(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 773 680**

(51) Int. CI.:

G07C 13/00 (2006.01)
H04L 9/30 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.03.2017 PCT/EP2017/054745**

(87) Fecha y número de publicación internacional: **05.10.2017 WO17167526**

(96) Fecha de presentación y número de la solicitud europea: **01.03.2017 E 17709398 (6)**

(97) Fecha y número de publicación de la concesión europea: **11.12.2019 EP 3411858**

(54) Título: **Procedimiento de voto con cadena de firmas**

(30) Prioridad:

29.03.2016 DE 102016205121

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.07.2020

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.0%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

GERKEN, STEFAN y
ECKELMANN-WENDT, UWE

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Procedimiento de voto con cadena de firmas

La presente invención hace referencia a un procedimiento de voto con cadena de firmas, así como a un dispositivo para la ejecución del procedimiento.

Los datos técnicos de seguridad deben haber sido calculados de manera redundante e idéntica múltiples veces, en donde cada tipo de cálculo también se denomina canal o replicante, o al menos deben haberse verificado de manera redundante para ser considerados técnicamente fiables. Esto es válido para todos los niveles de seguridad según las correspondientes normas (por ejemplo, las normas IEC61508, CENELEC EN50129) A partir del múltiple cálculo de una fecha mediante voto se obtiene un mensaje seguro desde el punto de vista de la técnica de señalización. En el voto, múltiples datos o mensajes entrantes son comparados entre sí por un votante y se genera una fecha "correcta". Un votante puede ejecutar, por ejemplo, una decisión por mayoría, es decir, cuando la mayoría de las entradas de un votante indican un determinado mensaje, entonces ese mensaje se emite. Hasta ahora, para el voto se ha utilizado un dispositivo especial con tecnología de señales segura o un componente con tecnología de señales segura. Sin embargo, sería más conveniente para el sistema completo si los votos también pudieran ser ejecutados en un dispositivo sin tecnología de señales segura, idealmente, en el mismo dispositivo que los mensajes de votos. Hasta el momento, sin embrago, al menos en los niveles de seguridad más altos, sólo se han utilizado hardware patentado para los votantes que no cumple con los estándares generales. Hasta ahora, no se han utilizado comercialmente hardware que no son seguros desde el punto de vista de la técnica de señalización.

La solicitud FR 2 926 911 A1 revela un método de voto electrónico certificado para la verificación del conteo del voto electrónico en la estación de voto e incluye la publicación de certificados anónimos mediante la presentación pública de la lista de votos según un sondeo para la estación de voto, en donde cada línea de la lista contiene un certificado. El método incluye la identificación anónima de un voto mediante la creación y la presentación de un código aleatorio a un votante antes del voto. Se obtiene una firma digital del voto mediante encriptación con la ayuda de una llave de firma privada al captar una cadena de caracteres que está conformada por el código y el voto. El certificado del voto se realiza mediante la presentación de un voto al votante después del voto. Los certificados anónimos se publican mostrando públicamente una lista de votos después de sondear una estación de voto, en donde cada línea de la lista contiene el certificado.

El objeto de la invención consiste en desarrollar un procedimiento de voto de mensajes, que cumpla con los requisitos de alta seguridad y se pueda ejecutar en hardware comercial.

El procedimiento de voto con cadena de firmas comprende fundamentalmente los siguientes pasos: En un primer paso a) se proporciona una pluralidad M de replicantes para la generación de M mensajes redundantes, en donde $M \geq 2$. En un paso b) se proporciona una pluralidad N de módulos de votantes con $N \geq 2$, en donde cada módulo de votantes presenta un votante para el voto de los mensajes redundantes, así como una unidad de cifrado con llave parcial privada para la firma de un mensaje. En un paso c) los mensajes redundantes de los replicantes se transfieren a cada módulo de votantes, de modo que el votante de cada módulo de votantes genera un mensaje de voto en base a los mensajes redundantes. En un paso d) se produce una primera firma del primer mensaje de voto a través del primer módulo de votantes con una primera llave parcial privada, cuando el primer votante genera un primer mensaje de voto. En un siguiente paso e) se transfiere una n-ésima firma y un n-ésimo mensaje de voto del n-ésimo módulo de votantes al (n+1)-ésimo módulo de votantes. En un siguiente paso f) se compara el mensaje de voto por el (n+1)-ésimo votante con el n-ésimo mensaje de voto y se crea una (n+1)-ésima firma sobre la n-ésima firma con una (n+1)-ésima llave parcial privada del (n+1)-ésimo módulo de votantes, cuando el primer mensaje de voto coincide con el (n+1)-ésimo mensaje de voto. En un siguiente paso g) se realizan los pasos e) y f) en secuencia ascendente para cada n con $1 \leq n \leq (N-1)$. En un siguiente paso h) la N-ésima firma y el N-ésimo mensaje de voto se transfiere a una unidad receptora. En un siguiente paso i) el N-ésimo mensaje de voto se acepta a través de una unidad receptora de cifrado, cuando la unidad receptora de cifrado verifica con éxito la N-ésima firma con una llave pública.

