

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 728 313**

51 Int. Cl.:

**G07C 13/00** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **23.12.2008 PCT/IB2008/055521**

87 Fecha y número de publicación internacional: **01.07.2010 WO10073065**

96 Fecha de presentación y número de la solicitud europea: **23.12.2008 E 08875902 (2)**

97 Fecha y número de publicación de la concesión europea: **13.02.2019 EP 2382606**

54 Título: **Método de votación electrónica verificable**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:  
**23.10.2019**

73 Titular/es:

**TUBITAK (100.0%)  
Ataturk Bulvari, No 221, Kavaklidere  
06100 Ankara, TR**

72 Inventor/es:

**TIRYAKIOGLU, FATIH**

74 Agente/Representante:

**ELZABURU, S.L.P**

ES 2 728 313 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Método de votación electrónica verificable

### Descripción

#### Antecedentes

5 En los sistemas de votación electrónica resulta difícil proporcionar transparencia y anonimato. El uso de evidencias por escrito para la verificación parece ser igual que los métodos de votación típicos basados en papel, y no resuelve completamente el problema de verificación. En el documento de la técnica anterior US 2008/0135632 A1 se dan a conocer sistemas de votación del tipo mencionado.

10 Los votantes desean sistemas de votación electrónica transparentes. Sin embargo, esto no debería dar como resultado la compra de votos. Los métodos de votación electrónica deberían ser, también, cómodos para el usuario y fáciles de entender. Para los sistemas de votación electrónica venideros se requieren métodos de votación electrónica seguros, transparentes, verificables por el votante y basados en el anonimato.

#### Breve descripción de la invención

15 La presente invención definida en el método de la reivindicación independiente 1 permite que un votante verifique que los votos emitidos por el mismo se contaron correctamente al mismo tiempo que manteniendo el anonimato del voto. Se logra un equilibrio entre el anonimato y la transparencia de tal manera que los votantes disponen de pruebas que demuestran que los votos emitidos por ellos se contaron correctamente, pero las mismas pruebas carecen de significado para los otros. De esta manera, la transparencia triunfa sin invadir la privacidad del votante. Mientras los votantes emiten sus votos, por ejemplo en una máquina de votación, se requiere que un testigo verifique que el voto es contado de manera correcta. El testigo que valida la privacidad del votante se implementa usando la superioridad de los votantes sobre el sistema de votación. Este punto fuerte se usa para resolver el problema de la transparencia-anonimato: el sistema de votación no puede anticipar el siguiente paso del votante, y, cuando se revelan todos los pasos, al sistema no se le permite volver atrás. Los votantes presentan una opción aleatoria de entre un conjunto predeterminado de opciones aleatorias junto con cada opción de voto en el proceso de votación, y los mismos esperan una salida de un algoritmo como prueba de inclusión de las opciones de voto y las opciones aleatorias de las opciones de voto. Después de recibir la salida del algoritmo, presentan todas las opciones aleatorias de cada opción posible, y obtienen las opciones aleatorias del sistema de votación cuando han realizado la presentación. Puesto que el sistema de votación no puede conocer las opciones aleatorias de las otras opciones posibles, un posible código maligno en el sistema no se atreverá a cambiar las opciones de voto del votante. Si se atreve a ello y las opciones aleatorias de las opciones de voto no deseadas que selecciona no son como las opciones aleatorias de la opción de voto no deseada introducida después de recibir la salida del algoritmo por parte del votante, entonces esta modificación ilegal queda al descubierto. La posibilidad de descubrimiento se incrementa exponencialmente a medida que aumentan los votos modificados ilegales del sistema de votación. La salida del algoritmo es una salida de un algoritmo criptográfico que obtiene entradas que comprenden opciones de voto y opciones aleatorias de las opciones de voto y que hace uso de un secreto. Las opciones de voto de los votantes no se pueden calcular usando la salida del algoritmo sin conocer el secreto. El secreto puede ser un texto de entrada, la clave del algoritmo, o una combinación de los mismos. Como secreto se usa preferentemente la clave debido a su fortaleza contra ataques de fuerza bruta.

40 La salida del algoritmo y las opciones aleatorias de posibles opciones cogidas por el votante durante la emisión del voto también se hacen públicas para una futura verificación. El votante compara su salida del algoritmo y sus opciones aleatorias de las posibles opciones con las que se han hecho públicas, y si son iguales garantiza el recuento correcto de su voto. El centro de votación verifica y evalúa los votos usando parámetros públicos que comprenden la salida del algoritmo y opciones aleatorias de posibles opciones y el secreto. Si hubiera alguno, el centro de votación descubre los procesos ilegales. Junto al centro de votación, para la verificación de los resultados de la votación se puede usar un tercero de confianza que obtiene secretos del centro de votación.

