de gestión de mezcla desencripta la lista de datos por el procedimiento de desencriptación descrito previamente y devuelve los resultados de la desencriptación y los datos de certificación al centro 30 de gestión de votos.

El centro 30 de gestión del voto recoge los resultados de desencriptación que ha recibido como datos de votos posdesencriptación y anuncia los resultados.

Seguidamente se considera la Fig. 8 para describir la tercera realización de la presente invención. La presente invención es adecuada para uso en licitaciones electrónicas anónimas y se ha añadido un centro 40 de gestión de licitación a la construcción que se ha proporcionado para el sistema de desencriptación anónima representado en la Fig. 1.

Como entrada al centro 40 de gestión de licitación se aplican una lista de licitaciones, parámetros de seguridad, período de licitaciones e ID de sesión. El centro 40 de gestión de licitación añade el ID de sesión descrito antes a los parámetros de seguridad antes descritos y los transfiere al centro 10 de gestión de mezcla.

Cuando los parámetros de seguridad con el ID de sesión añadido se envían desde el centro 40 de gestión de licitación, el centro 10 de gestión de mezcla realiza el proceso de ajuste inicial descrito previamente (referencia, Fig. 4) concertadamente con cada uno de los centros 20-1 a 20-m mezcladores de desencriptación y publica la información pública obtenida (que incluye, por ejemplo, las claves públicas *Y* y la información pública común *p, q* y *g*). El centro 40 de gestión de licitación comprueba si esta información pública es correcta de acuerdo con los parámetros de seguridad y luego lo notifica a cada licitador.

Cuando comienza el período de licitación, los licitadores encriptan sus valores de licitación propios sobre la base de la información pública, añaden sus signaturas digitales de licitación y envían los datos al centro 40 de gestión de licitación. En este momento se pueden transmitir los datos de certificación para certificar que los licitadores conocen sus valores de licitación propios (datos de certificación que son similares a los datos de certificación descritos en la segunda realización).

El centro 40 de gestión de licitación acepta las licitaciones de después de verificar las signaturas, confirmar los derechos de los licitadores a licitar basándose en la lista de licitadores y comprobar si hay doble licitación. Cuando se han enviado también los datos de certificación, el centro 40 de gestión de licitación acepta las licitaciones después de verifica adicionalmente los datos de certificación. Cuando termina el período de licitación, el centro 40 de gestión de licitación detiene la aceptación de licitaciones y envía los valores de licitaciones encriptadas que se han aceptado como lista de datos encriptados al centro 10 del sistema de desencriptación anónimo. Después de recibir la lista de datos encriptados, el centro 10 de gestión de mezcla desencripta la lista de datos por el procedimiento de desencriptación descrito previamente y devuelve los resultados de la desencriptación y los datos de certificación al centro 40 de gestión de licitación.

El centro 40 de gestión de la licitación anuncia los resultados de la desencriptación que ha recibido como valores de licitación posdesencriptación.

Seguidamente se considera la Fig. 9 para describir la cuarta realización de la presente invención. La presente invención es adecuada para uso cuando se realiza un sondeo electrónico anónimo y, por tanto, se ha añadido un centro receptor 50 a la construcción que se proporciona para el sistema de desencriptación anónima representado en la Fig. 1.

Al centro receptor 50 se aplican como entrada una lista de responsables, parámetros de seguridad, período de sondeo e ID de sesión. El centro receptor 50 añade el ID de sesión antes descrito a los parámetros de seguridad antes descritos y los transfiere al centro 10 de gestión de mezcla.

Cuando los parámetros de seguridad con el ID de sesión añadido se envían desde el centro receptor 50, el centro 10 de gestión de mezcla realiza el proceso de ajuste inicial descrito previamente (referencia, Fig. 4) concertadamente con cada uno de los centros 20-1 a 20-m mezclador de desencriptación y publica la información pública obtenida (que incluye, por ejemplo, las claves públicas *Y* y la información pública común *p, q* y *g*). El centro receptor 50 comprueba si esta información pública es correcta de acuerdo con los parámetros de seguridad y luego lo notifica a cada responsable.

Cuando comienza el período de sondeo, los responsables encriptan sus respuestas de sondeo propias sobre la base de la información pública, añaden sus signaturas digitales de responsables y envían los datos al centro receptor 50. En este momento se pueden transmitir los datos de certificación para certificar que los responsables conocen sus propias

respuestas de sondeo (datos de certificación que son similares a los datos de certificación descritos en la segunda realización).

El centro receptor 50 acepta las respuestas de sondeo después de verificar las signaturas, confirmar el derecho de los responsables a responder basándose en la lista de responsables y confirmar si hay dobles respuestas. Cuando se han enviado también los datos de certificación, el centro receptor 50 acepta las respuestas después de verifica adicionalmente los datos de certificación. Cuando termina el período de sondeo, el centro receptor 50 detiene la aceptación de respuestas de sondeo y envía las respuestas de sondeo encriptadas que se han aceptado como lista de datos encriptados al centro 10 de gestión de mezcla del sistema de desencriptación anónimo. Después de recibir la lista de datos encriptados, el centro 10 de gestión de mezcla desencripta la lista de datos por el procedimiento de desencriptación descrito previamente y devuelve los resultados de la desencriptación y los datos de certificación al centro receptor 50.

El centro receptor 50 anuncia los resultados de la desencriptación que ha recibido como respuestas de sondeo después de la desencriptación.

Además de las realizaciones descritas, se puede considerar también la conveniente verificación de la corrección de la información o los datos que se han publicado por un centro o tercera parte. Además, las fórmulas numéricas que se refieren al procedimiento de certificación son sólo un ejemplo, y un experto en la técnica puede llegar fácilmente a modificaciones de las fórmulas que producirían los mismos resultados.

Potencial para aplicación en la industria

Como se ha descrito en la explicación anterior, la presente invención permite la desencriptación de una lista de datos encriptados meramente intercambiando datos entre un centro de gestión de mezcla y centros mezcladores de desencriptación y tiene así el mérito de eliminar la necesidad de un procesamiento de la gestión complejo tal como el del sistema de descripción anónimo de la técnica anterior que usa un sistema de pantalla de información electrónico.

En la presente invención, además, el centro de gestión de mezcla y los centros mezcladores de desencriptación generan información pública que incluye claves públicas para encriptación concertadamente sobre la base de parámetros de seguridad que se reciben como entrada desde el exterior y, como resultado, la presente invención tiene además el mérito de permitir operaciones de ajuste inicial más fáciles y fiables.

A mayor abundamiento, un centro mezclador de desencriptación que gestiona la clave de desencriptación, que es el secreto importante, no exige una conexión directa con un sistema de información electrónico de pantalla que a su vez sea accesible para un gran número no especificado de personas y, por tanto, la presente invención es considerablemente ventajosa desde el punto de vista de la seguridad. Además, la construcción de los centros de mezcla de desencriptación se puede concentrar en sólo los procesos que se refieren a la clave de desencriptación y las funciones de comunicación con el centro de gestión de mezcla y, por tanto, la presente invención tiene adicionalmente el mérito de que un centro de mezcla de desencriptación puede ser realizado en un formato compacto. Finalmente, las funciones de gestión de sesiones y las funciones de gestión de claves de desencriptación están repartidas entre el centro de gestión de mezcla y los centros mezcladores de desencriptación y, como resultado, no sólo es posible una desencriptación anónima, sino que son posibles una pluralidad de casos de procesos de desencriptación anónima y, por tanto, se pueden realizar con un alto nivel de seguridad servicios tales como votaciones electrónicas, licitaciones electrónicas y sondeos electrónicos.

