(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 360 044**

(51) Int. Cl.:
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03748214 .8**
(96) Fecha de presentación : **16.07.2003**
(97) Número de publicación de la solicitud: **1523824**
(97) Fecha de publicación de la solicitud: **20.04.2005**

(54) Título: **Método de firma de lista y aplicación al voto electrónico.**

(30) Prioridad: **19.07.2002 FR 02 09218**

(45) Fecha de publicación de la mención BOPI:
31.05.2011

(45) Fecha de la publicación del folleto de la patente:
31.05.2011

(73) Titular/es: **FRANCE TELECOM**
6 place d'Alleray
75015 Paris, FR

(72) Inventor/es: **Canard, Sébastien;**
Girault, Marc y
Traore, Jacques

(74) Agente: **Lehmann Novo, María Isabel**

DESCRIPCIÓN

Método de firma de lista y aplicación al voto electrónico

La presente invención se refiere al campo general de la seguridad de los servicios accesible por una red de transmisión de datos digitales y, más concretamente, el campo de la firma electrónica.

Se aplica, en particular, pero no exclusivamente al voto electrónico o también a la petición electrónica.

La firma electrónica de un mensaje pone en práctica un mecanismo pertinente de la criptografía denominada de clave pública: el signatario que posee una clave secreta o privada y una clave pública asociada, puede proporcionar una firma de mensaje con la ayuda de la clave secreta. Para verificar la firma, basta disponer de la clave pública.

En algunas aplicaciones como el voto electrónico, el signatario debe poder quedar anónimo. A este efecto, se ha puesto a punto lo que se denomina la firma electrónica anónima, que permite, con la ayuda de una clave pública, determinar si el signatario de un mensaje posee algunos derechos (derecho de firmar el mensaje, derecho de poseer la clave secreta que se haya utilizado para firmar el mensaje, etc.), preservando el anonimato del signatario. Además, en las aplicaciones de voto o de petición electrónica, cada persona autorizada sólo debe poder firmar una sola vez.

Entre las firmas anónimas, existe, asimismo, lo que se denomina firma ciega, que permite a una persona obtener la firma de un mensaje de otra entidad, sin que esta última tenga que conocer el contenido del mensaje y pueda establecer, más tarde, el vínculo entre la firma y la identidad del signatario. Esta solución de firma ciega necesita, por lo tanto, la intervención de una entidad intermediaria que proporcione las firmas. En las aplicaciones como el voto o la petición electrónica, esta solución hace intervenir una autoridad habilitada que firme el voto de cada elector o la petición para cada peticionario.

Se ha dado a conocer, además, el concepto de firma de grupo que permite a cada miembro de un grupo proporcionar una firma tal que un verificador, que posea una clave pública adecuada, pueda verificar que la firma fue emitida por un miembro del grupo sin poder determinar la identidad del signatario.

Este concepto se describe, por ejemplo, en el documento:

[1] "A Practical and Provably Secure Coalition-Resistant Group Signature Scheme" de G. Ateniese, J Camenisch, M. Joye y G. Tsudik, en M. Bellare, Editor, Advance in Cryptology — CRYPTO 2000, vol. 1880 de LNCS, páginas 255- 270, Springer-Verlag 2000.

Sin embargo, en este concepto, una autoridad de confianza puede levantar, en cualquier momento, este anonimato y determinar la identidad de una persona del grupo que haya emitido una firma. Además, este tipo de firma se denomina "no fiable", es decir que no permite determinar si dos firmas han sido, o no, emitidas por la misma persona sin levantar el anonimato de la firma. Las firmas de grupo se utilizan en numerosas aplicaciones, tales como la venta electrónica en las subastas, la moneda electrónica o también el voto electrónico. La firma de grupo no conviene perfectamente a esta última aplicación, puesto que autoriza a una autoridad de confianza a acceder a la identidad de un signatario, y no permite relacionar dos firmas emitidas por una misma persona sin determinar la identidad del signatario. Además, el documento [1] no prevé procesos de revocación de un miembro del grupo.

Para subsanar este último inconveniente, el documento [2] "Efficient Revocation of Anonymous Group membership Certificates and Anonymous Credentials" de J. Camenisch y A. Lysyanskaya, publicado por Cryptologie ePrint Archive IACR 2002, prevé añadir a este concepto un proceso de revocación (este documento será también publicado por M. Jung, Editor CRYPTO 2002, Springer-Verlag 2002). Sin embargo, esta solución no aporta solución alguna a los problemas de la preservación del anonimato del signatario y de la "fiabilidad" de dos firmas.

En una aplicación de voto electrónico, es además necesario para garantizar una seguridad de la máxima aproximación del voto tradicional, asegurar las propiedades siguientes.

Nadie debe ser capaz de conocer, ni siquiera parcialmente los resultados del escrutinio antes de su cierre. Cualquier persona debe poder convencerse de la validez del resultado final del escrutinio. Por último, una autoridad habilitada debe ser capaz de retirar o de revocar el derecho de voto de una persona.

Cuando se trata del voto fuera de línea, es decir de la utilización de una máquina para votar electrónica instalada en una oficina de voto, o del voto en línea, es decir a distancia, a través de la red Internet por ejemplo, los sistemas propuestos actualmente, que utilizan una firma de grupo tal como se describe en el documento [1] y completada en el documento [2], no cumplen estas condiciones, sino en parte la revocación del derecho de firma.

Por otro lado, la aplicación del concepto de firma ciega al voto electrónico es una solución cuya puesta en práctica es onerosa, porque obliga al elector a conectarse varias veces a cada elección. Además, si el escrutinio se transmite mal, no se puede determinar quién es el responsable: un elector o el organizador del escrutinio.

Se ha dado a conocer, además, en particular en el documento [3] "Untraceable Electronic Mail Return Addresses and Digital Pseudonym" de D. Chaum, ACM 1981, el concepto de redes mezcladoras, siendo cada red mezcladora una función que proporcione una lista de números descifrados a partir de una lista de números cifrados, ocultando la correspondencia entre los números cifrados y los números descifrados. Aplicada al voto electrónico, esta

técnica presenta el importante inconveniente de no permitir verificar la validez de un voto sin comprometer el secreto de este último.

En el documento [4] "A Secure and Optimal Efficient Multi-Authority Election Scheme", de Cramer, Gennaro y Schoenmakers, Eurocrypt'97, LNCS — Springer-Verlag, se describe lo que se denomina el cifrado homomorfo que permite efectuar cálculos basados sobre números cifrados. Las soluciones basadas en este método no son, sin embargo, aplicables a los escrutinios que impliquen a un gran número de electores.

La presente invención tiene como objetivo suprimir este inconveniente. Este objetivo se alcanza por la previsión de un método de firma de lista, que comprende al menos:

— una fase de organización que consiste, para una autoridad de confianza, definir parámetros de puesta en práctica de una firma electrónica anónima, con una clave privada y una clave pública correspondiente,

— una fase de registro de personas en una lista de miembros autorizados para generar una firma electrónica propia a los miembros de la lista, en el transcurso de cuya fase cada persona a registrar calcula una clave privada con la ayuda de parámetros proporcionados por la autoridad de confianza y de parámetros elegidos, de forma aleatoria, por la persona a registrar, y la autoridad de confianza entrega, a cada persona a registrar, un certificado de miembro de la lista,

— una fase de firma, en cuyo transcurso, un miembro de la lista genera y emite una firma propia a los miembros de la lista, construyendo esta firma de modo que contenga una prueba de que el miembro de la lista, que ha emitido la firma, conoce un certificado de miembro de la lista, y

— una fase de verificación de la firma emitida que comprende etapas de aplicación de un algoritmo predefinido para poner en evidencia la prueba de que la firma fue emitida por una persona en posesión de un certificado de miembro de la lista.

Según la invención, este método comprende, además:

— una fase de definición de una secuencia que consiste, para la autoridad de confianza, en generar un número de secuencia a utilizar en la fase de firma, una firma generada durante la fase de firma que comprende un elemento de firma que es común a todas las firmas emitidas por un mismo miembro de la lista con un mismo número de secuencia y que contiene una prueba de que el número de secuencia fue utilizado para generar la firma, comprendiendo la fase de verificación, además, una etapa de verificación de la prueba de que el número de secuencia fue utilizado para generar la firma;

— una fase de revocación de un miembro de la lista para retirar un miembro de la lista, en cuyo transcurso, la autoridad de confianza retira de la lista el miembro a retirar y actualiza los parámetros de puesta en práctica de la firma electrónica anónima, para tener en cuenta la supresión del miembro de la lista y

— una fase de actualización de los certificados de los miembros de la lista para tener en cuenta las modificaciones de la composición de la lista.

Según una forma de realización de la invención, la fase de organización comprende la definición de un parámetro común, que depende de la composición de la lista, comprendiendo la fase de registro de una persona en la lista la definición de un parámetro propio de la persona a registrar, que se calcula en función del parámetro que depende de la composición de la lista y que está integrado en el certificado remitido a la persona, comprendiendo la fase de registro una etapa de actualización del parámetro común, que depende de la composición de la lista, comprendiendo la fase de revocación de un miembro de la lista una etapa de modificación del parámetro común, que depende de la composición de la lista, para tener en cuenta la supresión del miembro de la lista y presentando la fase de actualización de los certificados de los miembros de la lista una etapa de actualización del parámetro propio de cada miembro de la lista para tener en cuenta las modificaciones de la composición de la lista.

Según una forma de realización de la invención, una firma propia para un miembro de la lista y que posea el certificado $[A_i,e_i]$ comprende parámetros T_1, T_2, T_3 tales como:

$$T_1 = A_i b^{\omega} \text{ (mod.n)},$$

$$T_2 = g^{\omega} \text{ (mod.n)},$$

$$T_3 = g e_i h^{\omega} \text{ (mod.n)},$$

siendo ω un número elegido, de forma aleatoria, en el momento de la fase de firma, y siendo *b, g, h* y *n* parámetros generales de puesta en práctica de la firma de grupo, tales que los parámetros *b, g* y *h* no se puedan deducir los unos de los otros por funciones de elevación de potencia entera módulo n, de modo que el número A_i y, por lo tanto, la identidad del miembro de la lista que posea el certificado $[A_i\ e_i]$, no se pueda deducir de una firma emitida por el miembro.