El procedimiento conforme a la invención combina el principio del voto con métodos criptográficos. Siempre es una condición para ello que un voto de una etapa sea exitoso y coincida con el resultado de voto de la etapa preliminar. Sin este requisito, no se consigue ninguna firma parcial mediante de una llave parcial. Pero, solamente con la presencia de todas las firmas, la llave pública "coincide" con la firma generada por las llaves parciales y el mensaje de voto es aceptado por la unidad receptora. En otras palabras, una unidad receptora es una unidad de verificación, un dispositivo de verificación o un receptor. Mediante el concepto de firma concatenada se crea un alto nivel de seguridad para el mensaje de voto. La presente invención también presenta la ventaja de que el procedimiento se puede realizar en un hardware sin tecnología de señales segura, como, por ejemplo, en Pc disponibles comercialmente.

Preferentemente, todas las llaves parciales privadas son diferentes entre sí.

Preferentemente, las firmas se conforman en un valor hash del mensaje. De esta manera, se reduce ventajosamente el volumen de datos de mensajes más extensos y el proceso de la firma concadenada se puede desarrollar más rápido.

Preferentemente, una llave privada se genera por la multiplicación de las llaves parciales privadas en la clase residual y la llave pública multiplicada con la llave parcial privada resultante se genera en la clase residual 1; en donde de esta manera se obtiene nuevamente el valor hash original o el mensaje original. Esta es una realización preferida y de desarrollo particularmente rápido de la firma. El valor hash original o el mensaje original puede ser verificado después por la unidad receptora.

Preferentemente, la llave privada se puede calcular comunicativamente a partir de las llaves parciales privadas. En otras palabras, esto significa que el orden de la firma no influye. Por lo tanto, en la medida que todos los módulos de votantes estén involucrados, la secuencia de los módulos de votantes a verificar es irrelevante.

De manera ventajosa, la transmisión del mensaje de voto del n-ésimo módulo de votantes al (n+1)-ésimo módulo de votantes coincide temporalmente con la transmisión de los mensajes redundantes (O1, O2, OM) de la pluralidad de replicantes (R1, R2, RM) al (n+1)-ésimo módulo de votantes; en donde $1 \leq n \leq (N-1)$. De esta manera se reduce la demora de la firma concatenada.

Preferentemente, cada votante está separado de los demás votantes. Esto significa que se utilizan las mismas técnicas que para segregar replicantes, o, en otras palabras, encapsularlos o aislarlos. De este modo, se logra la independencia de las rutas de cálculo. Un encapsulado adecuado de los módulos de votantes se puede obtener, por ejemplo, mediante emuladores de colores para SIL3 o SIL4, en donde SIL indica el nivel de integridad de seguridad. Esto también es una ventaja cuando se desea implementar el procedimiento en Pc disponibles comercialmente.

Los votantes se pueden configurar como votantes discriminantes o como votantes mayoritarios. Los votantes discriminantes sólo envían un mensaje de voto cuando todas las entradas coinciden. Los votos mayoritarios conforman una decisión mayoritaria, es decir, cuando la mayoría de los mensajes presentan una coincidencia, entonces se emite este mensaje.

Preferentemente, un votante no envía ningún mensaje, o envía un mensaje negativo, cuando no puede conformar un mensaje de voto.

Preferentemente, la transferencia de los mensajes de votos del n-ésimo módulo de votantes al (n+1)-ésimo módulo de votantes se desarrolla sin interrupciones, en donde $1 \leq n \leq (N-1)$. De esta manera, se reduce la duración de la firma.