REIVINDICACIONES

1. Un sistema anónimo de desencriptación de votación y licitación que toma como entrada una lista de datos encriptados que incluye una pluralidad de cuestiones de datos encriptados que han sido encriptados por un procedimiento especificado y parámetros públicos especificados que suministra resultados de cada cuestión de desencriptación de datos encriptados de la lista de datos encriptados sin revelar la relación al orden en la lista, sistema de desencriptación anónimo que comprende:

(a) un centro (10) de gestión de mezcla y una pluralidad de mezcladores (20-1 a 20-m) cada uno de los cuales tiene su propia clave de desencriptación;

en el que:

para el mismo objeto de procesamiento, se añade un ID de sesión común para parámetros públicos mutuamente relevantes, listas de datos encriptados y claves de desencriptación que tienen los mezcladores;

el mencionado centro (10) de gestión de mezcla está adaptado de manera que, cuando se recibe como entrada desde el exterior una lista de datos encriptados con su correspondiente ID de sesión, transfiere la mencionada lista de datos encriptados al mezclador que es el primero en prioridad de procesamiento; cuando una lista de datos con el ID de sesión vuelve desde un mezclador diferente del mezclador último en prioridad de procesamiento, transfiere la mencionada lista de datos con el mencionado ID de sesión que ha vuelto al mezclador siguiente en la prioridad de procesamiento después de que el mezclador que devolvió la mencionada lista de datos con el mencionado ID de sesión como una lita de datos encriptados con ID de sesión; y cuando una lista de datos con ID de sesión vuelve desde el mezclador último en prioridad de procesamiento, suministra la mencionada lista de datos con ID de sesión como lista resultado de desencriptación; y cada uno de los mencionados mezcladores (20-1 a 20-m) está adaptado de manera que somete una lista de datos encriptados con el correspondiente ID de sesión que se transfiere desde el centro de gestión de mezcla a un proceso de conexión de órdenes usando parámetros públicos y a un proceso de desencriptación parcial usando parámetros públicos y un proceso de desencriptación parcial usando una clave de desencriptación en posesión de ese mezclador, realizando un proceso de conexión de órdenes usando parámetros públicos que corresponden al mencionado ID de sesión, añadiendo el mencionado ID de sesión a una lista de datos resultante y devolviendo la lista de datos con el mencionado ID de sesión al mencionado centro de gestión de mezcla.

2. El sistema de desencriptación anónimo de acuerdo con la reivindicación 1, en el que el mezclador mencionado está adaptado para dar cuenta al mencionado centro de gestión de mezcla certificación de que el proceso de conexión de órdenes se ha realizado correctamente y que el proceso de desencriptación parcial se ha realizado correctamente.

3. El sistema de desencriptación anónimo de acuerdo con la reivindicación 1, en el que el mezclador mencionado está adaptado para unirse a la mencionada lista de datos que resulta de la certificación de que el proceso de conexión de órdenes se ha realizado correctamente y el proceso de desencriptación parcial se ha realizado correctamente, y dar cuenta al mencionado centro de gestión de mezcla.

4. El sistema de desencriptación de acuerdo con la reivindicación 2 o 3, en el que el mencionado centro de gestión del mezcla está adaptado para verificar que la certificación realizada por un centro marcado de desencriptación es correcta.

5. El sistema de desencriptación de acuerdo con la reivindicación 2 o 3, en el que el mencionado centro de gestión de mezcla está adaptado para, después de verificar que la certificación realizada por un mezclador es correcta, transferir una lista de datos que ha sido devuelta desde el mencionado mezclador a un mezclador que tiene la siguiente prioridad de procesamiento como lista de datos encriptados.

6. El sistema de desencriptación anónimo de acuerdo con la reivindicación 2, 3, 4 o 5, en el que el mencionado centro de gestión de mezcla está adaptado para añadir a la mencionada lista resultado de la desencriptación certificación de que ha sido comunicado por todos los mezcladores y suministrar un resultado como producto.

7. El sistema de desencriptación anónimo de acuerdo con la reivindicación 1, en el que el mencionado centro de gestión de mezcla y el mencionado mezclador están adaptados para realizar la autentificación de un emisor durante la comunicación.

8. El sistema de desencriptación anónimo de acuerdo con la reivindicación 1, en el que el mencionado centro de gestión de mezcla y el mencionado mezclador están adaptados para añadir a los datos de comunicación una signatura digital de una fuente de transmisión.

9. El sistema de desencriptación anónimo de acuerdo con la reivindicación 1, en el que:

el mencionado centro de gestión de mezcla está adaptado para, cuando se recibe un parámetro de seguridad como entrada, generar parámetros comunes públicos basados en el mencionado parámetro de seguridad; notificar a todos los mezcladores la mencionada información común pública generada; y, cuando vuelven desde todos los mezcladores cla-

ves públicas de encriptación, generar claves públicas de encriptación basadas en las claves públicas de todos los mezcladores y publicar parámetros públicos que incluyen las mencionadas claves de encriptación públicas generadas y el mencionado parámetro público común; y el mencionado mezclador está adaptado para generar una clave pública y una clave de desencriptación basada en el parámetro común público que se ha comunicado desde el mencionado centro de gestión de mezcla y devolver la mencionada clave pública generada al mencionado centro de gestión de mezcla.

10. El sistema de desencriptación anónimo de acuerdo con la reivindicación 9, en el que el mencionado mezclador está adaptado para, cuando una clave pública vuelve al mencionado centro de gestión de mezcla, añadir certificación de que la mencionada clave pública se ha generado correctamente y devolver la mencionada clave pública al mencionado centro de gestión de mezcla.

11. El sistema de desencriptación anónimo de acuerdo con la reivindicación 10, en el que el mencionado centro de gestión de mezcla está adaptado para verificar que un certificado que se ha añadido a una clave pública es correcto.

12. El sistema de desencriptación anónimo de acuerdo con la reivindicación 10 u 11, en el que el mencionado centro de gestión de mezcla está adaptado para publicar una clave pública y un certificado que se ha añadido a la mencionada clave pública junto con información pública.

13. El sistema de desencriptación anónimo de acuerdo con la reivindicación 9, en el que el mencionado centro de gestión de mezcla y el mencionado mezclador están adaptados para realizar la autentificación del emisor durante la comunicación.

14. El sistema de desencriptación anónimo de acuerdo con la reivindicación 9, en el que el mencionado centro de gestión de mezcla y el mencionado mezclador están adaptados para conferir una signatura digital de un emisor a datos de comunicación.

15. El sistema de desencriptación anónimo de acuerdo con la reivindicación 1, en el que el mencionado centro de gestión de la mezcla está adaptado para añadir, además del mencionado ID de sesión, un ID de centro de gestión de mezcla que está conferido a ese centro de gestión de mezcla, un ID de mezclador que está conferido a un mezclador que es el destino de la transmisión, y una signatura de ese centro de gestión de mezcla cuando se transfiere una lista de datos encriptados a un mezclador.

16. El sistema de desencriptación anónimo de acuerdo con la reivindicación 1, en el que el mencionado mezclador está adaptado para añadir, además del mencionado ID de sesión, un ID de mezclador que está conferido a ese centro de gestión de la mezcla, un ID de centro de gestión de mezcla que está conferido al mencionado centro de gestión de mezcla, y una signatura de ese mezclador cuando vuelve una lista de datos al mencionado centro de gestión de mezcla.

17. El sistema de desencriptación anónimo de acuerdo con la reivindicación 16, en el que el mencionado mezclador está adaptado para añadir datos certificando que se ha realizado correctamente el proceso de conexión de órdenes y datos certificando que el proceso de desencriptación parcial se ha realizado correctamente cuando una lista de datos vuelve al mencionado centro de gestión de mezcla.

18. El sistema de desencriptación anónimo de acuerdo con la reivindicación 6, en el que la información que se suministra como salida por el mencionado centro de gestión de mezcla comprende:

un ID de centro de gestión de mezcla que está conferido a ese centro de gestión de mezcla,

una lista de datos encriptados que se ha recibido como entrada desde el exterior,

una lista resultado de desencriptación para esa lista de datos encriptados,

un ID de sesión que ha sido conferido a la mencionada lista de datos encriptados,

todos los datos que han sido devueltos de todos los mezcladores, y

una signatura del centro de gestión de mezcla.

19. El sistema de desencriptación anónimo de acuerdo con la reivindicación 9, en el que el mencionado centro de gestión de mezcla está adaptado para, cuando se notifican parámetros públicos y parámetros de seguridad a los mezcladores, añadir:

un ID de centro de gestión de mezcla que está conferido a ese centro de gestión de mezcla,

IDs de mezclador de todos los mezcladores que realizan desencriptación,

el ID de sesión, y

una signatura de ese centro de gestión de mezcla.

20. El sistema de desencriptación anónimo de acuerdo con la reivindicación 9 o 10, en el que el mencionado mezclador está adaptado para añadir a la información que se devuelve a un centro de gestión de mezcla:

un ID de centro de gestión de mezcla que está conferido al mencionado centro de gestión de mezcla;

el ID de sesión;

un ID de mezclador de ese mezclador, y una signatura de ese mezclador.