Preferentemente, el número de una secuencia utilizado para generar una firma de lista se calcula en función de una fecha de inicio de secuencia.

En una forma de realización preferida, la función de cálculo del número de una secuencia es de la forma:

$F(d)=(H(d))^2$ (mod.n)

en donde *H* es una función de resumen criptográfico resistente a las colisiones, *d* es la fecha de inicio de la secuencia y *n* es un parámetro general de puesta en práctica de la firma de grupo.

Según una forma de realización de la invención, una firma emitida por un miembro de la lista contiene un parámetro que se calcula en función del número de secuencia y de la clave privada del miembro signatario.

Según una forma de realización de la invención, el parámetro T_4 de una firma emitida por un miembro de la lista, y que depende del número de secuencia m y de la clave privada x_i del miembro signatario, se obtiene por la fórmula siguiente:

$T_4 = M^{xi}$ (mod. n)

siendo *n* un parámetro general de puesta en práctica de la firma de grupo, y la firma que comprende la prueba de que el parámetro T_4 fue calculado con la clave privada x_i del miembro de la lista que ha emitido la firma.

La invención se refiere, además, a un método de voto electrónico que comprende una fase de organización de las elecciones, en cuyo transcurso una autoridad organizadora procede a la generación de parámetros necesarios para un escrutinio y atribuye claves a escrutadores, que les permiten descifrar y verificar las papeletas de voto, una fase de atribución de un derecho de firma a cada uno de los electores, una fase de voto en cuyo transcurso los electores firman una papeleta de voto y una fase de recuento, en cuyo transcurso los escrutadores verifican las papeletas de voto y calculan el resultado del escrutinio en función del contenido de las papeletas de voto descifradas y válidas.

Según la invención, este método pone en práctica un método de firma de lista tal como se definió anteriormente, para firmar las papeletas de voto, estando cada elector registrado como miembro de una lista y siendo un número de secuencia generado para el escrutinio, para detectar si un mismo elector ha emitido, o no, varias papeletas de voto para el escrutinio.

Según una forma de realización de la invención, la fase de organización comprende la entrega a cada escrutador de una clave pública y de una clave privada, siendo las papeletas de voto cifradas con la ayuda de una clave pública obtenida por el producto de las claves públicas respectivas de todos los escrutadores, y siendo obtenida la clave privada de descifrado correspondiente calculando la suma de claves privadas respectivas de todos los escrutadores.

Preferentemente, el cifrado de las papeletas de voto se realiza con la ayuda de un algoritmo de cifrado probabilista.

Según una forma de realización de la invención, las papeletas de voto emitidas por los electores se guardan en una base de datos pública, siendo el resultado de la verificación y del recuento de cada papeleta de voto almacenado en la base de datos en asociación con la papeleta de voto, y la clave privada de descifrado de las papeletas de voto que se han publicado.

La invención se refiere, además, a un calculador para la puesta en práctica de una firma de lista, que comprende medios para:

- generar parámetros de puesta en práctica de una firma electrónica anónima propia para los miembros de una lista, comprendiendo los parámetros una clave privada y una clave pública correspondiente y

- transmitir a cada persona a registrar en la lista, parámetros a utilizar por la persona a registrar para calcular una clave privada, y un

— certificado de miembro de la lista.

Según la invención, el calculador comprende, además, medios para:

— generar un número de secuencia a utilizar por los miembros de la lista para emitir una firma anónima propia para los miembros de la lista, una firma anónima emitida por un miembro de la lista que comprende un elemento de firma que es común a todas las firmas emitidas por el mismo miembro de la lista, con un mismo número de secuencia, y que contenga una prueba de que el número de secuencia fue utilizado para generar la firma;

- retirar de la lista un miembro a revocar de la lista, y actualizar los parámetros de puesta en práctica de la firma electrónica anónima propia para los miembros de la lista, para tener en cuenta la retirada del miembro de la lista y actualizar los certificados de los miembros de la lista a cada modificación de la composición de la lista.

La invención se refiere, además, a un calculador para la puesta en práctica de un método de voto electrónica, que comprende medios para:

— generar, en el curso de una fase de organización de un escrutinio, parámetros de puesta en práctica de una firma electrónica anónima propia para los miembros de una lista de electores, conteniendo los parámetros una clave privada y una clave pública correspondiente;

- atribuir a escrutadores claves que les permitan descifrar y verificar las papeletas de voto emitidas para el escrutinio y

- transmitir a cada miembro de la lista de electores del escrutinio de los parámetros a utilizar por el elector para calcular una clave privada, y un certificado de miembro de la lista de electores del escrutinio.

Según la invención, el calculador comprende, además, medios para:

- generar un número de secuencia propio para el escrutinio a utilizar por los miembros de la lista de electores para firmar una papeleta de voto, una firma de una papeleta de voto que comprende un elemento de firma que es común a todas las firmas emitidas con un mismo número de secuencia por un mismo miembro de la lista de electores del escrutinio, y que contiene una prueba de que el número de secuencia fue utilizado para generar la firma;

— retirar de la lista un elector del escrutinio a revocar, y actualizar los parámetros de puesta en práctica de la firma electrónica anónima propia a los miembros de la lista de electores del escrutinio, para tener en cuenta la retirada del elector y

— actualizar los certificados de los electores del escrutinio a cada modificación de la composición de la lista de los electores del escrutinio.

La invención se refiere, asimismo, a un terminal para emitir una firma de lista que comprende medios para:

— recibir parámetros de cálculo de una clave privada;

- calcular la clave privada con la ayuda de los parámetros recibidos y de los parámetros elegidos de forma aleatoria;

- recibir un certificado de miembro de una lista;

- generar una firma propia para los miembros de la lista, siendo constituida esta firma de manera que contenga una prueba de que el miembro de la lista, que ha emitido la firma, conoce un certificado de miembro de la lista y

- comprobar una firma emitida por un miembro de la lista aplicando un algoritmo predefinido para poner en evidencia la prueba de que la firma fue emitida por una persona en posesión de un certificado de miembro de la lista.

Según la invención, el terminal comprende, además, medios para:

- recibir un número de secuencia a utilizar en una fase de firma;

- generar una firma calculando un elemento de firma que sea común a todas las firmas emitidas por un mismo miembro de la lista, con un mismo número de secuencia y que contenga una prueba de que el número de secuencia fue utilizado para generar la firma;

- comprobar la prueba de que el número de secuencia fue utilizado para generar una firma y

- recibir un nuevo certificado de miembro de la lista a cada modificación de la composición de la lista.

La invención se refiere, asimismo, a un terminal para emitir una firma de papeleta de voto para un escrutinio, que comprende medios para:

— recibir parámetros de cálculo de una clave privada;

- calcular la clave privada con la ayuda de los parámetros recibidos y de parámetros elegidos de forma aleatoria;

— recibir un certificado de miembro de una lista de electores del escrutinio;

- generar una firma de una papeleta de voto, siendo esta firma constituida de manera que contenga una prueba de que el miembro de la lista, que ha emitido la firma, conoce un certificado de miembro de la lista de electores y

— verificar una firma de una papeleta de voto, emitida por un miembro de la lista de elector, aplicando un algoritmo predefinido para poner en evidencia la prueba de que la firma fue emitida por una persona en posesión de un certificado de miembro de la lista.

Según la invención, el terminal comprende, además, medios para:

— recibir un número de secuencia a utilizar para firmar una papeleta de voto;

— generar una firma de una papeleta de voto calculando un elemento de firma que sea común a todas las firmas emitidas por un mismo miembro de la lista de electores, con un mismo número de secuencia, y que contenga una prueba de que el número de secuencia fue utilizado para generar la firma;

— verificar la prueba de que el número de secuencia fue utilizado para generar una firma de una papeleta de voto y

— recibir un nuevo certificado de miembro de la lista de electores a cada modificación de la composición de la lista de electores.

Una forma de realización preferida de la invención se describirá a continuación, a título de ejemplo no limitativo, con referencia a los dibujos adjuntos en donde:

La Figura 1 representa un sistema que permite la puesta en práctica de métodos de firma de lista y de voto electrónico, según la invención;

Las Figuras 2 a 8 ilustran, bajo la forma de organigramas, los diferentes procedimientos que se ejecutan en conformidad con los métodos de firma de lista y de voto electrónico, según invención.

La presente invención da a conocer un método de firma de lista, en donde todas las personas autorizadas, es decir, que Figuran en la lista, puedan proporcionar una firma que sea anónima, y sin importar que sea capaz de verificar la validez de la firma sin tener acceso a la identidad del miembro de la lista que ha firmado.

Un tal método puede ponerse en práctica en el sistema representado en la Figura 1. Este sistema presenta terminales 2 puestos a la disposición de los usuarios y conectados a una red de transmisión 5 de datos digitales, tal como la red Internet. Cada terminal 2 está ventajosamente conectado a un lector 8 de tarjeta de circuito integrado 7. Por intermedio de la red 5, los usuarios se pueden conectar a un servidor 6 que da acceso a informaciones, por ejemplo, almacenadas en una base de datos 4. Este sistema comprende, además, un calculador 1 de una autoridad de confianza que entrega, en particular, las tarjetas de circuitos integrados 7 a los usuarios.

El método de firma de lista, según la invención, retoma en el método de firma de grupo, descrito en el documento de referencia [1], los procedimientos siguientes:

— un procedimiento de organización de un grupo de signatarios, que consiste en establecer los diferentes parámetros y claves públicas que se necesiten,

— un procedimiento de registro, en donde una persona a inscribir en el grupo recibe de una autoridad de confianza un derecho de firma, es decir una clave privada y un certificado autorizados,

— un procedimiento de firma propiamente dicho en cuyo transcurso una persona, que posee un derecho de firma, firma un mensaje y

— un procedimiento de verificación que consiste en aplicar un algoritmo de verificación de una firma para verificar que la firma se haya proporcionado por una persona que posea un derecho de firma.

La invención prevé, además, una disposición para garantizar el anonimato de un signatario, incluso ante una autoridad de confianza, así como un procedimiento de organización de una secuencia, que consiste en definir un número de secuencia a utilizar para generar firmas de lista, comprendiendo, además, la verificación de una firma, una etapa de verificación de que la firma es única para un número de secuencia dado.