Ventajosamente, cada mensaje redundante del respectivo replicante se puede identificar de manera técnicamente segura. Esto puede realizarse, por ejemplo, mediante una suma de verificación con identificación replicantes.

También se propone un dispositivo para la ejecución del procedimiento de voto con cadena de firmas. El dispositivo comprende una pluralidad M de replicantes para la generación de M mensajes redundantes con $M \geq 2$. Además, se proporciona una pluralidad N de módulos de votantes con $N \geq 2$, en donde cada módulo de votantes presenta un votante para el voto de los mensajes redundantes, así como una llave parcial privada para la firma de un mensaje; en donde las entradas de cada votante están conectadas con las salidas de cada replicante. La salida de cada n-ésimo módulo de votantes está conectada con la entrada de cada (n+1)-ésimo módulo de votantes para la transferencia de mensajes de votos y firmas; en donde $1 \leq n \leq (N-1)$ y está proporcionada una unidad receptora, la cual recibe la firma y el mensaje de voto enviados por el N-ésimo módulo de votantes y verifica la firma N-ésima con una llave pública.

Además, se propone un programa informático que permite a un dispositivo de procesamiento de datos que ejecute un procedimiento de voto con cadena de firmas después de haber sido cargado en los medios de almacenamiento del dispositivo de procesamiento de datos.

Además, se propone un medio de almacenamiento legible por computador, en el cual está guardado un programa informático que le permite a un dispositivo de procesamiento de datos que ejecute un procedimiento de voto con cadena de firmas después de haber sido cargado en el medio de almacenamiento del dispositivo de procesamiento de datos.

Las propiedades, características y ventajas de la presente invención, arriba mencionadas, así como la forma en la que las mismas se consiguen, se clarifican y deducen en relación con la siguiente descripción de los ejemplos de ejecución, los cuales se explican en detalle en relación con los dibujos. Las figuras muestran:

Figura 1: una representación del procedimiento de voto con cadena de firmas según una posible forma de ejecución.

Figura 2: una representación de un dispositivo de voto con cadena de firmas según una posible forma de ejecución.

En la figura 1 se muestra un procedimiento de voto con cadena de firmas según una posible forma de ejecución. Está proporcionada respectivamente una pluralidad M de replicantes R1, R2, RM para la generación de M mensajes redundantes, en donde M≥2. El contenido de estos mensajes redundantes O1, O2, OM es equivalente (son idénticos en su significado). Además, se proporciona una pluralidad N de módulos de votantes VM1, VM2, VMN, en donde cada módulo de votantes VM1, VM2, VMN presenta un votante V1, V2, VN para el voto de los mensajes redundantes O1, O2, OM, así como una unidad de cifrado K1, K2, KN con llave parcial privada PR1, PR2, PRN para la firma de un mensaje.

Los mensajes redundantes O1, O2, OM de los replicantes R1, R2, RM se transfieren a cada módulo de votantes VM1, VM2, VM3, de modo que el votante V1, V2, VN de cada módulo de votantes VM1, VM2, VMN genera un mensaje de voto en base a los mensajes redundantes. Esto se indica gráficamente, a modo de ejemplo, en la figura 1 mediante líneas verticales discontinuas en cada módulo de votantes VM1, VM2, VMN, a los cuales los mensajes redundantes O1, O2, OM apuntan respectivamente mediante las flechas representadas.

Entonces se produce una primera firma del primer mensaje de voto M1 a través del primer módulo de votantes VM1 con una primera llave parcial privada PR1, cuando el primer votante V1 genera un primer mensaje de voto M1. La primera firma se aplica allí a través del operador de llave o el valor de llave pri_1 de la primera llave parcial privada PR1 al mensaje de voto M1 o, alternativamente, a un valor hash del mensaje, que en la figura está representado con $pri_1 \otimes M1$. Esta primera firma se transfiere después con el primer mensaje de voto M1 al segundo módulo de votantes VM2. En este segundo módulo de votantes VM2 se produce ahora un segundo mensaje de voto M2 a través del segundo votante V2 en base a los mensajes redundantes O1, O2, OM de los replicantes R1, R2, RM. Este segundo mensaje de voto se compara con el primer mensaje de voto M1. Cuando hay coincidencia, entonces se produce una segunda firma mediante una segunda llave parcial privada PR2 en la primera firma, lo cual está representado mediante $pri_2 \otimes pri_1 \otimes M1$con la operación ⊗. Esta primera firma se transfiere después con el primer mensaje de voto M1 o bien con el segundo mensaje de voto M2. Ya que ambos mensajes de votos M1, M2 deben coincidir como requisito previo para la firma, es irrelevante cuál de ellos se reenvía. Esto se representa en la figura 1 mediante el símbolo lógico de contravalencia exclusivo V, que corresponde a "o uno...u otro". Por ejemplo, se puede utilizar el primer mensaje de voto M1 para la transferencia.