21. El sistema de desencriptación anónimo de acuerdo con la reivindicación 9, en el que la información pública que publica el mencionado centro de gestión de mezcla comprende:

un ID de centro de gestión de mezcla que está conferido a ese centro de gestión de mezcla;

el ID de sesión;

un parámetro de seguridad;

una clave de encriptación pública;

IDs de todos los mezcladores, y

claves públicas que han sido generadas por todos los mezcladores.

22. El sistema de desencriptación anónimo de acuerdo con la reivindicación 2,3, 7 o 10, en el que la certificación que realiza un mezclador puede ser verificada por una tercera parte.

23. El sistema de desencriptación anónimo de acuerdo con la reivindicación 1, en el que el mencionado mezclador está adaptado para calcular una porción de datos que se usa en un proceso de conexión de órdenes antes de la entrada de una lista de datos encriptados y, cuando se ha recibido como entrada una lista de datos encriptados, realizar el proceso de conexión de órdenes usando los datos que han sido calculados de antemano.

24. El sistema de desencriptación anónimo de acuerdo con la reivindicación 3, en el que el mencionado mezclador está adaptado para calcular una porción de datos para certificar que es correcto un proceso de conexión de órdenes antes de la entrada de datos encriptados y, cuando se ha recibido como entrada una lista de datos encriptados, generar los mencionados datos de certificación usando datos que han sido calculados de antemano.

25. Un sistema de desencriptación anónimo de acuerdo con una cualquiera de las reivindicaciones 1 a 24, que comprende un centro de gestión de voto que está adaptado para:

aceptar datos de votos encriptados que son emitidos por cada votante, datos de votos encriptados que se han encriptado sobre la base de la mencionada información pública;

seleccionar entre los datos de votos encriptados, datos de votos encriptados legitimados de votantes legitimados, y

transmitir los datos de votos encriptados seleccionados como lista de datos encriptados al mencionado centro de gestión de mezcla.

26. El sistema de desencriptación anónimo de acuerdo con la reivindicación 25, en el que cada uno de los mencionados votantes está adaptado para transmitir al mencionado centro de gestión de votos datos para certificar que se han encriptado correctamente datos de votos, y

el mencionado centro de gestión de votos está adaptado para verificar datos de certificación que se han transmitido desde cada votante.

27. Un sistema de desencriptación anónimo de acuerdo con una cualquiera de las reivindicaciones 1 a 24, que comprende un centro de gestión de licitación que está adaptado para:

aceptar valores de licitación encriptados que remite cada licitador en los que los valores de licitación se han encriptado sobre la base de la mencionada información pública; seleccionar, entre los valores de licitación encriptados recibidos, valores de licitación legitimados encriptados, y

transmitir los valores de licitación encriptados seleccionados como lista de datos encriptados al mencionado centro de gestión de mezcla.

28. El sistema de desencriptación anónimo de acuerdo con la reivindicación 27, en el que cada uno de los mencionados licitadores está adaptado para transmitir al mencionado centro de licitación datos para certificar que se han encriptado correctamente valores de licitación, y

el mencionado centro de gestión de licitación está adaptado para verificar datos de certificación que se han enviado desde cada votante.

29. Un sistema de desencriptación anónimo de acuerdo con una cualquiera de las reivindicaciones 1 a 24, que comprende un centro receptor que está adaptado para:

recibir respuestas de sondeo encriptadas que se han enviado por cada responsable de sondeo, repuestas de sondeo que han sido encriptadas sobre la base de la mencionada información pública;

seleccionar entre las respuestas de licitación encriptadas recibidas respuestas de sondeo encriptadas legitimadas de responsables de sondeo legitimados, y

transmitir las respuestas encriptadas seleccionadas como lista de datos encriptados al mencionado centro de gestión de mezcla.

30. El sistema de desencriptación anónimo de acuerdo con la reivindicación 29, en el que:

los mencionados responsables de sondeo están adaptados para transmitir al mencionado centro receptor datos de certificación para certificar que las respuestas de sondeo han sido encriptadas correctamente, y

el mencionado centro receptor está adaptado para verificar datos de certificación que han sido enviados por cada responsable de sondeo.

31. Un procedimiento de desencriptación anónimo de votación y licitación que toma como entrada una lista de datos encriptados que incluye una pluralidad de asuntos de datos encriptados que han sido encriptados por un procedimiento especificado y parámetros públicos especificados y que suministra resultados de desencriptar cada asunto de los datos encriptados en la lista de datos encriptados sin revelar la relación al orden en la lista, procedimiento de desencriptación anónimo que comprende etapas, en el que:

para el procesamiento de un mismo objeto, se añade un ID de sesión común a parámetros mutuamente relevantes, listas de datos encriptados y claves de desencriptación que poseen los mezcladores;

un centro de gestión de mezcla que, habiendo recibido como entrada una lista de datos encriptados con el correspondiente ID de sesión desde el exterior, transfiere la mencionada lista de datos con el correspondiente ID de sesión a un mezclador que es el primero en prioridad de procesamiento; cada uno de los mencionados mezcladores somete la lista de datos encriptados con el correspondiente ID de sesión que ha sido transferida desde el mencionado centro de gestión de mezcla a un proceso de conexión de órdenes usando parámetros públicos que corresponden al mencionado ID de sesión y a un proceso de desencriptación parcial usando una clave de desencriptación que corresponde al mencionado ID de sesión que posee ese mezclador y devuelve la lista de datos resultante con el correspondiente ID de sesión al mencionado centro de gestión de mezcla, y

cuando una lista de datos con el correspondiente ID de sesión vuelve desde un mezclador que no es el mezclador último en prioridad de procesamiento, el mencionado centro de gestión de mezcla transfiere la mencionada lista de datos con el correspondiente ID de sesión que ha sido devuelta como lista de datos encriptados a un mezclador que es el siguiente en prioridad de procesamiento después del mezclador que devolvió la mencionada lista de datos con el correspondiente ID de sesión; y cuando una lista de datos con el correspondiente ID de sesión vuelve desde el mezclador último en prioridad de procesamiento, suministra la mencionada lista de datos con el correspondiente ID de sesión como lista resultado de desencriptación.

32. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 31, en el que los mencionados mezcladores comunican al mencionado centro de gestión de mezcla certificación de que el proceso de conexión de órdenes se ha realizado correctamente y que el proceso de desencriptación parcial se ha realizado correctamente.

33. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 31, en el que los mencionados mezcladores adjuntan certificación de que el proceso de conexión de órdenes se ha realizado correctamente y que el proceso de desencriptación parcial se ha realizado correctamente a las mencionadas listas de datos que resultan del procesamiento y dan cuenta al mencionado centro de gestión de la mezcla.

34. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 32 o 33, en el que el mencionado centro de gestión de mezcla verifica que la certificación realizada por un mezclador es correcta.

35. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 32 o 33, en el que el mencionado centro de gestión de mezcla, después de verificar que la certificación realizada por un mezclador es correcta, transmite una lista de datos que ha sido devuelta por el mencionado mezclador como lista de datos encriptados a un mezclador que es el siguiente en prioridad de procesamiento.

36. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 32, 33, 34 o 35, en el que el mencionado centro de gestión de mezcla adjunta certificación de que todos los mezcladores han contribuido a una lista resultado de desencriptación y suministra la mencionada lista de desencriptación como resultado.

37. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 31, en el que el mencionado centro de gestión de mezcla y los mencionados mezcladores realizan autentificación del emisor durante la comunicación.

38. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 31, en el que el mencionado centro de gestión de mezcla y los mencionados mezcladores confieren signaturas digitales de una fuente de transmisión a datos de comunicación.

39. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 31, en el que:

el mencionado centro de gestión de mezcla, cuando se recibe como entrada un parámetro de seguridad, genera parámetros públicos comunes basados en los mencionados parámetros de seguridad y notifica a todos los mezcladores los mencionados parámetros públicos comunes producidos;

todos los mencionados mezcladores generan claves públicas y claves de desencriptación basadas en el parámetro público común que ha notificado el mencionado centro de gestión de mezcla y devuelven las mencionadas claves públicas generadas al mencionado centro de gestión de mezcla, y

el mencionado centro de gestión de mezcla, cuando vuelven las claves públicas de todos los mencionados mezcladores, genera claves de encriptación basadas en las claves públicas de todos los mezcladores mencionados y publica parámetros públicos que incluyen las mencionadas claves de encriptación públicas generadas y el mencionado parámetro público común.

40. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 39, en el que los mencionados mezcladores, cuando vuelven claves públicas al mencionado centro de gestión de mezcla, añaden certificación de que las mencionadas claves públicas se han generado correctamente y luego devuelven las mencionadas claves públicas al mencionado centro de gestión de mezcla.

41. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 40, en el que el mencionado centro de gestión de mezcla verifica que la certificación añadida a claves públicas es correcta.

42. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 40 o 41, en el que el mencionado centro de gestión de mezcla publica claves públicas y certificación que se ha añadido a las claves públicas junto con información pública.

43. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 39, en el que el mencionado centro de gestión de mezcla y los mencionados mezcladores realizan autentificación del emisor durante la comunicación.

44. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 39, en el que el mencionado centro de gestión de mezcla y los mencionados mezcladores añaden una signatura digital de una fuente de transmisión a datos de comunicación.

45. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 31, en el que:

cuando se transfiere una lista de datos encriptados a un mezclador, el mencionado centro de gestión de mezcla añade, además del mencionado ID de sesión, un ID de sesión de centro de gestión de mezcla que está conferido a ese centro de gestión de mezcla, un ID de mezclador que está conferido al mezclador que es un destino de transferencia, y una signatura de ese centro de gestión de mezcla.

46. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 31, en el que:

cuando vuelven listas de datos al mencionado centro de gestión de mezcla, los mencionados mezcladores añaden, además del mencionado ID de sesión, un ID de centro de gestión de mezcla que está conferido a ese mezclador, un ID de centro de gestión de mezcla que está conferido al mencionado centro de gestión de mezcla y una signatura de ese mezclador.

47. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 46, en el que:

el mencionado mezclador, cuando vuelve una lista de datos al mencionado centro de gestión de mezcla, añade también datos de certificación para certificar que el proceso de conexión de órdenes se ha realizado correctamente y datos de certificación para certificar que el proceso de desencriptación parcial se ha realizado correctamente.

48. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 36, en el que la información que suministra el mencionado centro de gestión de mezcladura comprende:

un ID de centro de gestión de mezcla que está conferido a ese centro de gestión de mezcla,

una lista de datos encriptados que se ha recibido como entrada desde el exterior,

resultados de desencriptación para la mencionada lista de datos encriptados,

un ID de sesión que está conferido a la mencionada lista de datos encriptados,

todos los datos que se han devuelto desde todos los mezcladores, y

una signatura del centro de gestión de mezcla.

49. Un procedimiento de desencriptación anónimo de acuerdo con la reivindicación 39,

en el que el mencionado centro de gestión de mezcla, cuando se notifica información pública común y un parámetro de seguridad a los mezcladores, añade: un ID de centro de gestión de mezcla que está conferido a ese centro de gestión de mezcla;

IDs de todos los mezcladores que realizan desencriptación;

un ID de sesión, y

una signatura del centro de gestión de mezcla.

50. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 39 o 40, en el que un mezclador añade a la información que es devuelta al centro de gestión de mezcla:

un ID de centro de gestión de mezcla que está conferido a ese centro de gestión de mezcla;

un ID de sesión;

un ID de ese mezclador, y

una signatura para ese mezclador.

51. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 39, en el que la información pública que publica ese centro de gestión de mezcla comprende:

un ID de centro de gestión de mezcla que está conferido a ese centro de gestión de mezcla,

un ID de sesión;

un parámetro de seguridad;

una clave de encriptación pública;

IDs de todos los mezcladores y claves públicas que se han generado por todos los mezcladores.

52. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 32, 33, 37 o 40, en el que la certificación realizada por un mezclador puede ser verificada por un tercero.

53. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 31, en el que el mencionado mezclador calcula una porción de datos que se usan en un proceso de conexión de órdenes antes de la entrada de una lista de datos encriptados y, cuando se ha recibido como entrada la lista de datos encriptados, realiza el proceso de conexión de órdenes usando los datos que se han calculado de antemano.

54. El procedimiento de desencriptación anónimo de acuerdo con la reivindicación 33, en el que el mencionado mezclador calcula una porción de datos que se usan al generar datos de certificación para certificar que un proceso de conexión de órdenes es correcto antes de la entrada de una lista de datos encriptados y, cuando se ha recibido como entrada la lista de datos encriptados, genera la mencionada lista de certificación usando los datos que se han calculado de antemano.

55. El procedimiento de desencriptación anónimo de acuerdo con una cualquiera de las reivindicaciones 31 a 54, en el que un centro de gestión de votos:

acepta datos de votos encriptados enviados desde cada votante, siendo los mencionados votos encriptados datos de votos que se han encriptado sobre la base de la mencionada información pública;

selecciona datos de votos encriptados legitimados de votantes legitimados entre los datos de votos encriptados, y

transmite los datos de votos encriptados seleccionados como lista de datos encriptados al mencionado centro de gestión de mezcla.

56. El sistema de desencriptación anónimo de acuerdo con la reivindicación 55, en el que:

cada uno de los mencionados votantes transmite al mencionado centro de gestión de votos datos de certificación para certificar que los datos de votos han sido encriptados correctamente, y

el mencionado centro de gestión de votos verifica datos de certificación que se han transmitido de cada votante.

57. El procedimiento de desencriptación anónimo de acuerdo con una cualquiera de las reivindicaciones 31 a 54, en el que un centro de gestión de licitación:

acepta valores de licitación encriptados enviados desde cada licitador y en los que los valores de licitación han sido encriptados sobre la base de la mencionada información pública;

selecciona entre estos valores de licitación encriptados recibidos valores de licitación encriptados legitimados de licitadores legitimados, y

transmite estos valores de licitación encriptados seleccionados como lista de datos encriptados al mencionado centro de gestión de mezcla.

58. El sistema de desencriptación anónimo de acuerdo con la reivindicación 57, en el que:

cada uno de los mencionados licitadores transmite al mencionado centro de gestión de licitación datos de certificación para certificar que los valores de licitación han sido encriptados correctamente, y

el mencionado centro de gestión de la licitación verifica datos de certificación que se han transmitido desde cada licitador.

59. El procedimiento de desencriptación anónimo de acuerdo con una cualquiera de las reivindicaciones 31 a 54, en el que un centro de recepción:

recibe respuestas de sondeo que se envían desde cada responsable de sondeo y en las que las respuestas de sondeo se han encriptado sobre la base de la mencionada información pública;

selecciona entre las respuestas del sondeo encriptadas recibidas respuestas de sondeo de responsables del sondeo legitimados, y

transmite las respuestas del sondeo encriptadas como lista de datos encriptados al mencionado centro de gestión de mezcla.

60. Un procedimiento de desencriptación anónimo de acuerdo con la reivindicación 59, en el que:

los mencionados responsables del sondeo transmiten al mencionado centro de recepción datos de certificación para certificar que las respuestas del sondeo han sido encriptadas correctamente, y

el mencionado centro de recepción verifica que los datos de certificación se han transmitido desde cada responsable de sondeo.

61. Un programa de ordenador que, cuando actúa en un ordenador, causa que el ordenador realice todas las etapas de procedimiento de la reivindicación 31.