El método, según la invención, puede comprender, además, un procedimiento de revocación, tal como se define en el documento de referencia [2]. Con la ayuda de este procedimiento de revocación, una autoridad de confianza puede retirar, a un miembro de la lista, los derechos de firma que le fueron anteriormente atribuidos, a partir de la identidad del miembro. El establecimiento de esta posibilidad de revocación implica la ejecución por los miembros de la lista de un procedimiento de actualización, en cuyo transcurso los miembros de la lista actualizan sus certificados para tener en cuenta las modificaciones (adición o retiradas) efectuadas en la lista de las personas autorizadas para firmar.

La Figura 2 ilustra las diferentes etapas del procedimiento de organización 10 ejecutado en el calculador 1 de la autoridad de confianza.

De conformidad con el documento de referencia [1], este procedimiento consiste en elegir, 11, números enteros siguientes:

$\varepsilon > 1, k, l_p,$

$\lambda_1, \lambda_2, \gamma_1, \gamma_2$ que son longitudes de números enteros en números de bits, con:

$$\lambda_2 > 4l_p \quad (1)$$

$$\lambda_1 > \varepsilon(\lambda_2 + k) + 2 \quad (2)$$

$$\gamma_2 > \lambda_1 + 2 \quad (3)$$

$$\gamma_1 > \varepsilon(\gamma_2 + k) + 2 \quad (4)$$

y en definir los conjuntos de números enteros siguientes:

$$\Lambda =]2^{\lambda 1} - 2^{\lambda 2}, 2^{\lambda 1} + 2^{\lambda 2}[\text{ y}$$
$$\Gamma =]2^{\gamma 1} - 2^{\gamma 2}, 2^{\gamma 1} + 2^{\gamma 2}[.$$

Este procedimiento consiste, además, en elegir una función de resumen criptográfico resistente a las colisiones *H* tal que una secuencia binaria de cualquier longitud indicada $\{O,1\}^*$ se transforma en una secuencia binaria de longitud k indicada $\{0,1\}^k$.

A continuación, el calculador 1 de la autoridad de confianza genera, de forma aleatoria, en la etapa 12, números primos p' y q' de magnitud l_p, tales que p=2p'+1 y q=2q'+1 son también números primos. A continuación, calcula, en la etapa 13, el módulo n=pq y genera, de forma aleatoria, en la etapa 14, números enteros a, a_0, b, g y h en el conjunto QR(n) de los residuos cuadráticos de n, es decir, el conjunto de los números enteros y tales que $y=x^2$ (mod.n), siendo x un número entero. Se considera, entonces, que la clave pública PK de la autoridad de confianza está constituida por la secuencia de números enteros (n, a, a_0, b, g, h) y que la clave privada de esta última está constituida por la secuencia de números enteros (p', q').

Para ser registrado por la autoridad de confianza, un usuario, que desee llegar a ser miembro de la lista, ejecuta en su terminal 2 el procedimiento 20 ilustrado en la Figura 3. La ejecución de este procedimiento establece un diálogo con el calculador 1 de la autoridad de confianza, que ejecuta, entonces, un procedimiento 20'. El procedimiento 20 comprende, ante todo, una etapa 21 de generación aleatoria de números enteros $\tilde{\tilde{X}}_i$ y $\tilde{r}$, respectivamente, en los intervalos $\left]0,2^{\lambda_2}\right[$ y $\left]0,n^2\right[$. A partir de estos números enteros, se calcula 22 un número entero C_1 tal que:

$$C_1 = g^{\tilde{X}_i} h^{\tilde{r}} (\text{mod} n) \qquad (5)$$

En la etapa 23, se establece la prueba U del conocimiento de dos números α y β (es decir $\tilde{\tilde{X}}_i$ y $\tilde{r}$) tal que $C_1 = g^{\alpha} h^{\beta}$ (mod n).

Una tal prueba se constituye, por ejemplo, eligiendo de forma aleatoria dos números enteros r_1 y r_2 en el conjunto de los números binarios con signo en $\varepsilon(21_p + k)$ bits, indicado $\pm\{0, 1\}^{\varepsilon(2l_p+k)}$, y calculando los números siguientes:

$$d_1 = g^{r1} h^{r2} (\text{mod n}), \qquad (6)$$
$$c = H(g \| h \| C_1 \| d_1), \qquad (7)$$

en donde el símbolo ‖ representa el operador de concatenación,

$$s_1 = r_1 - c\alpha, \qquad (8)$$
$$s_2 = r_2 - c\beta. \qquad (9)$$

siendo s_1 y s_2 números enteros relativos.

La prueba U es entonces igual a (c, s_1, s_2, C_1).

El número C_1 y la prueba U se envían, a continuación, a la autoridad de confianza, que verifica, en la etapa 21' la prueba U y que C_1 se encuentra en el conjunto QR(n) de los residuos cuadráticos de n.

En el ejemplo precedente, la verificación de la prueba U consiste en calcular:

$$t_1 = C_1^c g^{s_1} h^{s_2} (\text{modn}), \text{ y} \qquad (10)$$
$$c' = H(g \| h \| C_1 \| t_1). \qquad (11)$$

La prueba se verifica si c' = c y si s_1 y s_2 pertenecen al conjunto $\pm\{0, 1\}^{\varepsilon(2l_p+k)+1}$.

Si tal es el caso, el calculador 1 de la autoridad de confianza genera de forma aleatoria 22' dos números enteros α_i, β_i en el intervalo $]0,2^{\lambda 2}[$, y envía estos números al terminal 2 del usuario. En el procedimiento 20, el terminal del usuario calcula, entonces, en la etapa 24, los números enteros x_i y C_2 aplicando las fórmulas siguientes:

$$x_i = 2^{\lambda_1} + (\alpha_i \tilde{x}_i + \beta_i (\mathrm{mod} 2^{\lambda_2})), \text{ y} \quad (12)$$

$$C_2 = a^{x_i} (\mathrm{mod} n). \quad (13)$$

Luego, construye, en la etapa 25, las pruebas siguientes (por ejemplo, según el mismo principio que la prueba U):

— la prueba V de conocer un número α que pertenece al conjunto Λ tal que:

$$C_2 = a^{\alpha} (\mathrm{mod}\, n) \quad (14)$$

— la prueba W de conocer tres números β, γ, δ tales que $\beta \in]-2^{\lambda_2}, 2^{\lambda_2}[$ y

$$C_2 / a^{\lambda_2} = a^{\beta} \text{ y} \quad (15)$$

$$C_1^{\alpha_i} g^{\beta_i} = g^{\beta} (g^{2^{\lambda_2}})^{\gamma} h^{\delta} \quad (16)$$

C_2 y las pruebas V y W son, luego, enviadas al calculador 1 de la autoridad de confianza que verifica 23' las pruebas V y W, y que C_2 pertenecen al conjunto QR(n). Si tal es el caso, genera 24', de forma aleatoria, un número primo e_i que pertenece al conjunto Γ y aplica la fórmula siguiente:

$$A_i = (C_2 a_0)^{1/e_i} (\mathrm{mod} n) \quad (17)$$

y reenvía al usuario los enteros A_i y e_i considerados como un certificado $[A_i, e_i]$ de pertenencia del usuario a la lista.

El calculador 1 crea 26' entonces una nueva entrada en una tabla de los miembros de la lista, por ejemplo en la base de datos 4, en donde memoriza el certificado $[A_i, e_i]$ en vista de modificaciones de la lista (por ejemplo, revocaciones de miembros) y, preferentemente, los mensajes intercambiados entre la autoridad de confianza y el usuario durante este procedimiento de registro del usuario.

Por otro lado, el usuario puede comprobar 26 la autenticidad del certificado recibido comprobando que se satisface la ecuación siguiente:

$$a^{x_i} a_0 = A_i^{e_i} (\mathrm{mod} n) \quad (18)$$

Al final de este procedimiento de registro 20, el usuario dispone de una clave privada x_i y de un certificado $[A_i, e_i]$ de miembro de la lista, que se memorizan, por ejemplo, en una tarjeta de circuito integrado 7.

Con la ayuda de un tal certificado, el usuario puede generar una firma de un mensaje M que pertenece al conjunto $\{O, 1\}^*$.

A este efecto, la autoridad de confianza publica, según la invención, un número m de secuencia, elegido, de forma aleatoria, en el conjunto QR(n). Este número deberá utilizarse por los miembros de la lista para firmar un mensaje durante una secuencia dada. Los números respectivos de secuencias diferentes no deben poder estar vinculados. En particular, debe ser imposible calcular un logaritmo discreto de un número de secuencia dado, con respecto a la base de otro número de secuencia, es decir que no debe ser posible, en la práctica, calcular números enteros x e y tales que: $m^x = m'^y$ (mod n), siendo m y m' números de secuencia.

Este número m de secuencia se puede calcular en función de la fecha de inicio de la secuencia: m = F(fecha). Esta función F se elige, por ejemplo, igual a:

$$F(d) = (H'(d))^2 (\mathrm{mod}\, n) \quad (19)$$

en donde *H'* es una función de resumen criptográfico, resistente a las colisiones, tal como una secuencia binaria de cualquier longitud indicada $\{0,1\}^*$, se transforma en una secuencia binaria de longitud 21_p indicada $\{0,1\}^{21_p}$. Por lo tanto, es fácil comprobar la validez del número de secuencia aplicando la fórmula (19).

El procedimiento de firma de un mensaje está diseñado para permitir, en particular, a un usuario demostrar que conoce un certificado de miembro y una clave privada de miembro y que utiliza el número de secuencia correcto.

Para firmar un mensaje M, un miembro de la lista debe ejecutar, por ejemplo, en su tarjeta de circuito integrado 7, conectada a un terminal 2 y memorizando su certificado $[A_i, e_i]$ y su clave privada x_i, un procedimiento 30 de firma,

según se ilustra en la Figura 4. Este procedimiento comprende, ante todo, una etapa 31 de generación aleatoria de un número ω que pertenece al conjunto $\{0,1\}^{21_p}$.