#### Breve descripción de los dibujos

La FIG. 1 representa un diagrama de bloques de un sistema de votación que puede implementar el método de votación.

La FIG. 2 representa el diagrama de flujo del método de votación.

50 La FIG. 3 representa una interfaz de usuario en la cual un votante puede introducir opciones de votación y las opciones aleatorias de las opciones de votación.

La FIG. 4 representa un papel óptico que se puede usar para introducir opciones aleatorias de todas las opciones posibles en el sistema de votación.

La FIG. 5 representa un papel que puede ser recibido por el votante para la verificación de votantes.

La FIG. 6 representa una tabla de consulta en la máquina de votación, que comprende textos de verificación de los votantes.

**Descripción detallada**

5 La presente invención permite que un votante verifique que los votos emitidos por el mismo se contaron correctamente al mismo tiempo que manteniendo el anonimato del voto. El sistema 5 se puede implementar tal como se muestra en la FIG. 1. El sistema 5 incluye máquinas 10 de votación que están situadas en circunscripciones electorales. Aunque, en la FIG. 1, hay tres máquinas de votación, se puede proporcionar un número cualquiera de máquinas de votación. Cada máquina de votación comprende una interfaz hombre-máquina 15, una unidad 20 de procesado, y bases de datos locales 25 y 30. La interfaz hombre-máquina 15 proporciona comunicación y transferencia de datos con el entorno. La unidad 20 de procesado es, en general, responsable de ejecutar el método de votación electrónica y, específicamente, ejecuta un algoritmo que usa el secreto S. La base 25 de datos local contiene textos de verificación de votantes. La base 30 de datos local contiene información de candidatos que se visualizará en la interfaz hombre-máquina. Antes de las elecciones, se carga información de candidatos en cada base 30 de datos local de las máquinas 10 de votación de manera independiente con respecto a 15 una base 40 de datos central del centro 35 de votación por parte de una autoridad central.

La FIG. 2 es un diagrama de flujo que muestra el método de votación electrónica. El método se puede implementar en un sistema 5 mostrado en la FIG. 1. El método comienza en la etapa 100. A un votante se le autoriza a emitir el voto en una máquina 10 de votación. En la etapa 105, el votante se enfrenta con una interfaz de usuario para seleccionar opciones de voto en la interfaz hombre-máquina 15. La interfaz de usuario se puede implementar como 20 la referencia 300 mostrada en la FIG. 3. En la interfaz 300 de usuario, se presentan todos los candidatos u opciones 310. Cada candidato u opción tiene un conjunto de opciones aleatorias 320 cuyo número y designaciones son determinados por una autoridad electoral. No más tarde de la etapa 120, preferentemente antes del proceso de votación por comodidad, el votante debe haber determinado opciones aleatorias de cada candidato u opción excepto opciones aleatorias de las opciones de voto. Las opciones aleatorias de las opciones de voto se deben haber determinado al llegar a esta etapa. La determinación de las opciones aleatorias del votante se puede realizar en un papel 400 como en la FIG. 4. En la FIG. 4, las opciones 410 se muestran en la primera columna, las opciones aleatorias 420 de las opciones 410 se muestran en filas para cada opción. Las opciones aleatorias del votante en la FIG. 4, por ejemplo, son rojo, verde, verde, rojo, azul, verde, para la opción de alcalde, y verde, azul para la opción de sí/no, respectivamente. En la interfaz 300 de usuario de la FIG. 3, el votante selecciona opciones de voto junto con opciones aleatorias de las opciones de voto que se determinan con anterioridad a ello. Por ejemplo, si se selecciona "Mehmet Camlibel" y "Sí" tal como se muestra en la FIG. 3, introduce también "verde" para "Mehmet Camlibel" y "verde" para "Sí" debido a la determinación previa mostrada en la FIG. 4. Tras la selección de las opciones de voto y las opciones aleatorias de estas, emite el voto. La emisión del voto se puede implementar por medio de un botón Emisión tal como se muestra en la FIG. 3. En la etapa 110, la máquina de votación, que recibe 35 opciones de voto del votante y opciones aleatorias de las opciones de voto del votante, procesa un algoritmo criptográfico usando un secreto.