62. Un medio de registro para almacenar el programa de la reivindicación 61.

Fig. 1

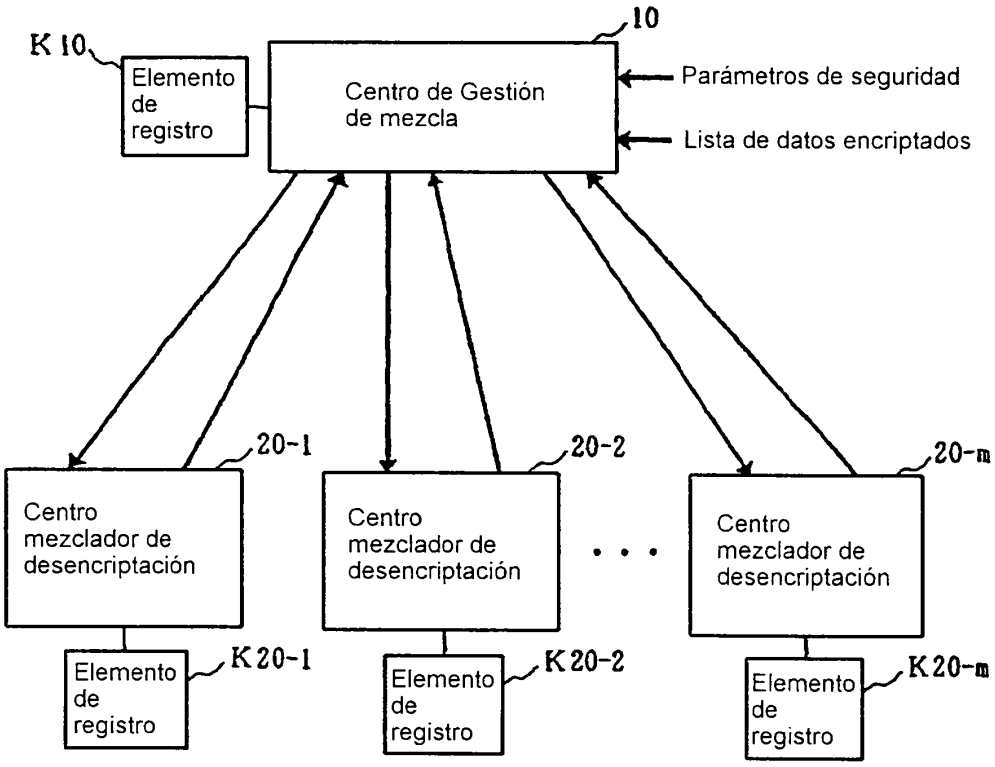

10
K 10
Elemento de registro
Centro de Gestión de mezcla
Parámetros de seguridad
Lista de datos encriptados
20-1
20-2
20-m
Centro mezclador de desencriptación
Centro mezclador de desencriptación
Centro mezclador de desencriptación
Elemento de registro
K20-1
Elemento de registro
K20-2
Elemento de registro
K20-m

FIG. 2

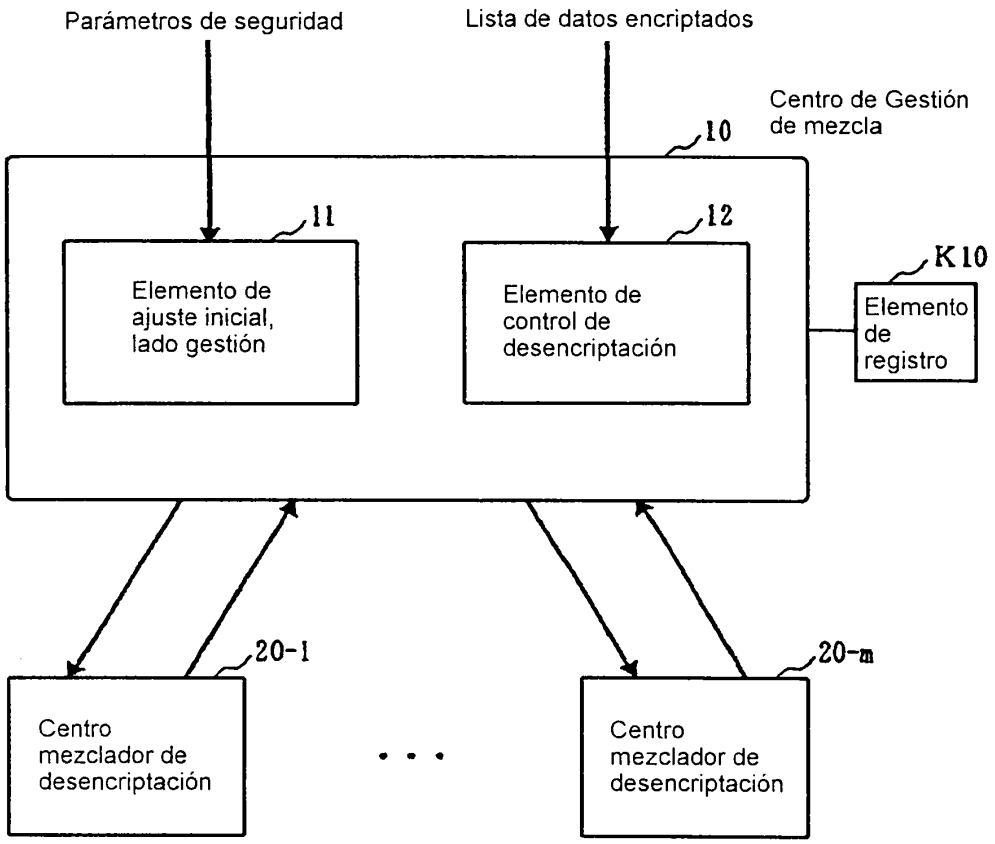

Parámetros de seguridad
Lista de datos encriptados
Centro de Gestión de mezcla
10
11
12
K10
Elemento de ajuste inicial, lado gestión
Elemento de control de desencriptación
Elemento de registro
20-1
20-m
Centro mezclador de desencriptación
Centro mezclador de desencriptación

Fig. 3

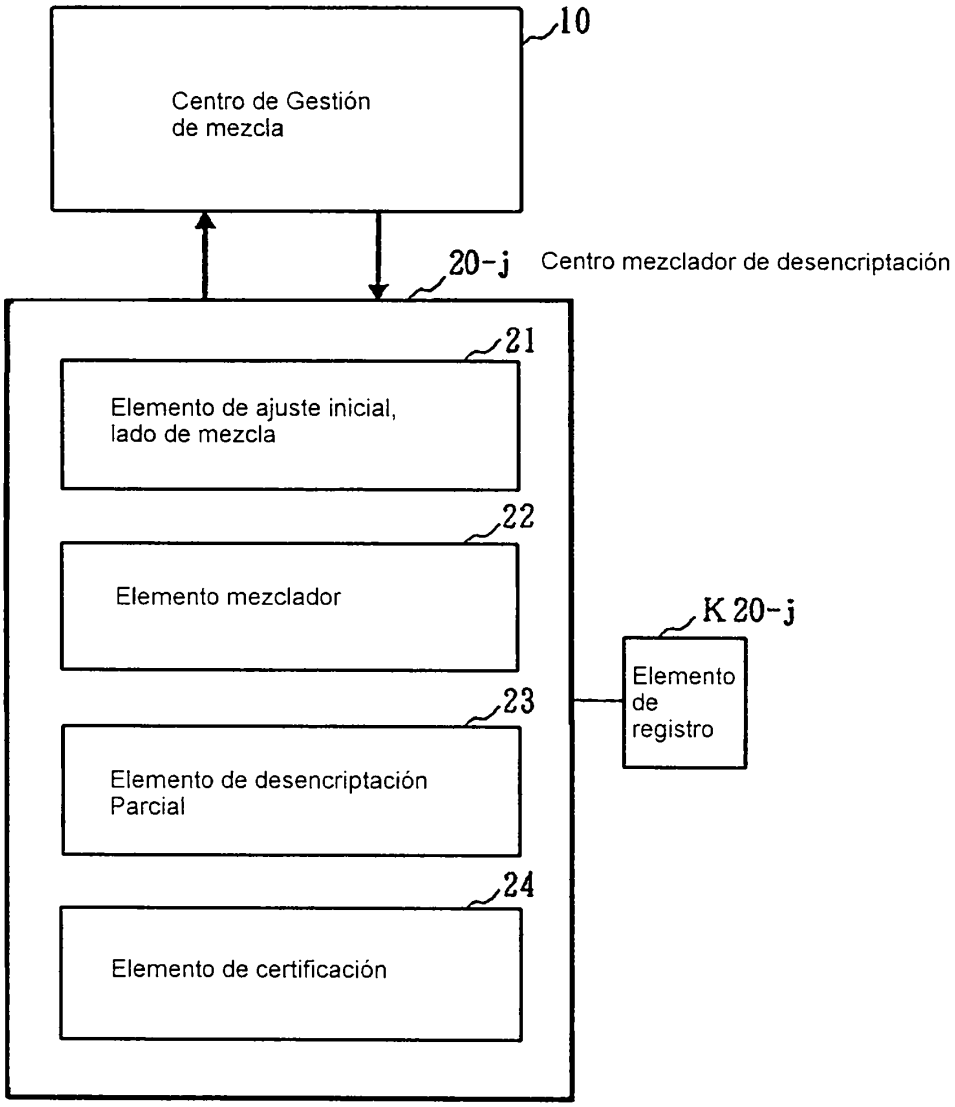

10
Centro de Gestión de mezcla
20-j
Centro mezclador de desencriptación
21
Elemento de ajuste inicial, lado de mezcla
22
Elemento mezclador
23
Elemento de desencriptación Parcial
24
Elemento de certificación
K 20-j
Elemento de registro