Además, comprende una etapa 32 que consiste en calcular los números siguientes a partir de ω:

$$T_1 = A_i b^{\omega} \pmod n, \quad (20)$$

$$T_2 = g^{\omega} \pmod n, \quad (21)$$

$$T_3 = g^{e_i} h^{\omega} \pmod n. \quad (22)$$

De conformidad con la invención, se calcula, asimismo, el número siguiente:

$$T_4 = m^{x_i} \pmod n \quad (23)$$

En la etapa 33 siguiente, se genera, de una forma aleatoria, los números r_1 en el conjunto de los números binarios, con signo, en $\varepsilon(\gamma_2+k)$ bits, indicado $\pm\{0,1\}^{\varepsilon(\gamma_2+k)}$, r_2 en el conjunto $\pm\{0,1\}^{\varepsilon(\lambda_2+k)}$, r_3 en el conjunto $\pm\{0,1\}^{\varepsilon(\gamma_1+2l_p+k+1)}$ y r_4 en el conjunto $\pm\{0,1\}^{\varepsilon(2l_p+k)}$. Luego, en la etapa 34, se calcula las magnitudes siguientes:

$$d_1 = T_1^{r1}/(a^{r2}y^{r3}) \pmod n \quad (24)$$

$$d_2 = T_2^{r1}/g^{r3} \pmod n \quad (25)$$

$$d_3 = g^{r4} \pmod n \quad (26)$$

$$d_4 = g^{r1}h^{r4} \pmod n \quad (27)$$

Según la invención, se calcula, asimismo, el número siguiente:

$$d_5 = m^{r2} \pmod n \quad (28)$$

A continuación, en la etapa 35, se calcula los números siguientes:

$$c = H(m\|b\|g\|h\|a_0\|a\|T_1\|T_2\|T_3\|T_4\|d_1\|d_2\|d_3\|d_4\|d_5\|M), \quad (29)$$

en donde $\|$ representa la operación de concatenación,

$$s_1 = r_1 - c(e_i - 2^{\gamma_1}), \quad (30)$$

$$s_2 = r_2 - c(x_i - 2^{\lambda_1}), \quad (31)$$

$$s_3 = r_3 - ce_i\omega, \quad (32)$$

$$s_4 = r_2 - c\omega, \quad (33)$$

siendo s_l, s_2, s_3, s_4 números enteros relativos.

La firma está, al final, constituida por el conjunto de números siguientes:

$$(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3, T_4). \quad (34)$$

que se emite, por ejemplo, por la red 5.

La verificación de una firma de un mensaje M se desarrolla ejecutando el procedimiento 40 ilustrado en la Figura 5. Este procedimiento comprende, ante todo, en la etapa 41, el cálculo de los números siguientes:

$$t_1 = a_0^c T_1^{s_1 - c2^{\gamma_1}} / (a^{s_2 - c2^{\lambda_1}} b^{s_3}) (\mathrm{mod} n) \quad (35)$$

$$t_2 = T_2^{s_1 - c2^{\gamma_1}} / g^{s_3} (\mathrm{mod} n) \quad (36)$$

$$t_3 = T_2^c g^{s_4} (\mathrm{mod} n) \quad (37)$$

$$t_4 = T_3^c g^{s_1 - c2^{\gamma_1}} h^{s_4} (\mathrm{mod} n) \quad (38)$$

Según la invención. Comprende, además, el cálculo de los números siguientes:

$$t_5 = T_4^c m^{s_2 - c2^{\lambda_1}} (\mathrm{mod} n) \quad (39)$$

$$c' = H(m||b||g||h||a_0||a||T_1||T_2||T_3||T_4||t_1||t_2||t_3||t_4||t_5||M) \quad (40)$$

La firma es auténtica si las condiciones siguientes se verifican en la etapa 42:

$$c' = c \quad (41)$$

$$s_1 \in \pm\{0, 1\}^{\varepsilon(\gamma_2 + k)+1}, \quad (42)$$

$$s_2 \in \pm\{0, 1\}^{\varepsilon(\lambda_2 + k)+1}, \quad (43)$$

$$s_3 \in \pm\{0, 1\}^{\varepsilon(\gamma_1 + 2l_p + k + 1)+1}, \quad (44)$$

$$s_4 \in \pm\{0, 1\}^{\varepsilon(2l_p + k)+1}. \quad (45)$$

Si no se cumplen estas condiciones, la firma no es válida (etapa 45).

Además, accediendo a todas las firmas que se emitieron durante una secuencia dada, por ejemplo en la base de datos 4, se puede verificar fácilmente, en la etapa 43, con la ayuda del parámetro T_4, si un miembro de la lista ha firmado varias veces: todas las firmas emitidas por un miembro de la lista comprenden un parámetro T_4 que tiene el mismo valor para un número de secuencia dado.

Conviene señalar, además, que un miembro no puede engañar utilizando otro valor porque T_4 está muy vinculado a T_1. En efecto, la fórmula de cálculo de T_1 se puede escribir también de la manera siguiente:

$$T_1^{e_i} = a_0 a^{x_i} b^{\omega e_i} (\mathrm{mod} n) \quad (46)$$

Si T_4 ya se encuentra en el conjunto de las firmas emitidas para un número de secuencia dado, se deduce de ello que la firma fue ya emitida por un miembro de la lista para este número de secuencia (etapa 46).

Para incluir una posibilidad de revocación de un miembro de la lista, el método, que se acaba de describir, se puede modificar de la forma siguiente.

El procedimiento de organización 10 de la lista comprende, además, en la etapa 14, la elección aleatoria de un número u, que pertenece al conjunto QR(n), y la definición de dos conjuntos E_{add} y E_{del} que están inicialmente vacíos.

La clave pública PK de la autoridad de confianza está, entonces, constituida por la secuencia de números enteros (n, a, a_0, b, g, h, u) y conjuntos E_{add} y E_{del}.

Durante el procedimiento de registro 20, 20', el calculador 1 de la autoridad de confianza atribuye, en la etapa 25', el parámetro u_i al nuevo miembro U_i de la lista, siendo este parámetro tal que $u_i = u$, y actualiza el valor del parámetro u sustituyendo este valor por u^{ei}.

El certificado del nuevo miembro reagrupa, entonces, los enteros A_i, e_i y u_i, siendo este certificado memorizado, en la etapa 26', para modificaciones futuras y se transmite al nuevo miembro.

La autoridad de confianza introduce, asimismo, el número e_i atribuido al nuevo miembro en el conjunto E_{add}.

A la recepción de su certificado, el nuevo miembro verifica, además, que:

$$u_i^{e_i} = u \pmod n \quad (47)$$

Los otros miembros U_j de la lista deben, entonces, ejecutar un procedimiento de actualización para tener en cuenta la llegada del nuevo miembro y por lo tanto, la modificación del parámetro de lista u. Este procedimiento consiste en recalcular su parámetro u_j de la forma siguiente:

$$u_j = u_j^{e_i} \pmod n \quad (48)$$

De esta manera, la relación (47) se verifica siempre para todas las parejas (u_j, e_j) de todos los miembros de la lista.

El procedimiento de revocación de un miembro U_k de la lista, cuyo certificado es (A_k, e_k, u_k) consiste, para la autoridad de confianza, en modificar el parámetro u de la manera siguiente:

$$u = u^{1/e_k} \pmod n \quad (49)$$

y en introducir el parámetro e_k en el conjunto E_{del}.

Además, cada miembro no revocado U_j de la lista debe tener en cuenta esta revocación (cambio del parámetro u) recalculando su parámetro u_j de la forma siguiente:

$$u_j = u_j^b u^a \pmod n \quad (50)$$

siendo a y b tales que $ae_j + be_k = 1$

Para determinar a y b, basta aplicar el algoritmo de Euclides extendido, que consiste en efectuar una serie de divisiones euclidianas.

Conviene señalar que el miembro revocado (que posee e_k) no puede determinar a y b con la ayuda de la fórmula (50), que se convierte en $e_k(a + b) = 1$, y por lo tanto, recalcular el parámetro u_k.

Durante el procedimiento 30 de firma por un miembro de la lista, es preciso, además, en la etapa 31, elegir, de forma aleatoria, los números w_1, w_2 y w_3 de longitud binaria igual a 21_p, es decir, que pertenezca al conjunto $\{0,1\}^{21_p}$, y calcular, en la etapa 32, los números siguientes:

$$T_5 = g^{e_i} h^{w_1} (\mathrm{mod} n) \quad (51)$$

$$T_6 = u_i h^{w_2} (\mathrm{mod} n) \quad (52)$$

$$T_7 = g^{w_2} h^{w_3} (\mathrm{mod} n) \quad (53)$$

Además, es preciso, en la etapa 33, elegir, de forma aleatoria, números r_5, r_6, r_7 que pertenecen al conjunto $\pm\{0,1\}^{\varepsilon(2l_p+k)}$ y números r_8 y r_9 que pertenecen al conjunto $\pm\{0,1\}^{\varepsilon(\gamma_1+2l_p+k+1)}$ y luego, calcular, en la etapa 34, los números siguientes:

$$d_6 = g^{r1} h^{r5} \pmod n \quad (54)$$

$$d_7 = g^{r6} h^{r7} \pmod n \quad (55)$$

$$d_6 = T_6^{r1} / h^{r8} \pmod n \quad (56)$$

$$d_9 = T_7^{r1} / (g^{r8} h^{r9}) \pmod n \quad (57)$$

El número c incluye, entonces, los elementos siguientes:

$$c = H(m \| b \| g \| h \| a_0 \| a \| T_1 \| T_2 \| T_3 \| T_4 \| T_5 \| T_6 \| T_7 \| d_1 \| d_2 \| d_3 \| d_4 \| d_5 \| d_6 \| d_7 \| d_8 \| d_9 \| M) \quad (58)$$

Es preciso, entonces, calcular en la etapa 35:

$$s_5 = r_5 - cw_1 \quad (59)$$

$$s_6 = r_6 - cw_2 \quad (60)$$

$$s_7 = r_7 - cw_3 \quad (61)$$

$$s_8 = r_8 - ce_iw_2 \quad (62)$$

$$s_9 = r_9 - ce_iw_3 \quad (63)$$

La firma está, entonces, constituida por el conjunto de números siguientes:

$$(c, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, T_1, T_2, T_3, T_4, T_5, T_6, T_7). \quad (64)$$