Este procedimiento se continúa ejecutando de esta forma para los demás módulos de votantes VM1, VM2, VMN. En general se puede decir que una n-ésima firma y un n-ésimo mensaje de voto del n-ésimo módulo de votantes se transfiere al (n+1)-ésimo módulo de votantes. Después, el mensaje de voto por el (n+1)-ésimo votante se compara con el n-ésimo mensaje de voto y se crea una (n+1)-ésima firma en la n-ésima firma con una (n+1)-ésima llave parcial privada del (n+1)-ésimo módulo de votantes, cuando el primer mensaje de voto coincide con el (n+1)-ésimo mensaje de voto. Esto se realiza en secuencia ascendente para cada n con $1 \leq n \leq (N-1)$.

Así, en el último paso se produce una N-ésima firma mediante una N-ésima llave parcial privada PRN en la (N+1)-ésima firma, lo cual en la figura 1 está representado mediante $pri_N \otimes ... \otimes pri_1 \otimes M1$ con la operación ⊗.

Después, la N-ésima firma y el N-ésimo mensaje de voto MN (o bien otro mensaje de voto idéntico) se transmite a una unidad receptora E. Allí, el N-ésimo mensaje de voto se acepta a través de una unidad receptora de cifrado EK, cuando la unidad receptora de cifrado EK verifica con éxito la N-ésima firma con una llave pública PU.

Este procedimiento se puede explicar matemáticamente a continuación. Una llave privada PR, a continuación indicada con pri, resulta como vínculo de la llave parcial privada PR1, PR2, PRN, indicada con prin con $1 \leq n \leq N$, mediante una operación ⊗, de modo que $pri_N \otimes ... \otimes pri_1 \equiv pri \bmod a^l$. En otras palabras, la llave privada PR no es prim, ya que la misma se puede presentar como vínculo de múltiples llaves parciales P1, P2, PN. La llave privada PR resulta entonces con la llave pública PU, aquí indicada como pub, vinculando el elemento neutral 1 en la clase residual, es decir, $pri \otimes pub \equiv 1 \bmod a^l$, en donde a es el número de posibles valores por señal, l es la longitud de señal subyacente, a^l representa el número de llaves diferentes entre sí y ≡ la congruencia. La llave privada PR y la llave pública son, por lo tanto, inversas modulares entre sí en lo que respecta a la operación ⊗. Por lo general, los procesadores funcionan en sistema binario, lo que corresponde a a=2 y es la variante preferida. La longitud de bit l se encuentra generalmente en 128 a 160 bits, aunque se pueden utilizar longitudes de bit más cortas o más largas y, por lo tanto, se pueden usar llaves más cortas y más largas.

En el caso de que faltara una firma de una clave parcial privada PR1, PR2, PRN, entonces, la unidad receptora E no podría recuperar el mensaje original. Mediante el concepto de firma concatenada se crea un alto nivel de seguridad para el mensaje de voto. El procedimiento se puede realizar en un hardware sin tecnología de señales segura, como, por ejemplo, en Pc disponibles comercialmente. Mediante el procedimiento conforme a la invención se combina el principio de voto con métodos criptográficos. Siempre es una condición para ello que un voto de una etapa sea exitoso y coincida con el resultado de voto de la etapa preliminar. Sin este requisito, no se consigue ninguna firma parcial mediante de una llave parcial. Pero, solamente con la presencia de todas las firmas, la llave

pública "coincide" con la firma generada por las llaves parciales y el mensaje es aceptado entonces por la unidad receptora.