Fig. 4

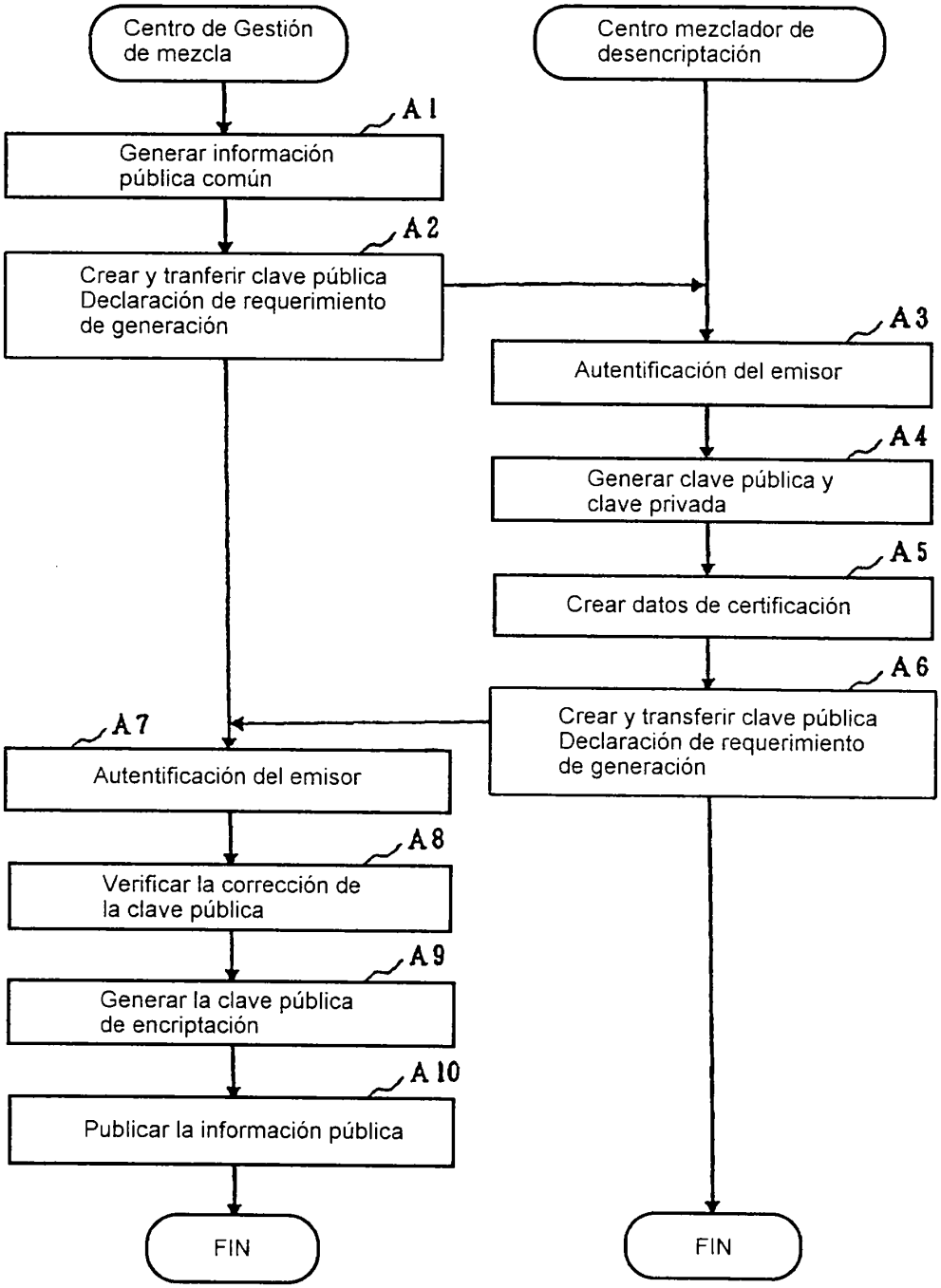

Centro de Gestión de mezcla
Centro mezclador de desencriptación
A1
Generar información pública común
A2
Crear y tranferir clave pública Declaración de requerimiento de generación
A3
Autentificación del emisor
A4
Generar clave pública y clave privada
A5
Crear datos de certificación
A6
Crear y transferir clave pública Declaración de requerimiento de generación
A7
Autentificación del emisor
A8
Verificar la corrección de la clave pública
A9
Generar la clave pública de encriptación
A10
Publicar la información pública
FIN
FIN

Fig. 5

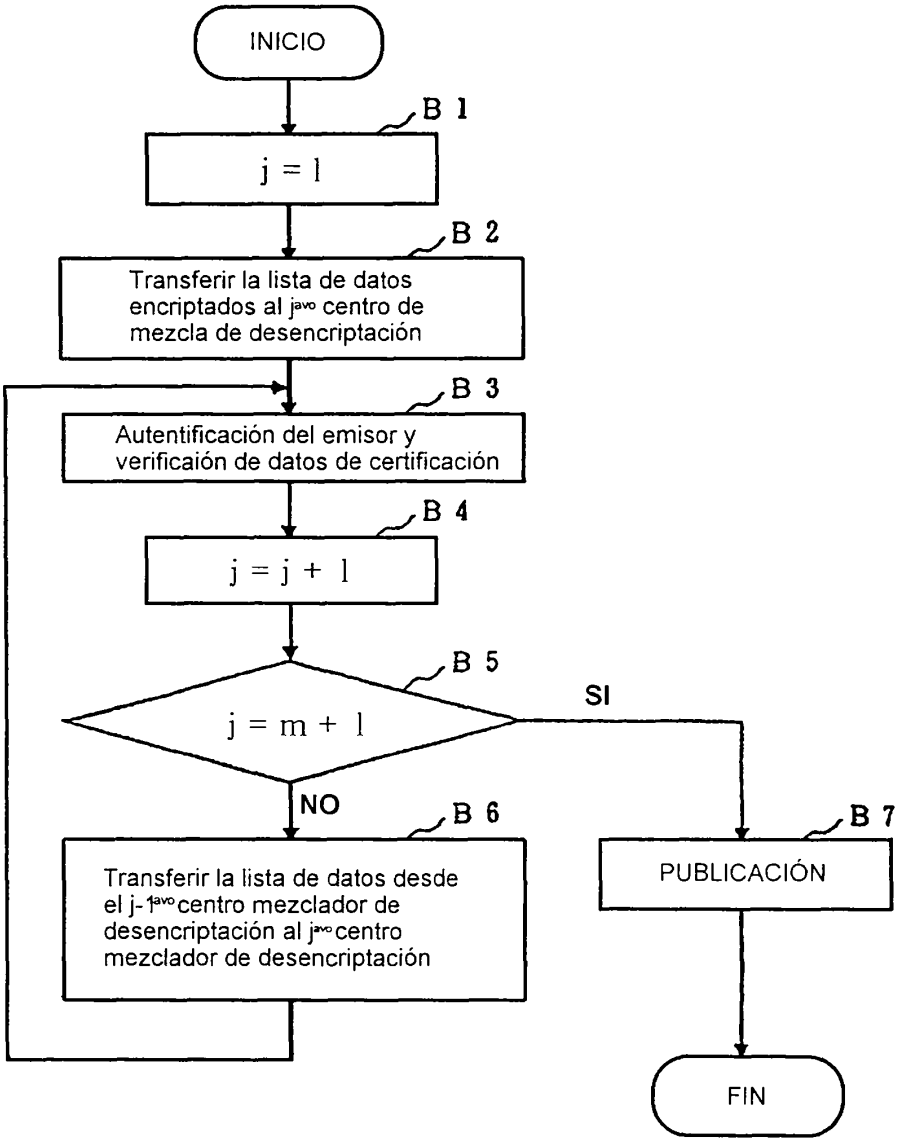

INICIO
B 1
j = 1
B 2
Transferir la lista de datos encriptados al j-avo centro de mezcla de desencriptación
B 3
Autentificación del emisor y verificaión de datos de certificación
B 4
j = j + 1
B 5
j = m + 1
SI
NO
B 6
Transferir la lista de datos desde el j-1-avo centro mezclador de desencriptación al j-avo centro mezclador de desencriptación
B 7
PUBLICACIÓN
FIN