El procedimiento 40 de verificación de una firma comprende entonces, además, el cálculo de los números siguientes en la etapa 41:

$$t_6 = T_5^c g^{s_1 - c2^{\gamma_1}} h^{s_5} (\mathrm{mod} n) \quad (65)$$

$$t_7 = T_7^c g^{s_6} h^{s_7} (\mathrm{mod} n) \quad (66)$$

$$t_8 = u^c T_6^c g^{s_1 - c2^{\gamma_1}} / h^{s_8} (\mathrm{mod} n) \quad (67)$$

$$t_9 = T_7^{s_1 - c2^{\gamma_1}} / (g^{s_8} h^{s_9}) (\mathrm{mod} n) \quad (68)$$

$$c' = H(m \| b \| g \| h \| a_0 \| a \| T_1 \| T_2 \| T_3 \| T_4 \| T_5 \| T_6 \| T_7 \| t_1 \| t_2 \| t_3 \| t_4 \| t_5 \| t_6 \| t_7 \| t_8 \| t_9 \| M) \quad (69)$$

La firma es auténtica si las condiciones suplementarias siguientes se verifican en la etapa 42:

$$s_5 \in \pm\{0, 1\}^{\varepsilon(2l_p+k)+1}, \quad (70)$$

$$s_6 \in \pm\{0, 1\}^{\varepsilon(2l_p+k)+1}, \quad (71)$$

$$s_7 \in \pm\{0, 1\}^{\varepsilon(2l_p+k)+1}, \quad (72)$$

$$s_8 \in \pm\{0, 1\}^{\varepsilon(\gamma_1+2l_p+k+1)+1} \text{ et} \quad (73)$$

$$s_9 \in \pm\{0, 1\}^{\varepsilon(\gamma_1+2l_p+k+1)+1}. \quad (74)$$

Conviene señalar que, contrariamente a la firma de grupo descrita en el documento [1], no es posible, para la autoridad de confianza, reencontrar la identidad de un signatario, es decir el número A_i del certificado del signatario a partir de una firma de lista, tal como se ha descrito. En efecto, contrariamente al método descrito en este documento, la autoridad de confianza no utiliza una clave privada *x* para generar el parámetro b y por lo tanto, el número A_i no puede deducirse de T_1 y T_2.

Además, la firma generada por un miembro revocado U_k se detectará no válida. En efecto, el parámetro T_6 hace intervenir el parámetro u_k que fue determinado a partir del parámetro común u, y el parámetro t_8, que se calcula para verificar la firma, hace intervenir, asimismo, el parámetro u que fue modificado como resultado de la revocación del miembro k. Se deduce de ello que, en el momento de la verificación de la firma, los parámetros T_6 y t_8 son incoherentes y, por lo tanto, que la igualdad entre c y c' no se puede verificar por la firma del miembro k.

El método de firma de lista, que se acaba de describir, se puede aplicar a un método de voto electrónico. El método de voto electrónico, según la invención, comprende varias fases cuya ejecución de los procedimientos del método de firma de lista se describe a continuación.

Este método implica la intervención de una autoridad de confianza 1 organizadora de las elecciones que ejecuta, a este efecto, un procedimiento 50 de organización del escrutinio. Este procedimiento consiste en generar los datos necesarios para el buen desarrollo de las elecciones, una base de datos pública accesible a todos, en donde se recogen las papeletas de voto. En el curso de la organización del escrutinio, se designa, asimismo, escrutadores que se encargarán de recontar los votos y determinar el resultado de la elección.

La autoridad organizadora procede, ante todo, a la generación de los diferentes parámetros necesarios para el establecimiento de una firma de lista, ejecutando el procedimiento 10 de organización de una firma de lista. A continuación, los electores deben inscribirse previamente, por ejemplo en una alcaldía, en una lista electoral de modo

que reciba todos los datos necesarios, a saber una clave privada x_i y un certificado (A_i, e_i, u_i), para generar una firma de lista. Con la ayuda de estos parámetros, los electores pueden participar en todas las elecciones futuras. Este procedimiento de inscripción puede, por ejemplo, ejecutarse entre una tarjeta de circuito integrado 7 y un terminal 2, memorizando la tarjeta de circuito integrado, al final del procedimiento, el certificado del elector.

Antes de una elección, la autoridad organizadora procede a la actualización de las listas electorales ejecutando el procedimiento 20, 20' para los electores nuevamente inscritos, y retirando (revocando) los derechos de firma de lista a todas las personas excluidas de los registros de electores (por ejemplo, las personas que hayan abandonado la circunscripción o despojados de sus derechos cívicos). Estas revocaciones se realizan ejecutando el procedimiento de revocación antes descrito. En la etapa 51 del procedimiento 50, la autoridad organizadora publica, asimismo, un número de secuencia m necesario para el establecimiento de una nueva secuencia de firma de lista, de modo que se impida a los electores votar (firmar) dos veces en esta elección.

Por otro lado, los escrutadores procederán a crear 52 las parejas de claves públicas/privadas necesarias, de tal modo que todos deban cooperar para poder descifrar un mensaje cifrado con la clave pública. A este efecto, el sistema criptográfico establecido se elige de modo que se permita a un elector cifrar un mensaje (papeleta de voto) con la ayuda de al menos una clave pública, imponiendo la cooperación de todos los escrutadores para utilizar la o las claves privadas correspondientes y así descifrar el mensaje.

La repartición de las claves privadas de descifrado entre todos los escrutadores se puede efectuar, del modo siguiente.

Se considera g un generador del grupo cíclico G. Una clave privada x_i respectiva se atribuye a cada escrutador i que calcule el número y_i que pertenece a G tal que:

$$y_i = g^{x_i} \qquad (75)$$

La clave pública Y a utilizar por los electores se obtiene por la fórmula siguiente:

$$Y = \prod_i y_i \qquad (76)$$

y la clave privada X correspondiente compartida por todos los escrutadores i es la siguiente:

$$X = \sum_i x_i \qquad (77)$$

Se puede llegar a un resultado análogo procediendo a un cifrado utilizando todas las claves públicas respectivas de los escrutadores, necesitando el descifrado el conocimiento de todas las claves privadas correspondientes.

Antes de ir a votar, cada elector debe actualizar su certificado de firma de lista, de conformidad con el procedimiento de modificación antes descrito, con la ayuda de los parámetros anteriormente publicados. Si el elector no está excluido de las listas electorales, se podrá efectuar esta modificación.

Durante la apertura de las oficinas de voto, cada elector emite una papeleta de voto ejecutando, en un terminal, un procedimiento 60. En la etapa 61, el elector selecciona su voto v_i y cifra este último con la ayuda de la clave pública de los escrutadores para obtener un voto cifrado D_i. A continuación, firma el voto cifrado con la ayuda del método de firma de lista para obtener una firma S_i. La papeleta de voto constituida por el conjunto (D_i, S_i) del voto y de la firma, se publica, a continuación, de manera anónima, en una base de datos pública 4.

En la etapa 62, se realiza el cifrado del voto utilizando un algoritmo de cifrado probabilista (es decir que la probabilidad de que dos cifrados de un mismo mensaje sean idénticos es casi nula), tal como, por ejemplo, el algoritmo de El Gamal o de Paillier. Si se aplica el algoritmo de El Gamal, el cifrado se efectúa calculando los números siguientes:

$$a_j = v_j Y^r \quad y \, b_j = g^r \qquad (78)$$

en donde r es un elemento aleatorio. El voto v_j cifrado está, entonces, constituido por el par $D_i = (a_i, b_i)$. El elector E_j determina 63, a continuación, la firma de lista del voto cifrado $S_j = Sig_{liste}(a_j \| b_j)$, siendo Sig_{liste} la firma de lista tal como se describió antes, ejecutando el procedimiento 30 por su tarjeta de circuito integrado 7, que luego se transmite al terminal 2.

El elector E_j ha generado así su papeleta de voto (D_j, S_j) que envía 64 a la base de datos pública 4 por medio de un canal de transmisión anónima, es decir, impidiendo relacionar un mensaje transmitido con el emisor de este último. El elector puede, a este efecto, utilizar un terminal público o una red de mezcladores.

Al final del escrutinio, los escrutadores efectúan el recuento del escrutinio ejecutando el procedimiento 70 en el terminal 3. Este procedimiento consiste, ante todo, en generar 71 la clave privada de descifrado X a partir de sus claves

privadas respectivas x_i y con la ayuda de la fórmula (77). Luego, en la etapa 72, acceden a la base de datos pública 4 de las papeletas de voto para obtener las papeletas de voto (D_i, S_i) y para descifrarlas.

El descifrado propiamente dicho de las papeletas de voto consiste para cada papeleta de voto emitida (etapa 73) a verificar 74 la firma S_i ejecutando el procedimiento 40 de verificación de firma de lista antes descrita y si la firma es válida y única (etapa 75), a descifrar 76 el voto cifrado D_j aplicando la fórmula siguiente:

$$v_j = a_j / b_j^X \qquad (79)$$

Los votos v_j así descifrados y verificados, con el resultado de la verificación correspondiente, se introducen 77 en la base de datos 4 de las papeletas de voto, en asociación con la papeleta de voto (D_j, S_j).

La clave privada de descifrado X se publica, asimismo, para permitir a todos verificar el recuento de las papeletas de voto.

Una vez recontadas todas las papeletas de voto, este procedimiento 70 calcula, en la etapa 78, el resultado de la elección y actualiza la base de datos pública de las papeletas de voto, introduciendo en ella este resultado y en caso necesario, la clave privada de descifrado X.

Resulta fácil constatar que las propiedades antes enunciadas, necesarias para el establecimiento de un sistema de voto electrónico, se verifican por el método descrito con anterioridad. En efecto, cada elector solamente puede votar una sola vez puesto que es fácil encontrar, en la base de datos, dos firmas emitidas por un mismo elector para un mismo escrutinio (para un mismo número de secuencia). En este caso, los escrutadores pueden no tener en cuenta los dos votos o contabilizar un solo voto si son idénticos.

Como alternativa, se puede prever que, en la etapa 64 de introducción de un voto en la base de datos 4, se comprueba que el voto emitido por el elector ya no figura en la base de datos, al buscar en ella el parámetro T_4 propio del elector. Si se detecta, de este modo, que el elector ya ha votado para este escrutinio, el nuevo voto no se introducirá en la base de datos 4.