Como vínculos $\otimes$, pueden ser consideradas diferentes operaciones apropiadas. Por ejemplo, también están incluidas las operaciones de matriz. Entonces, por ejemplo, el orden de las firmas es esencial y generalmente no se puede intercambiar. Además, todas las llaves parciales privadas PR1, PR2, PRN son diferentes entre sí. Preferentemente, las firmas se conforman en un valor hash del mensaje. De esta manera, se reduce ventajosamente el volumen de datos de mensajes más extensos y el proceso de la firma concatenada se puede desarrollar más rápido.

Aunque, preferentemente, una llave privada PR resulta por la multiplicación de las llaves parciales privadas PR1, PR2, PRN en la clase residual. La llave pública PU multiplicada por la clave privada resultante PR resulta en la clase residual 1, en donde, de esta manera se obtiene nuevamente el valor hash original o el mensaje original. Esta es una realización preferida y particularmente rápida de la firma. El valor hash original o el mensaje original puede ser verificado entonces por la unidad receptora E, por ejemplo, calculando el valor hash con la correspondiente función hash del mensaje de voto y comparándolo con el valor hash transferido después de la aplicación (multiplicación) de todas las llaves privadas parciales.

La llave privada PR se puede calcular comunicativamente a partir de las llaves parciales privadas PR1, PR2, PRN. Entonces, la secuencia de los módulos de voto VM1, VM2, VMN a verificar es irrelevante, siempre que estén involucrados al menos todos los módulos de voto VM1, VM2, VMN. Este es el caso, por ejemplo, en la multiplicación descrita anteriormente.

Además, adicionalmente también puede tener lugar una sincronización. Para un proceso de firma rápido, resulta útil, cuando la transmisión del mensaje de voto del n-ésimo módulo de votantes al (n+1)-ésimo módulo de votantes se sincroniza temporalmente con la transmisión de los mensajes redundantes (O1, O2, OM) de la pluralidad de replicantes (R1, R2, RM) al (n+1)-ésimo módulo de votantes; en donde $1 \leq n \leq (N-1)$. De esta manera se reduce la demora de la firma concatenada.

Cada votante V1, V2, VN está preferentemente separado de los demás votantes V1, V2, VN. Esto significa que aquí se utilizan las mismas técnicas que para segregar replicantes R1, R2, RM, o en otras palabras, encapsularlos o aislarlos. De esta manera se obtiene la independencia de las rutas de cálculo, con lo cual se reduce significativamente el riesgo de salidas de error idénticas. Un encapsulado adecuado de los módulos de votantes se puede obtener, por ejemplo, mediante emuladores de colores para SIL3 o SIL4, en donde SIL indica el nivel de integridad de seguridad. Esto también es una ventaja cuando se desea implementar el procedimiento en Pc disponibles comercialmente.

Los votantes V1, V2, VN se pueden configurar como votantes discriminantes o como votantes mayoritarios. Los votantes discriminantes sólo envían un mensaje de voto cuando todas las entradas coinciden. Los votos mayoritarios conforman una decisión mayoritaria, es decir, cuando la mayoría de los mensajes presentan una coincidencia, entonces se emite este mensaje. Cuando un votante V1, V2, VN no puede conformar un mensaje de voto, preferentemente, no envía ningún mensaje, o envía un mensaje negativo. Este sería el caso, por ejemplo, si, por ejemplo, un votante mayoritario recibe exactamente dos mensajes que se contradicen entre sí. En el caso de los votantes discriminantes, este también sería el caso si un mensaje de entrada difiere del resto. Preferentemente, la transferencia de los mensajes de votos del n-ésimo módulo de votantes al (n+1)-ésimo módulo de votantes se desarrolla sin interrupciones, en donde $1 \leq n \leq (N-1)$.

Ventajosamente, cada mensaje redundante O1, O2, OM del respectivo replicante R1, R2, RM se puede identificar de manera técnicamente segura. Esto se puede realizar, por ejemplo, mediante una suma de verificación con identificación replicantes. De esta manera se puede identificar, por ejemplo, un comportamiento incorrecto de un replicante R1, R2, RM.