Fig.6

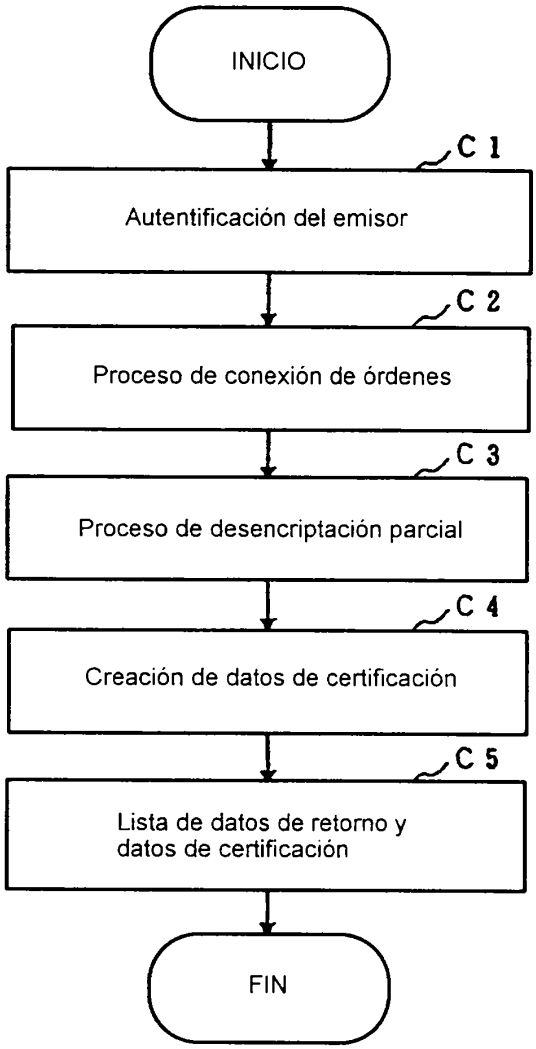

INICIO
C 1
Autentificación del emisor
C 2
Proceso de conexión de órdenes
C 3
Proceso de desencriptación parcial
C 4
Creación de datos de certificación
C 5
Lista de datos de retorno y datos de certificación
FIN

Fig. 7

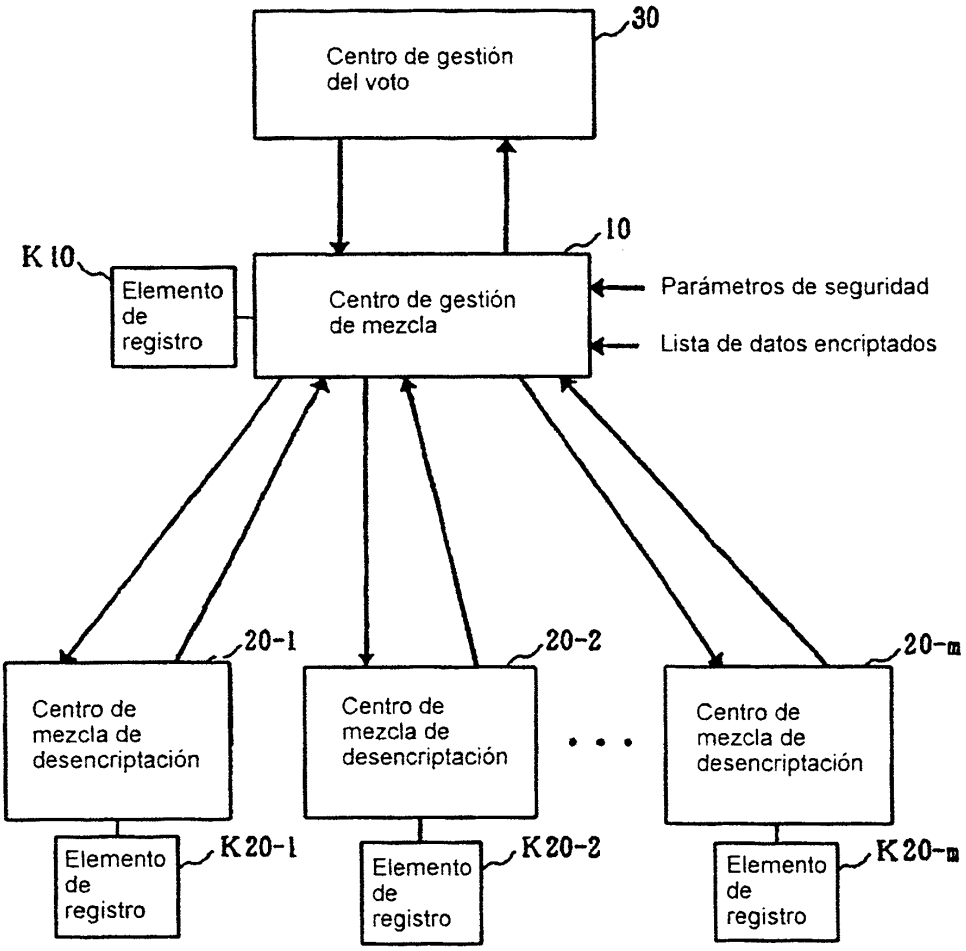

Centro de gestión del voto
30
10
K10
Elemento de registro
Centro de gestión de mezcla
Parámetros de seguridad
Lista de datos encriptados
20-1
20-2
20-m
Centro de mezcla de desencriptación
Centro de mezcla de desencriptación
Centro de mezcla de desencriptación
Elemento de registro
K20-1
Elemento de registro
K20-2
Elemento de registro
K20-m