En consecuencia, no es posible comenzar el recuento de las papeletas de voto antes del final del escrutinio si al menos uno de los escrutadores respeta la regla, puesto que es precisa la presencia de todos los escrutadores para realizar el recuento de una papeleta de voto. Por último, el resultado de la elección es verificable por todos, puesto que los escrutadores proporcionan, en la base de datos, todos los elementos necesarios (en particular, la clave privada de recuento) para proceder a una tal verificación y que la verificación de una firma es accesible para todos, utilizando la clave pública PK=(n, a, a_0, b, g, h, u) de la autoridad de confianza. De este modo, cualquier persona de confianza podrá efectuar el recuento de la misma manera que los escrutadores y por lo tanto, será posible cerciorarse de que lo realizó de forma correcta.

Por supuesto, las claves de los escrutadores quedarán obsoletas al final del escrutinio, puesto que se hicieron públicas.

REIVINDICACIONES

1.- Un método de firma de lista que comprende al menos:

— una fase de organización (10) que consiste, para una autoridad de confianza (1), en definir parámetros de puesta en práctica de una firma electrónica anónima, que presenta una clave privada y una clave pública correspondiente,

— una fase de registro (20, 20') de personas en una lista de miembros autorizados para generar una firma electrónica propia para los miembros de la lista, en cuyo transcurso cada persona (2) a registrar calcula (24) una clave privada (x_i) con la ayuda de parámetros proporcionados por la autoridad de confianza y de parámetros elegidos, de forma aleatoria, por la persona a registrar, y la autoridad de confianza entrega (25') a cada persona a registrar un certificado ($[A_i, e_i]$) de miembro de la lista,

- una fase de firma (30), en cuyo transcurso un miembro de la lista genera (35) y emite (36) una firma propia a los miembros de la lista, siendo esta firma constituida de manera que contenga una prueba de que el miembro de la lista, que ha emitido la firma, hace conocer un certificado ($[A_i, e_i]$) de miembro de la lista y

- una fase de comprobación (40) de la firma emitida que comprende etapas (41, 42) de aplicación de un algoritmo predefinido para poner en evidencia la prueba de que la firma fue emitida por una persona en posesión de un certificado de miembro de la lista, caracterizado porque comprende, además:

- una fase de definición de una secuencia que consiste en que la autoridad de confianza (1) genere un número de secuencia m a utilizar en la fase de firma (30), una firma (Sig_{liste}), generada durante la fase de firma, que comprende un elemento de firma (T_4) que es común a todas las firmas emitidas por un mismo miembro de la lista, con un mismo número de secuencia, y que contiene una prueba de que el número de secuencia m fue utilizado para generar la firma, comprendiendo la fase de verificación (40), además, una etapa de verificación (43) de la prueba de que el número de secuencia fue utilizado para generar la firma;

- una fase de revocación de un miembro de la lista para retirar un miembro de la lista, en cuyo transcurso la autoridad de confianza (1) retira de la lista el miembro a retirar y actualiza los parámetros de puesta en práctica de la firma electrónica anónima, para tener en cuenta la retirada del miembro de la lista y

— una fase de actualización de certificados ($[A_i, e_i]$) de los miembros de la lista para tener en cuenta modificaciones de la composición de la lista.

2.- El método, según la reivindicación 1, caracterizado porque que la fase de organización (10) comprende la definición de un parámetro común (u) que depende de la composición de la lista, la fase de registro (20, 20') de una persona en la lista que comprende la definición de un parámetro (u_i) propio de la persona a registrar, que se calcula en función del parámetro (u) que depende de la composición de la lista y que está integrado en un certificado ($[A_i, e_i, u_i]$) remitido a la persona, comprendiendo la fase de registro (20, 20') una etapa de actualización del parámetro común (u) que depende de la composición de la lista, la fase de revocación de un miembro de la lista, que comprende una etapa de modificación del parámetro común (u) que depende de la composición de la lista, para tener en cuenta la retirada del miembro de la lista, y la fase de actualización de certificados de los miembros de la lista que presenta una etapa de actualización del parámetro (u_i), propio de cada miembro de la lista, para tener en cuenta modificaciones de la composición de la lista.

3.- El método, según la reivindicación 1 o 2, caracterizado porque una firma propia a un miembro de la lista y que posee el certificado ($[A_i, e_i]$) comprende parámetros T_1, T_2, T_3, tales como:

$$T_1 = A_i b^{\omega} \pmod n,$$
$$T_2 = g^{\omega} \pmod n,$$
$$T_3 = g^{e_i} h^{\omega} \pmod n,$$

siendo ω un número elegido, de forma aleatoria, en el momento de la fase de firma (30), y siendo *b, g, h* y *n* parámetros generales de puesta en práctica de la firma de grupo, tales como los parámetros *b, g* y *h*, no se pueden deducir los unos de los otros mediante funciones de elevación de potencia entera módulo n, por lo que el número A_i y por lo tanto, la identidad del miembro de la lista que posee el certificado ($[A_i, e_i]$) no puede deducirse de una firma emitida por el miembro.

4.- El método, según una de las reivindicaciones 1 a 3, caracterizado porque el número m de una secuencia, utilizado para generar una firma de lista, se calcula en función de una fecha de inicio de secuencia.

5.- El método, según la reivindicación 4, caracterizado porque la función de cálculo del número de una secuencia es de la forma:

$$F(d) = (H(d))^2 \pmod n$$

en donde *H* es una función del resumen criptográfico resistente a las colisiones, *d* es la fecha de inicio de la secuencia y *n* es un parámetro general de la puesta en práctica de la firma de grupo.

6.- El método, según una de las reivindicaciones 1 a 5, caracterizado porque una firma (Sig_{liste}) emitida por un miembro de la lista contiene un parámetro (T_4) que se calcula en función del número de secuencia y de la clave privada (x_i) del miembro signatario.

7.- Método según la reivindicación 6,caracterizado porque el parámetro T_4 de una firma emitida por un miembro de la lista y que depende del número de secuencia m y de la clave privada x_i del miembro signatario se obtiene por la fórmula siguiente:

$$T_4 = m^{x_i} \pmod n$$

siendo n un parámetro general de puesta en práctica de la firma de grupo, y porque la firma comprende la prueba de que el parámetro T_4 fue calculado con la clave privada x_i del miembro de la lista que ha emitido la firma.

8.- Método de voto electrónico que comprende una fase de organización (50) de las elecciones, en cuyo transcurso una autoridad organizadora procede a la generación de parámetros necesarios para un escrutinio y atribuye a escrutadores de las claves que les permiten descifrar y comprobar las papeletas de voto, una fase de atribución de un derecho de firma a cada uno de los electores, una fase de voto (60) en cuyo transcurso los electores firman una papeleta de voto y una fase de recuento (70) en cuyo transcurso los escrutadores que comprueban las papeletas de voto y calculan el resultado del escrutinio en función del contenido de las papeletas de voto descifradas y válidas, caracterizado porque pone en práctica un método de firma de lista, según una de las reivindicaciones 1 a 7, para firmar las papeletas de voto, siendo cada elector registrado como miembro de una lista y siendo un número de secuencia m generado para el escrutinio, para detectar si un mismo elector ha emitido, o no, varias papeletas de voto para el escrutinio.

9.- Método según la reivindicación 8, caracterizado porque la fase de organización (50) comprende la entrega a cada escrutador de una clave pública y de una clave privada, porque las papeletas de voto (v_i) son cifradas (62) con la ayuda de una clave pública (Y) obtenida por el producto de las claves públicas (y_i) respectivas de todos los escrutadores y porque la clave privada (X) de descifrado correspondiente se obtienen calculando la suma de claves privadas (x_i) respectivas de todos los escrutadores.

10.- Método según la reivindicación 9, caracterizado porque el cifrado(62) de las papeletas de voto se efectúa con la ayuda de un algoritmo de cifrado probabilista.

11.- Método según una de las reivindicaciones 8 a 10, caracterizado porque las papeletas de voto emitidas por los electores se almacenan en una base de datos pública (4), porque el resultado de la comprobación y del recuento de cada papeleta de voto se guarda en la base de datos en asociación con la papeleta de voto y porque se publica la clave privada (X) de descifrado de las papeletas de voto.

12.- Calculador para la puesta en práctica de una firma de lista, que comprende medios para:

- generar parámetros de puesta en práctica de una firma electrónica anónima propia de los miembros de una lista, conteniendo los parámetros una clave privada y una clave pública correspondiente y

- transmitir a cada persona (2), a registrar en la lista, parámetros a utilizar por la persona a registrar para calcular (24) una clave privada (x_i) y un certificado ($[A_i, e_i]$) de miembro de la lista,

caracterizado porque comprende, además, medios para:

- generar un número de secuencia m a utilizar por los miembros de la lista para emitir una firma anónima propia de los miembros de la lista, una firma anónima (Sig_{liste}) emitida por un miembro de la lista que comprende un elemento de firma (T_4) que es común a todas las firmas emitidas por el mismo miembro de la lista con un mismo número de secuencia, y que contiene una prueba de que el número de secuencia m fue utilizado para generar la firma;

— retirar de la lista un miembro a revocar de la lista y actualizar los parámetros de puesta en práctica de la firma electrónica anónima propia de los miembros de la lista, para tener en cuenta la retirada del miembro de la lista y

- actualizar los certificados ($[A_i, e_i]$) de los miembros de la lista a cada modificación de la composición de la lista.