En la figura 2 está representado esquemáticamente, a modo de ejemplo, un dispositivo de voto con cadena de firmas. Allí, se pone a disposición una pluralidad M de replicantes R1, R2, RM para la generación de M mensajes redundantes con $M \geq 2$. A ello se suma una pluralidad N de módulos de votantes VM1, VM2, VMN con $N \geq 2$. Allí, cada módulo de votantes VM1,VM2,VMN está provisto de un votante V1, V2,VN para el voto de los mensajes redundantes O1,O2,OM de los replicantes redundantes R1,R2, RM, así como una unidad de cifrado K1,K2,KN con una llave parcial privada PR1,PR2,PRN para la firma de un mensaje; en donde las entradas de cada módulo de votantes VM1,VM2,VMN están conectadas con las salidas de cada replicante R1,R2,RM. La salida de cada n-ésimo módulo de votantes está conectada con la entrada de cada (n+1)-ésimo módulo de votantes para la transferencia de mensajes de votos y firmas; en donde $1 \leq n \leq (N-1)$ y está proporcionada una unidad receptora E, la cual recibe la firma y el mensaje de voto enviados por el N-ésimo módulo de votantes VMN y verifica la firma N-ésima con una llave pública PU.

En resumen, se propone un procedimiento de voto que se combina con métodos criptográficos (asimétricos). Allí, se utilizan cadena de firmas en múltiples etapas. Siempre es una condición para ello que un voto de una etapa sea exitoso y coincida con el resultado de voto de la etapa preliminar. Sin este requisito, no se consigue ninguna firma parcial mediante de una llave parcial. Pero, solamente con la presencia de todas las firmas parciales, la llave pública "coincide" con la firma generada por las llaves parciales y el mensaje de voto es aceptado por la unidad receptora. Mediante el concepto de firma concatenada se crea un alto nivel de seguridad para el mensaje de voto. De esta manera, el procedimiento se puede realizar en un hardware sin tecnología de señales segura, como, por ejemplo, en PC´s disponibles comercialmente.

Aunque la invención ha sido descrita e ilustrada en detalle mediante ejemplos de ejecución preferidos, dicha invención no está limitada por los ejemplos revelados y, sin abandonar el alcance de la presente invención, el especialista puede derivar de aquí otras variaciones.

Lista de símbolos de referencia

R1, R2, RM Replicantes

O1, O2, OM Mensajes redundantes

VM1, VM2, VMN Módulo de votantes

K1, K2, KN Unidad de cifrado

PR1, PR2, PRN Llave parcial privada

PR Llave privada

E Unidad receptora

EK Unidad receptora de cifrado

PU Llave pública

M1, M2, MN Mensaje de voto

REIVINDICACIONES

1. Procedimiento de voto con cadena de firmas que comprende los siguientes pasos:

a) provisión de una pluralidad M de replicantes (R1, R2, RM) para la generación de M mensajes redundantes (O1, O2, OM) con M≥2;

b) provisión de una pluralidad N de módulos de votantes (VM1, VM2, VMN) con N≥2, en donde cada módulo de votantes (VM1, VM2, VMN) presenta un votante (V1, V2, VN) para el voto de los mensajes redundantes, así como una unidad de cifrado (K1, K2, KN) con llave parcial privada (PR1, PR2, PRN) para la firma de un mensaje;

c) transferencia de los mensajes redundantes (O1, O2, OM) de los replicantes (R1, R2, RM) a cada módulo de votantes (VM1, VM2, VMN), de modo que el votante (V1, V2, VN) de cada módulo de votantes (VM1, VM2, VMN) genera un mensaje de voto (M1, M2, MN) en base a los mensajes redundantes (O1,O2,OM);

d) producción de una primera firma del primer mensaje de voto a través del primer módulo de votantes (VM1) con una primera llave parcial privada (PR1), cuando el primer votante (V1) genera un primer mensaje de voto;

e) transferencia de una n-ésima firma y un n-ésimo mensaje de voto del n-ésimo módulo de votantes al (n+1)-ésimo módulo de votantes;

f) comparación del mensaje de voto por el (n+1)-ésimo votante con el n-ésimo mensaje de voto y creación de una (n+1)-ésima firma sobre la n-ésima firma con una (n+1)-ésima llave parcial privada del (n+1)-ésimo módulo de votantes, cuando el primer mensaje de voto coincide con el (n+1)-ésimo mensaje de voto;

g) ejecución de los pasos e) y f) en secuencia ascendente para cada n con 1≤n≤(N-1);

h) transferencia de la N-ésima firma y del N-ésimo mensaje de voto a una unidad receptora (E);

i) aceptación del N-ésimo mensaje de voto a través de una unidad receptora de cifrado (EK), cuando la unidad receptora de cifrado (EK) verifica con éxito la N-ésima firma con una llave pública (PU).