La entrada del algoritmo comprende opciones de voto del votante y opciones aleatorias de las opciones de voto del votante, y el algoritmo produce la salida. El número de proceso/procesos puede ser uno o mayor que uno. Por ejemplo, puede haber un proceso que reciba "Mehmet Camlibel", "verde", "Sí", "verde" o dos procesos, uno de ellos que recibe "Mehmet Camlibel", "verde" y el otro que recibe "Sí", "verde", etcétera. Los procesos, al ser más de uno, pueden ser independientes o estar en cascada uno con respecto al otro cuando la salida de uno de ellos se introduce en el otro. En todas las condiciones, se garantiza la introducción de todas las opciones de voto y las opciones aleatorias de las opciones de voto y la recepción de una salida independiente del número de proceso/procesos y la salida/salidas. Lo importante aquí es que todas las opciones de voto y las opciones aleatorias de las opciones de voto se deben poder anticipar o determinar usando salida/salidas de algoritmo y los otros parámetros de entrada conocidos en caso de que se conozca el secreto. Junto a estos, las opciones de voto y las opciones aleatorias se pueden simbolizar con diferentes elementos cuando se introducen en el algoritmo. Por ejemplo, puede realizarse una enumeración de las opciones de voto y las opciones aleatorias. Sin embargo, la regla de la sustitución debe ser pública. 45

50 La entrada del algoritmo puede incluir una id determinada por el votante, por la máquina de votación o por ambos si se desea un proceso de verificación cómodo para el usuario en la etapa de verificación. La entrada del algoritmo también puede incluir una id de la máquina de votación que garantice salidas de algoritmo variables en máquinas de votación. La entrada del algoritmo puede incluir cualesquiera datos opcionales siempre que se garantice que, en los parámetros de entrada, están las opciones de voto del votante y las opciones aleatorias de las opciones de voto del votante. 55

El algoritmo hace uso de un secreto en el procesado. El secreto puede ser una clave, un texto introducido en el algoritmo o el propio algoritmo. Es, preferentemente, una clave debido a su fortaleza contra ataques de fuerza bruta que intentan determinar opciones de voto usando salida/salidas del algoritmo y los otros parámetros de entrada conocidos. Lo importante es que las opciones de voto y las opciones aleatorias de las opciones de voto no se pueden determinar usando solamente el algoritmo, salidas del algoritmo y los otros parámetros conocidos, sino que se requiere, también, un secreto. 60

En la etapa 115, el votante recibe la salida del algoritmo y se asegura de que no cambie en las etapas venideras. Después de recibir la salida/salidas del algoritmo, pero antes de eso, en la etapa 120, el votante introduce todas las opciones aleatorias de todas las opciones posibles del sistema de votación. Esta entrada se puede realizar introduciendo un papel óptico 400 de la FIG. 4 en un escáner óptico de la máquina de votación. A continuación, en la etapa 125, el votante recibe opciones aleatorias de todas las opciones posibles que se acaban de introducir. Esta recepción junto con la salida del algoritmo, recibida en la etapa 115, se puede denominar texto de verificación del votante. El texto de verificación y los otros parámetros opcionales son proporcionados al votante para su futura verificación por el mismo. Se le pueden proporcionar al votante en un papel 500 de la FIG. 5. En la FIG. 5, se muestran la salida 510 del algoritmo, las opciones aleatorias 520 junto con parámetros opcionales, los cuales son la id 530 de votante y la id 540 de la máquina de votación. En la etapa 130, el votante compara las opciones aleatorias introducidas y recibidas. En la etapa 135, si son iguales, el mismo da su aprobación a la votación. Si no son iguales, rechaza la votación, y el proceso de votación acaba con un fallo. El votante informa a la autoridad de la incompatibilidad mostrándole su recibo. En la etapa 140, si se ha dado la aprobación, todo lo recibido se registra en la base de datos local de la máquina de votación, y la emisión del voto finaliza exitosamente para el votante. El votante coge también todos los recibos, que pueden ser como el papel 500 de la FIG. 5. Junto a estos, en la etapa 120, si se introducen nuevamente las opciones aleatorias de las opciones de voto, lo cual es habitual en la implementación con papel óptico, el proceso de votación puede finalizar con un fallo o puede continuar con el flujo normal en función de la decisión de la autoridad electoral sobre la implementación del método. Si el método se implementa como el proceso de votación que finaliza con fallo, cuando se produce la incompatibilidad en la etapa 120, es decir, las opciones aleatorias de las opciones de voto introducidas en la interfaz 300 de usuario de la FIG. 3 en la etapa 105 no concuerdan con las opciones aleatorias de las opciones de voto del papel 400 de la FIG. 4 en la etapa 120, la interfaz de votación avisa al votante de esta incompatibilidad. Si el votante acepta la incompatibilidad, la emisión del voto puede ser todavía válida, pero debe aparecer una señal de incompatibilidad, aunque no detallada como qué es lo que no concuerda con qué, en el texto de verificación que es recibido por el votante y almacenado en la base de datos local. Si no acepta la incompatibilidad, la emisión del voto finaliza con un fallo. En un fallo, todo el proceso de votación debe iniciarse desde el mismo comienzo debido a la revelación de las opciones aleatorias.