Fig. 8

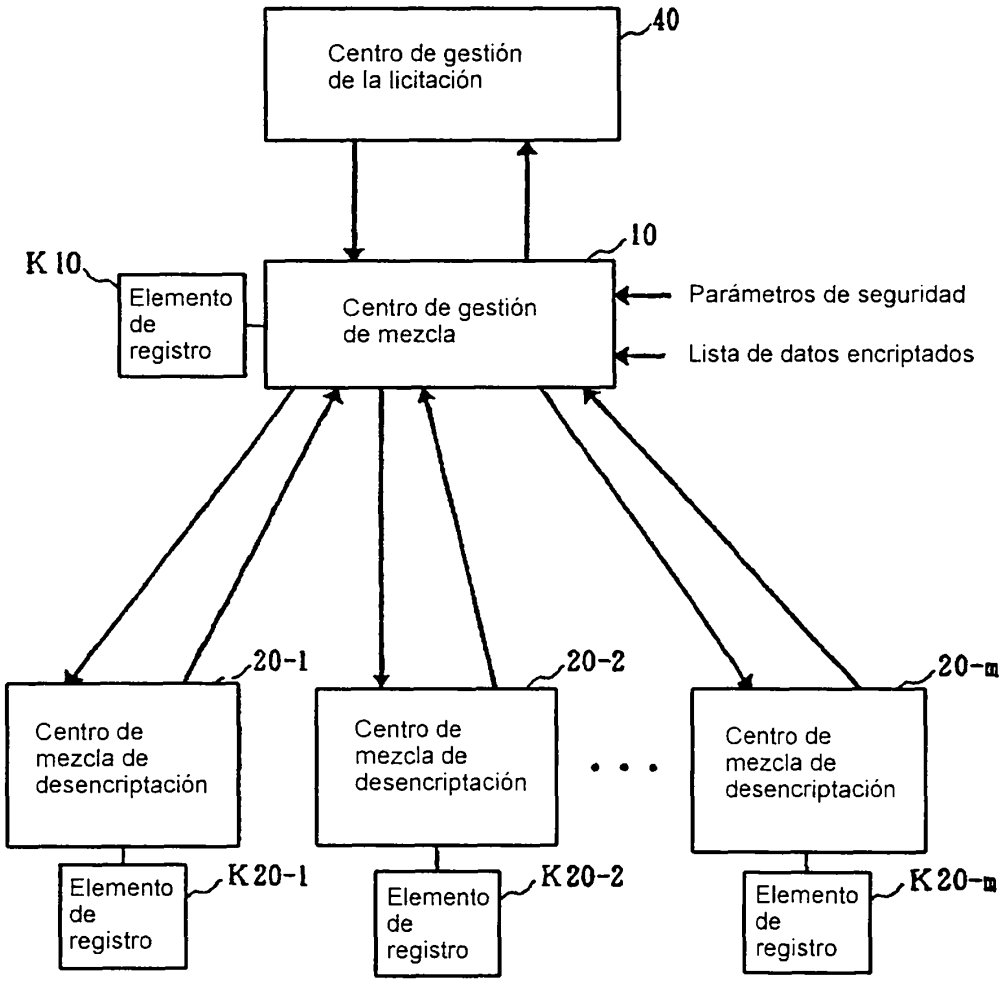

Centro de gestión de la licitación
40
10
K 10
Elemento de registro
Centro de gestión de mezcla
Parámetros de seguridad
Lista de datos encriptados
20-1
20-2
20-m
Centro de mezcla de desencriptación
Centro de mezcla de desencriptación
Centro de mezcla de desencriptación
K 20-1
K 20-2
K 20-m
Elemento de registro
Elemento de registro
Elemento de registro

Fig. 9

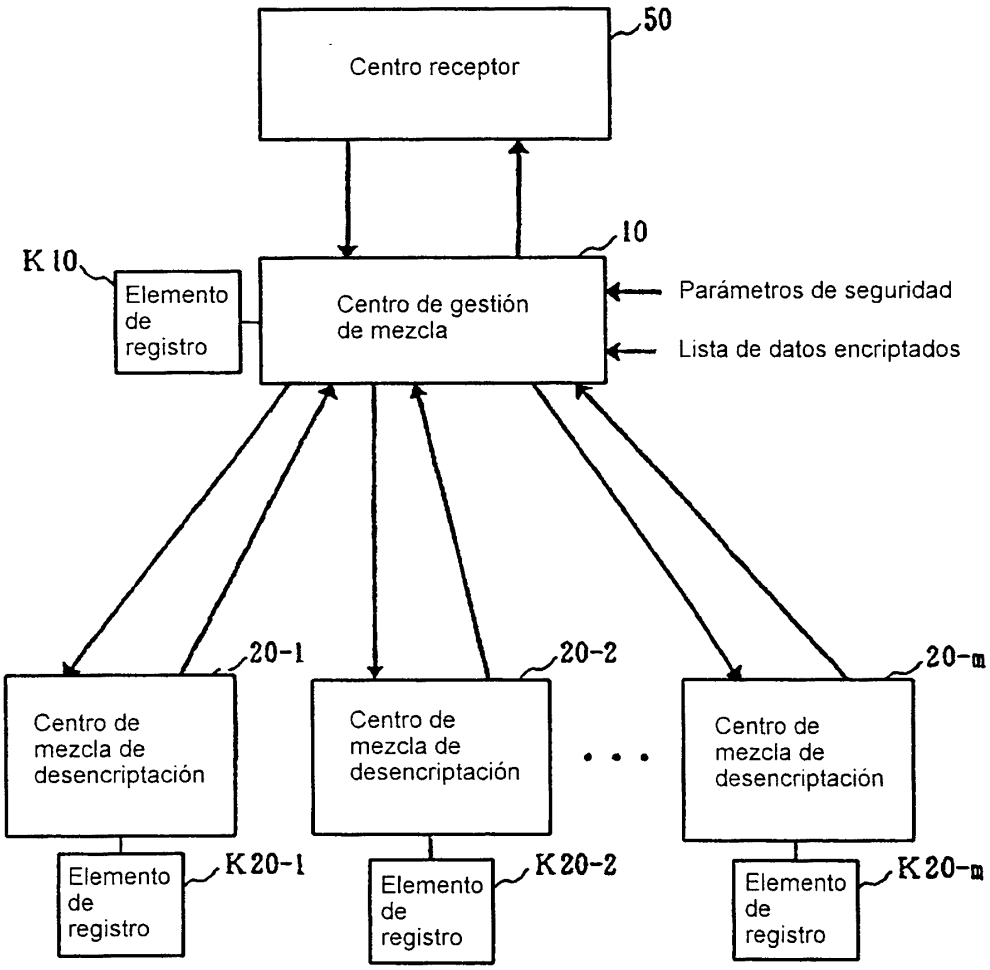
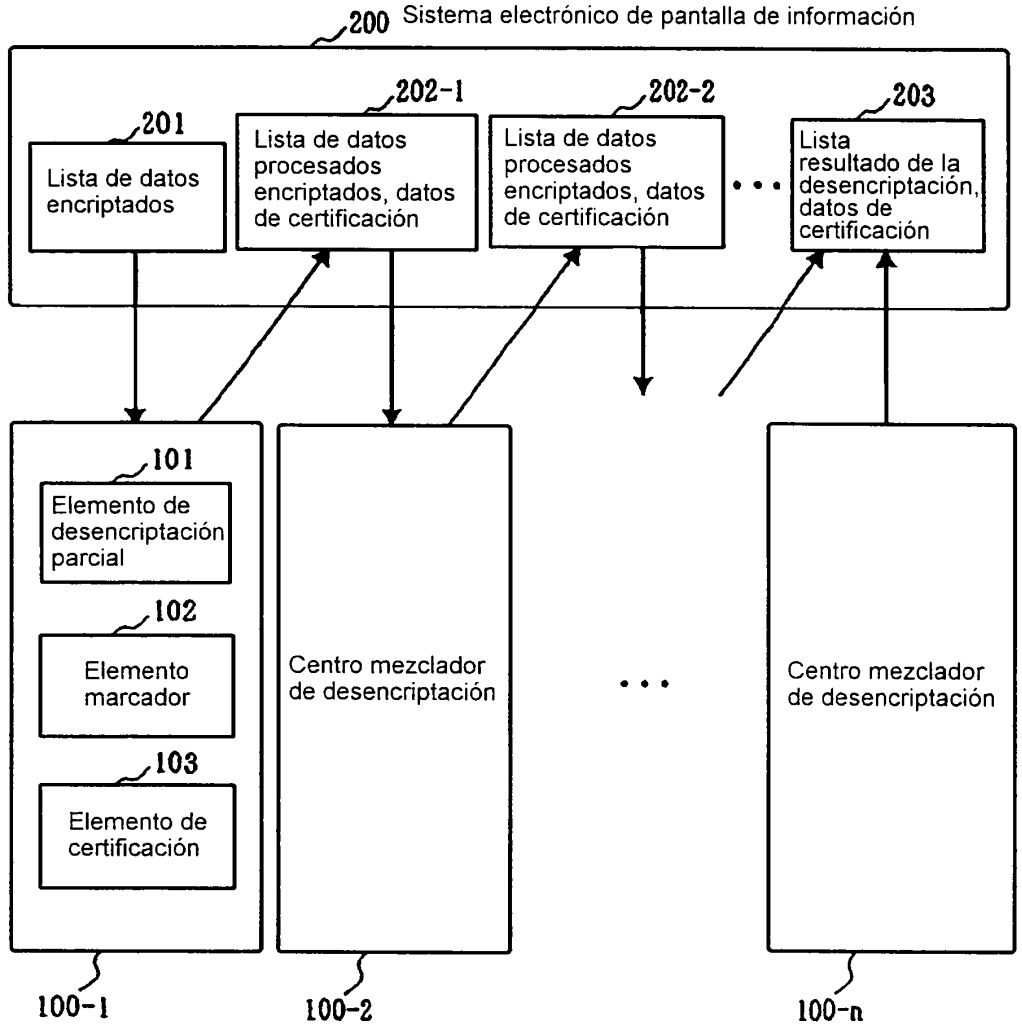

Centro receptor
50
10
K10
Elemento de registro
Centro de gestión de mezcla
Parámetros de seguridad
Lista de datos encriptados
20-1
20-2
20-m
Centro de mezcla de desencriptación
Centro de mezcla de desencriptación
Centro de mezcla de desencriptación
Elemento de registro
K20-1
Elemento de registro
K20-2
Elemento de registro
K20-m

Fig. 10



Centro mezclador de desencriptación