2. Procedimiento según la reivindicación 1; en donde todas las llaves parciales privadas (PR1, PR2, PRN) son diferentes entre sí.

3. Procedimiento según una de las reivindicaciones precedentes, en donde las firmas se conforman en un valor hash del mensaje.

4. Procedimiento según una de las reivindicaciones precedentes, en donde una llave privada (PR) se genera por la multiplicación de las llaves parciales privadas (PR1, PR2, PRN) en la clase residual y la llave pública (PU) multiplicada con la llave parcial privada resultante se genera en la clase residual 1; en donde de esta manera se obtiene nuevamente el valor hash original o el mensaje original.

5. Procedimiento según una de las reivindicaciones precedentes, en donde una llave privada (PR) se puede calcular comunicativamente a partir de las llaves parciales privadas (PR1, PR2, PRN).

6. Procedimiento según una de las reivindicaciones precedentes, en donde la transmisión del mensaje de voto del n-ésimo módulo de votantes al (n+1)-ésimo módulo de votantes coincide temporalmente con la transmisión de los mensajes redundante (O1, O2, OM) de la pluralidad de replicantes (R1, R2, RM) al (n+1)-ésimo módulo de votantes; en donde 1≤n≤(N-1).

7. Procedimiento según una de las reivindicaciones precedentes, en donde cada votante (V1, V2, VN) se separa de los demás votantes (V1, V2, VN).

8. Procedimiento según una de las reivindicaciones precedentes, en donde los votantes (V1, V2, VN) se configuran como votantes discriminantes o como votantes mayoritarios.

9. Procedimiento según una de las reivindicaciones precedentes, en donde cada votante (V1, V2, VN) genera un mensaje negativo o no genera ningún mensaje, cuando no puede conformar un mensaje de voto.

10. Procedimiento según una de las reivindicaciones precedentes, en donde la transferencia de los mensajes de votos del n-ésimo módulo de votantes al (n+1)-ésimo módulo de votantes se desarrolla sin interrupciones, en donde 1≤n≤(N-1).

11. Procedimiento según una de las reivindicaciones precedentes, en donde en cada mensaje redundante (O1, O2, ON), el respectivo replicante (R1, R2, RM) se identifica de manera técnicamente segura.

12. Sistema para la ejecución del procedimiento de voto con cadena de firmas según una de las reivindicaciones 1-11; en donde el sistema comprende:

- una pluralidad M de replicantes (R1, R2, RM) para la generación de M mensajes redundantes con M≥2;

- una pluralidad N de módulos de votantes (VM1,VM2,VMN) con N≥2, en donde cada módulo de votantes (VM1,VM2,VMN) presenta un votante (V1, V2,VN) para el voto de los mensajes redundantes, así como una llave parcial privada (PR1,PR2,PRN) para la firma de un mensaje; en donde las entradas de cada votante (V1,V2,VN) están conectadas con las salidas de cada replicante (R1,R2,RM);

- la salida de cada n-ésimo módulo de votantes está conectada con la entrada de cada (n+1)-ésimo módulo de votantes para la transferencia de mensajes de votos y firmas; en donde 1≤n≤(N-1) y está proporcionada una unidad receptora (E), la cual recibe la firma y el mensaje de voto enviados por el N-ésimo módulo de votantes (VMN) y verifica la firma N-ésima con una llave pública (PU).

13. Programa informático que comprende instrucciones, las cuales, cuando el programa se ejecuta por los replicantes (R1, R2, RN), los módulos de votantes (VM1, VM2, VMN) y la unidad receptora (E) del sistema según la reivindicación independiente 12, los replicantes (R1, R2, RN), los módulos de votantes (VM1, VN2, VMN) y la unidad receptora (E) disponen realizar los pasos de un procedimiento de voto con cadena de firmas según una de las reivindicaciones 1-11.

14. Medio de almacenamiento legible por computador que comprende instrucciones, las cuales, cuando se ejecutan por los replicantes (R1, R2, RN), los módulos de votantes (VM1, VM2, VMN) y la unidad receptora (E) del sistema según la reivindicación independiente 12, los replicantes (R1, R2, RN), los módulos de votantes (VM1, VM2, VMN) y la unidad receptora (E) disponen realizar los pasos de un procedimiento de voto con cadena de firmas según una de las reivindicaciones 1-11.