Este proceso se repite para todos los votantes durante las elecciones. Después de que hayan terminado las elecciones, los textos de verificación y los otros parámetros opcionales de todos los votantes están en la base 25 de datos local de la FIG. 1. La base de datos local se puede implementar en forma de la tabla 600 mostrada en la FIG. 6. En la FIG. 6, cada fila 610 contiene información relacionada con un votante. La secuencia de los votantes es, preferentemente, aleatoria, y la tabla no contiene, preferentemente, la hora de la votación e información adicional que amenace el anonimato del votante en caso de que se requiera un grado máximo de anonimato del voto-votante.

Después de que hayan terminado las elecciones, los datos que están en las bases de datos locales de las máquinas de votación se transfieren a la base 40 de datos central del centro 35 de votación de la FIG. 1. La transferencia de la información puede ser en línea o fuera de línea. Para mejorar la seguridad, los datos se copian, preferentemente, desde la base de datos local a unos medios de almacenamiento fuera de línea, a continuación los datos se pueden transferir al centro de votación en línea. Esto garantiza que no se saque ninguna información intencionada o no intencionada que amenace el anonimato del voto, de la máquina de votación. La publicación de la base de datos de cada máquina de votación puede ser realizada por cada máquina de votación localmente, por el centro de votación globalmente después de la transferencia, o tanto local como globalmente.

La evaluación y la declaración de los resultados pueden ser realizadas por el centro de votación globalmente, o tanto por el centro de votación globalmente como por cada máquina de votación localmente. Evaluación significa aquí determinar todas las opciones de voto de la base de datos de cada máquina de votación lo cual comprende salidas del algoritmo, opciones aleatorias de todos los candidatos/opciones, y los otros parámetros conocidos de cada votante usando el secreto de cada máquina de votación. Para la evaluación es necesario el secreto. La máquina de votación también puede contar votos simplemente durante las elecciones, y los recuentos se pueden usar en la declaración local sin evaluación de los resultados. No obstante, estos resultados no son básicos, sino que, para ciertos resultados, se requiere una evaluación de resultados por parte del centro de votación. Los datos almacenados y los resultados de votación de cada máquina de votación son hechos públicos globalmente por el centro de votación o globalmente por el centro de votación y localmente por cada máquina de votación después de que finalicen las elecciones. En la FIG. 1 se visualiza la declaración de los datos almacenados y los resultados de cada máquina de votación.

Los secretos de los algoritmos se pueden generar en las máquinas de votación localmente, o se pueden generar en el centro de votación, y distribuir a cada máquina de votación. En este último caso, los secretos se almacenan en el centro de votación. Si los secretos se generan en las máquinas de votación, los mismos se transfieren al centro de votación antes de la evaluación de resultados. Sin embargo, debe garantizarse la confidencialidad de los secretos durante la transferencia. Las máquinas de votación no dejan al descubierto los secretos, preferentemente eliminan por *zeroization* los secretos después de que finalicen las elecciones, y se materializa la confidencialidad de los

secretos en caso de que la misma sea necesaria para la transferencia.

5 Después de que hayan finalizado las elecciones, se hacen públicos los datos recogidos de las bases de datos locales. Cada votante encuentra su recibo obtenido de las máquinas de votación durante el proceso de votación a partir de los datos que se han hecho públicos. Si encuentra el recibo tal como es, puede estar seguro del recuento  
10 correcto de su voto. Por otro lado, el centro de votación evalúa votos y verifica la emisión correcta de votos usando datos recogidos de las bases de datos de máquinas de votación. Junto a estos, un tercero de confianza puede repetir la verificación y la evaluación de votos usando los secretos recibidos confidencialmente del centro de votación. Y finalmente, los secretos de parte o la totalidad de las máquinas de votación se pueden dar a conocer para una evaluación y verificación públicas de los votos. En la FIG. 1 se muestran las verificaciones, verificación y evaluación por parte del centro de votación, la verificación por parte de los votantes y la verificación por parte de un tercero de confianza.