13.- Calculador para la puesta en práctica de un método de voto electrónico, que comprende medios para:

— generar, en el transcurso de una fase de organización de un escrutinio de los parámetros de puesta en práctica de una firma electrónica anónima propia de los miembros de una lista de electores, conteniendo los parámetros una clave privada y una clave pública correspondiente;

— atribuir a los escrutadores claves que les permitan descifrar y comprobar las papeletas de voto emitidas para el escrutinio y

— transmitir a cada miembro (2) de la lista de electores del escrutinio de los parámetros a utilizar por el elector para calcular (24) una clave privada (x_i) y un certificado ($[A_i, e_i]$) de miembro de la lista de electores del escrutinio,

caracterizado porque comprende, además, medios para:

- generar un número de secuencia m propio al escrutinio a utilizar por los miembros de la lista de electores para firmar una papeleta de voto, una firma (Sig_{liste}) de una papeleta de voto, que comprende un elemento de firma (T_4) que es común a todas las firmas emitidas con un mismo número de secuencia por un mismo miembro de la lista de electores del escrutinio y que contiene una prueba que el número de secuencia m fue utilizado para generar la firma;

- retirar de la lista un elector del escrutinio a revocar y actualizar los parámetros de puesta en práctica de la firma electrónica anónima propia a los miembros de la lista de electores del escrutinio, para tener en cuenta de la retirada del elector y

- actualizar los certificados ($[A_i, e_i]$) de los electores del escrutinio a cada modificación de la composición de la lista de los electores del escrutinio.

14 - Terminal (2) para emitir una firma de lista que comprende medios para:

- recibir parámetros de cálculo de una clave privada (x_i);

- calcular (24) la clave privada (x_i) con la ayuda de los parámetros recibidos y de parámetros elegidos de forma aleatoria;

— recibir (25) un certificado ($[A_i, e_i]$) de miembro de una lista;

- generar (35) una firma propia a los miembros de la lista, siendo esta firma constituida de modo que contenga una prueba de que el miembro de la lista que emitió la firma, conoce un certificado ($[A_i, e_i]$) de miembro de la lista y

— comprobar una firma emitida por un miembro de la lista aplicando un algoritmo predefinido para poner en evidencia la prueba de que la firma fue emitida por una persona en posesión de un certificado de miembro de la lista, caracterizado porque comprende, además, medios para:

— recibir un número de secuencia m a utilizar en una fase de firma (30)

- generar una firma (Sig_{liste}) calculando un elemento de firma (T_4) que es común a todas las firmas emitidas por un mismo miembro de la lista con un mismo número de secuencia y que contiene una prueba de que el número de secuencia m fue utilizado para generar la firma;

— comprobar la prueba de que el número de secuencia m fue utilizado para generar una firma y

— recibir un nuevo certificado ($[A_i, e_i]$) de miembro de la lista a cada modificación de la composición de la lista.

15.- Terminal (2) para emitir una firma de papeleta de voto a un escrutinio, que comprende medios para:

- recibir parámetros de cálculo de una clave privada (x_i);

— calcular (24)la clave privada (x_i) con la ayuda de los parámetros releídos y de parámetros elegidos de forma aleatoria;

— recibir (25) un certificado ($[A_i, e_i]$) de miembro de una lista de electores del escrutinio;

- generar (35) una firma de una papeleta de voto, estando esta firma constituida de modo que contenga una prueba de que el miembro de la lista, que ha emitido la firma, conoce un certificado ($[A_i, e_i]$) de miembro de la lista de electores y

- comprobar una firma de una papeleta de voto, emitida por un miembro de la lista de elector, aplicando un algoritmo predefinido para poner en evidencia la prueba de que la firma fue emitida por una persona en posesión de un certificado de miembro de la lista, caracterizado porque comprende, además, medios para:

- recibir un número de secuencia m a utilizar para firmar una papeleta de voto

— generar una firma (Sig_{liste})de una papeleta de voto calculando un elemento de firma (T_4) que es común a todas las firmas emitidas por un mismo miembro de la lista de electores con un mismo número de secuencia y que contiene una prueba de que el número de secuencia m fue utilizado para generar la firma;

— comprobar la prueba de que el número de secuencia m fue utilizado para generar una firma de una papeleta de voto y

- recibir un nuevo certificado ($[A_i, e_i]$) de miembro de la lista de electores a cada modificación de la composición de la lista de electores.

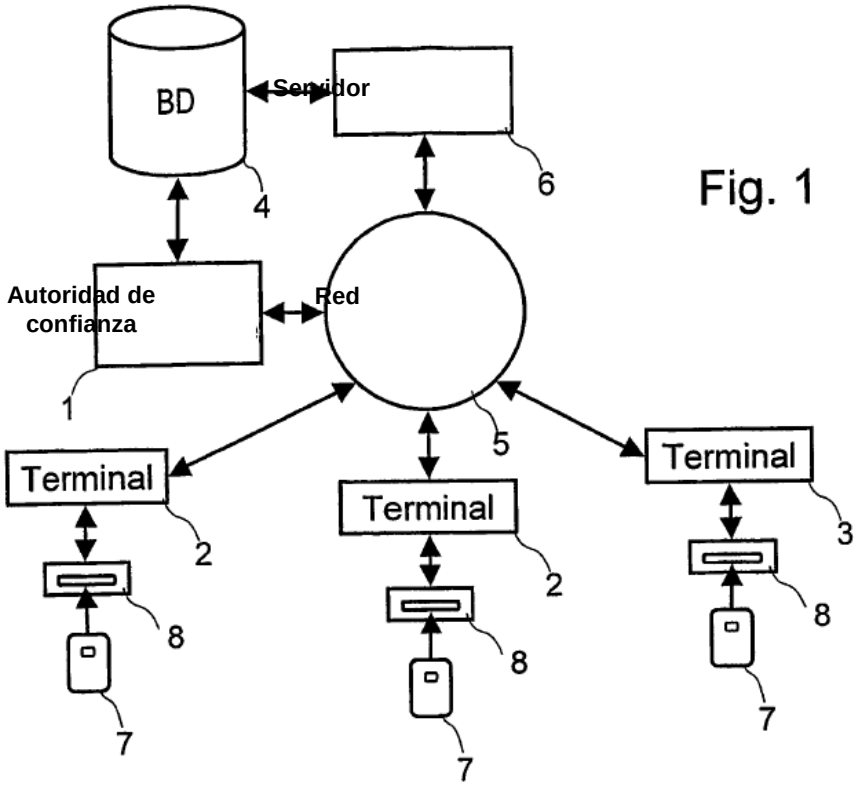

BD
Servidor
4
6
Autoridad de confianza
Red
1
5
Terminal
Terminal
Terminal
2
2
3
8
8
8
7
7
7

Fig. 1

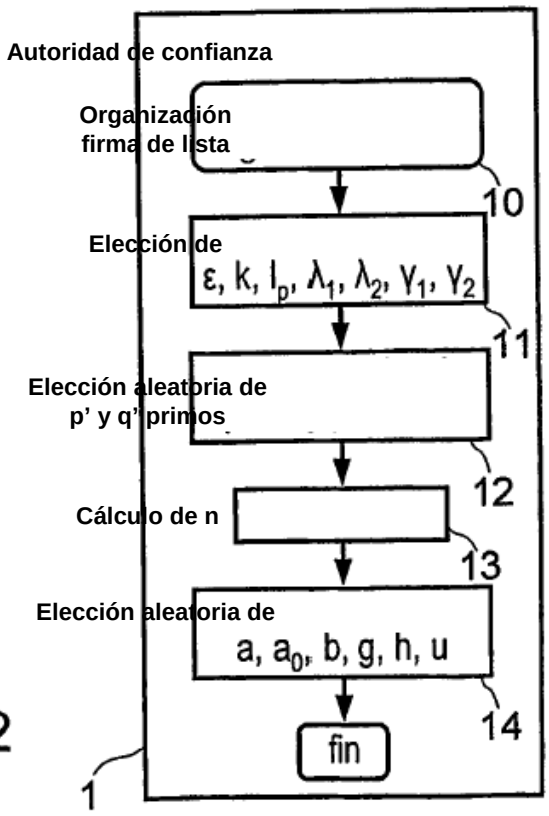
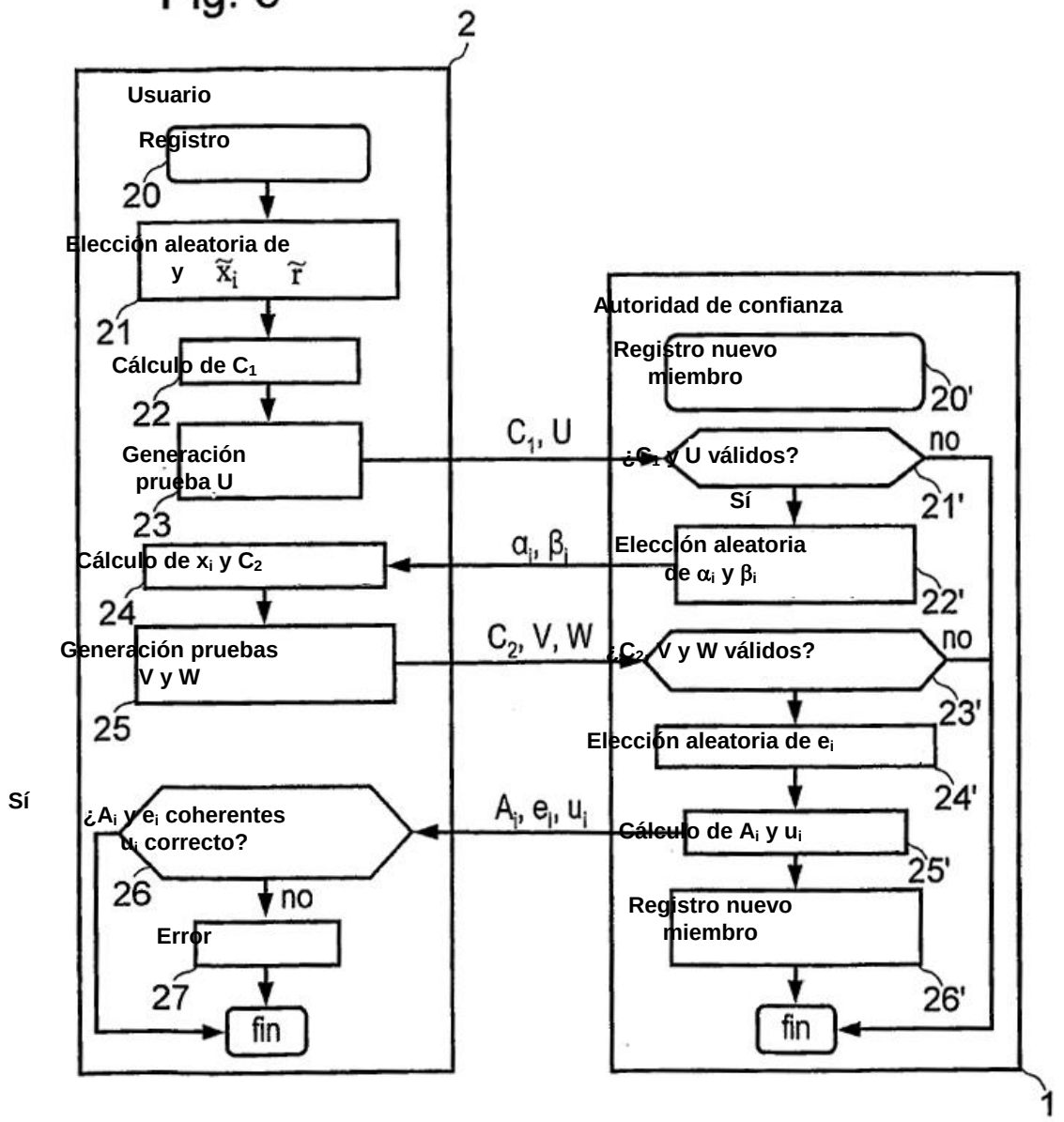