FIG 1

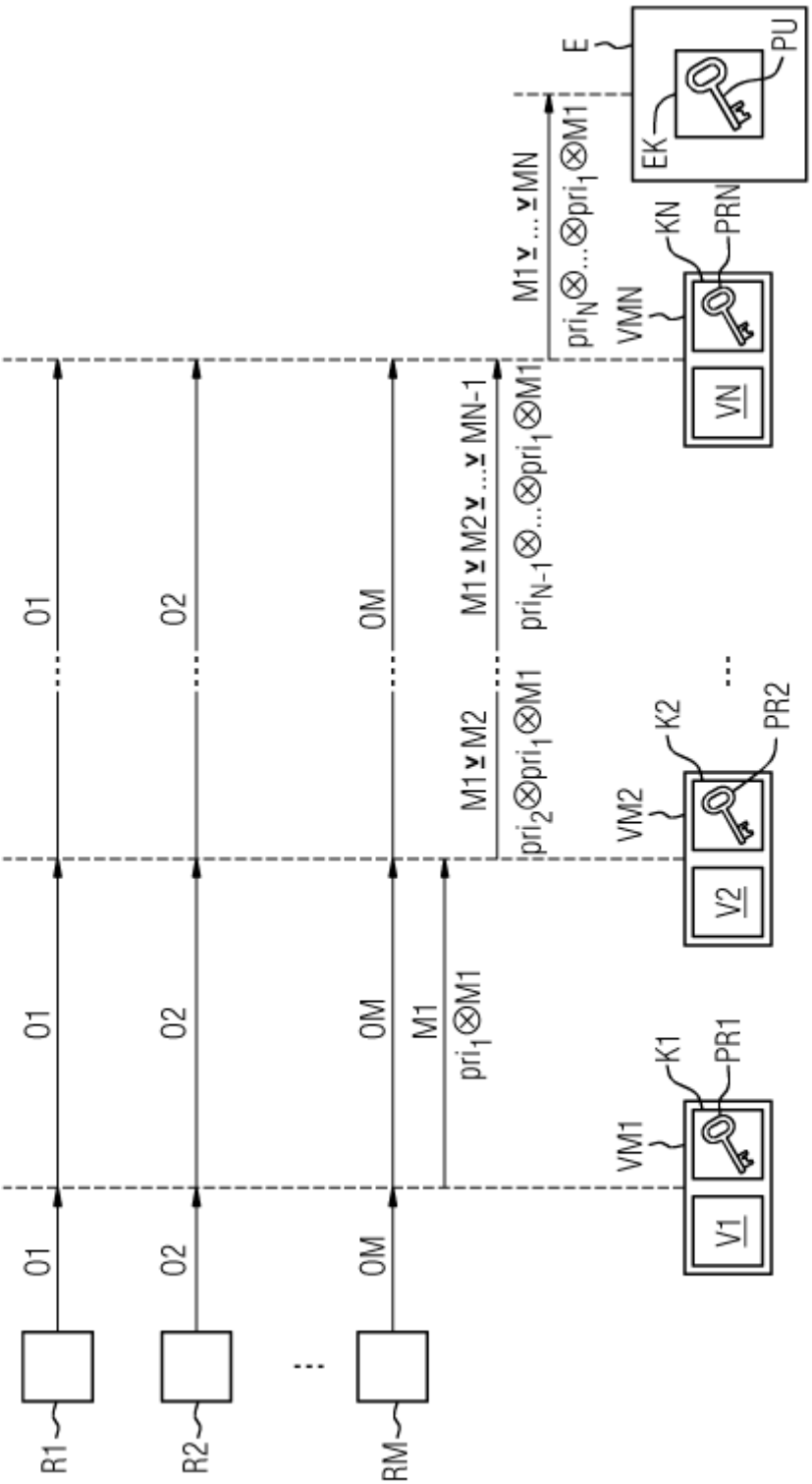
R1
R2
RM
O1
O2
OM
M1
pri1⊗M1
M1≥M2
pri2⊗pri1⊗M1
M1≥M2≥...≥MN-1
priN-1⊗...⊗pri1⊗M1
M1≥...≥MN
priN⊗...⊗pri1⊗M1
V1
V2
VN
VM1
VM2
VMN
K1
K2
KN
PR1
PR2
PRN
E
EK
PU

FIG 2