Autoridad de confianza
Organización firma de lista
10
Elección de
ε, k, l_p, λ_1, λ_2, γ_1, γ_2
11
Elección aleatoria de p' y q' primos
12
Cálculo de n
13
Elección aleatoria de
a, a_0, b, g, h, u
14
fin
1

Fig. 2

Fig. 3


2
Usuario
Registro
20
Elección aleatoria de
y $\tilde{x}_i$ $\tilde{r}$
21
Cálculo de C_1
22
Generación
prueba U
23
Cálculo de x_i y C_2
24
Generación pruebas
V y W
25
Sí
¿A_i y e_i coherentes
u_i correcto?
26
no
Error
27
fin
C_1, U
α_i, β_i
C_2, V, W
A_i, e_i, u_i
Autoridad de confianza
Registro nuevo
miembro
20'
¿C_1 y U válidos?
no
Sí
21'
Elección aleatoria
de α_i y β_i
22'
¿C_2 V y W válidos?
no
23'
Elección aleatoria de e_i
24'
Cálculo de A_i y u_i
25'
Registro nuevo
miembro
26'
fin
1

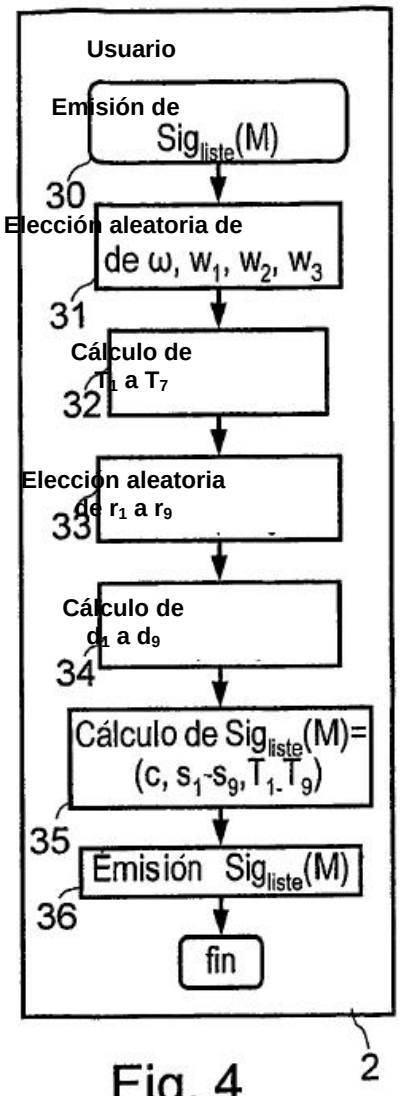


Fig. 4

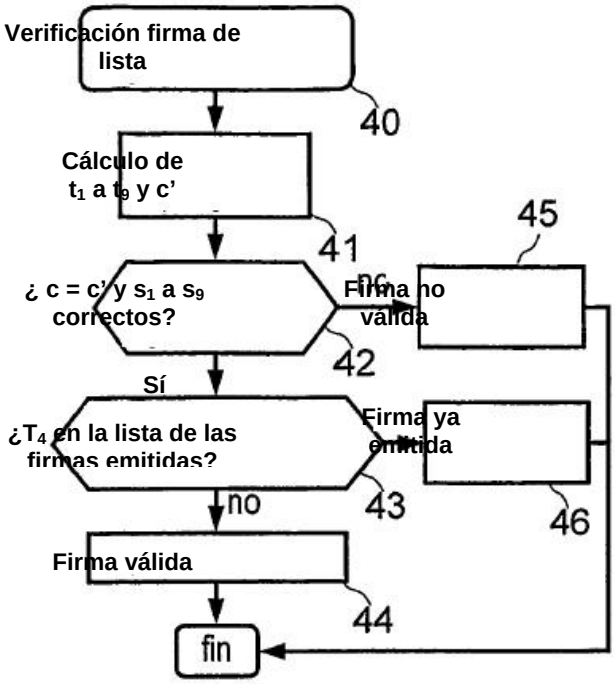


Fig. 5

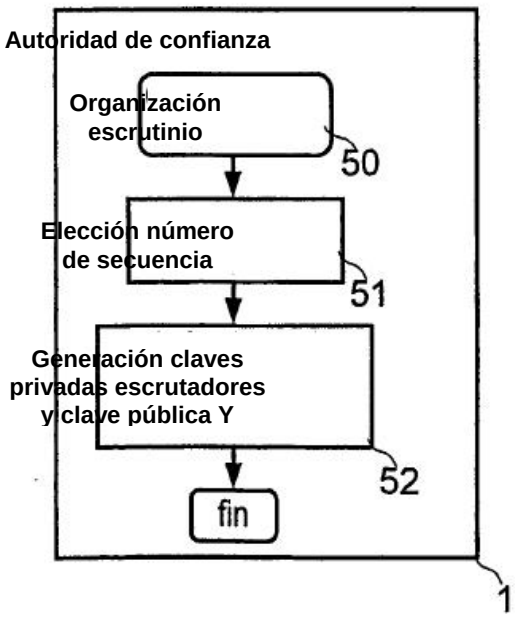


Fig. 6

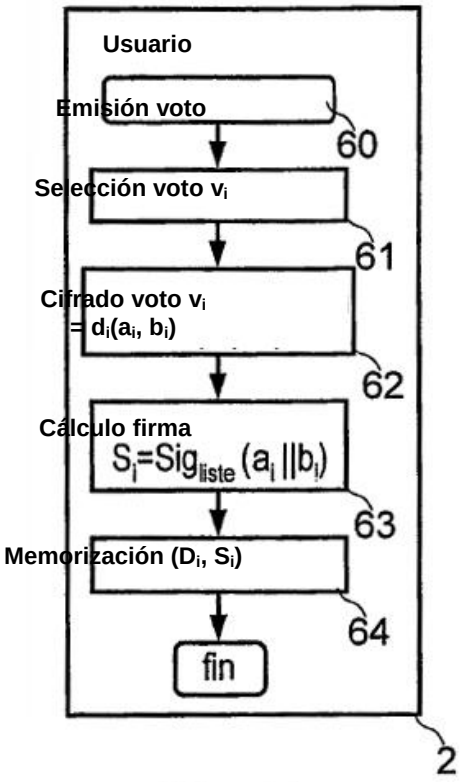

Usuario
Emisión voto
60
Selección voto v_i
61
Cifrado voto v_i = $d_i(a_i, b_i)$
62
Cálculo firma
$S_i=Sig_{liste}(a_i||b_i)$
63
Memorización (D_i, S_i)
64
fin
2

Fig. 7

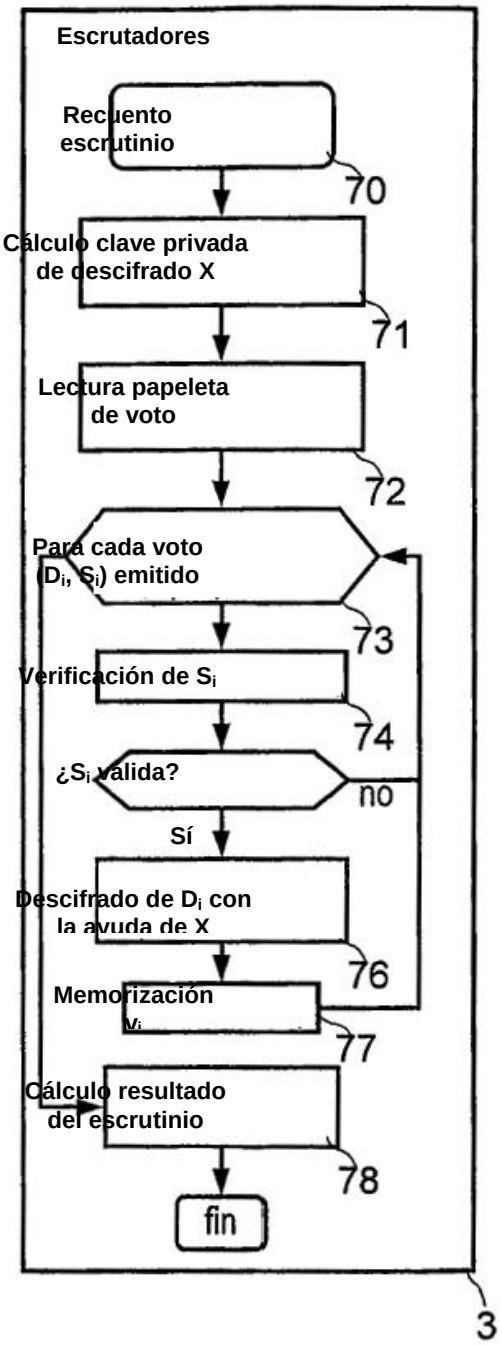

Escrutadores
Recuento escrutinio
70
Cálculo clave privada de descifrado X
71
Lectura papeleta de voto
72
Para cada voto (D_i, S_i) emitido
73
Verificación de S_i
74
¿S_i valida?
no
Sí
Descifrado de D_i con la ayuda de X
76
Memorización v_i
77
Cálculo resultado del escrutinio
78
fin
3

Fig. 8