**REIVINDICACIONES**

1. Método de votación electrónica que comprende:
  - a. Recibir una opción de voto en relación con un candidato soportado y una opción aleatoria de entre un conjunto de opciones aleatorias predeterminadas, asignándose la opción aleatoria recibida a la opción de candidato recibida, a saber la opción de voto, por medio de una interfaz hombre-máquina de una máquina de votación,
  - b. generar una salida de un algoritmo criptográfico para realizar un cifrado por parte de la máquina de votación, en donde
    - el algoritmo criptográfico hace uso de un secreto,
    - las entradas al algoritmo criptográfico comprenden la opción de voto y la opción aleatoria
  - c. Imprimir la salida del algoritmo en un recibo de papel,
  - d. Recibir una opción aleatoria para cada candidato de entre el conjunto de opciones aleatorias predeterminadas asignadas a cada uno de los candidatos por medio de un escáner óptico de la máquina de votación,
  - e. Imprimir todas las opciones aleatorias recibidas en la etapa (d) en el recibo de papel,
  - f. Esperar hasta que las opciones aleatorias recibidas de la etapa (d) se comparen con las opciones aleatorias impresas de la etapa (e) por parte de un votante,
  - g. Recibir aprobación del votante si las opciones aleatorias recibida e impresa son iguales o,
  - h. Recibir un rechazo por parte del votante si las opciones aleatorias recibida e impresa no son iguales e informar a una autoridad sobre la incompatibilidad,
  - i. si se ha recibido la aprobación, almacenar datos que comprenden un texto de verificación del votante que está compuesto por la salida del algoritmo de la etapa (b) y las opciones aleatorias de la etapa (d) en una base de datos local de la máquina de votación, y proporcionar el recibo de papel al votante,
  - j. después de que hayan finalizado las elecciones, transferir los datos de las bases de datos locales de las máquinas de votación a una base de datos central de un centro de votación y hacer públicos los datos transferidos,
  - k. comprobar el recuento correcto de los votos cuando los votantes comprueban sus textos de verificación con los datos hechos públicos,
  - l. garantizar un recuento correcto de los votos por parte del centro de votación verificando la emisión correcta de votos durante la evaluación de votos a partir de los datos recogidos de las bases de datos de máquinas de votación usando los datos almacenados que comprenden la salida del algoritmo, las opciones aleatorias de la etapa (d) y el secreto de cada máquina de votación en la cual se emite un voto.
2. Método de votación electrónica según la reivindicación 1, en el que si la opción aleatoria, introducida en primer lugar, relacionada con la opción de voto, en la etapa (a), y la opción aleatoria, introducida en último lugar, relacionada con la opción de voto, en la etapa (d), no son iguales, el proceso de votación finaliza con un fallo o continúa con el flujo normal dependiendo de la decisión de la autoridad electoral sobre la implementación del método.
3. Método de votación electrónica según la reivindicación 1, en el que el método de votación se realiza en todas las máquinas de votación.
4. Método de votación electrónica según la reivindicación 1, en el que si un posible código maligno en el sistema se atreve a cambiar la opción de voto del votante, se revela una modificación ilegal/software maligno siempre que cuando el votante introduce opciones aleatorias relacionadas con todas las opciones de candidato posibles y si la opción aleatoria introducida por el votante en relación con la opción de candidato asociada al software maligno no es igual a la opción aleatoria escogida por el código maligno y tomada como entrada para el algoritmo criptográfico con el fin de producir la salida del algoritmo en la etapa anterior a la introducción de opciones aleatorias relacionadas con todas las opciones posibles por parte del votante.
5. Método de votación electrónica según la reivindicación 1, en el que un tercero de confianza puede llevar a cabo la evaluación y la verificación de votos de la misma manera que lo hace el centro de votación usando los datos almacenados en las máquinas de votación que contienen información con respecto a la salida del algoritmo y opciones aleatorias de todas las opciones posibles específicas de cada votante así como los secretos de las

máquinas de votación recibidos confidencialmente del centro de votación.

- 5
6. Método de votación electrónica según la reivindicación 5, en el que los resultados de votación obtenidos en cada una de las máquinas de votación a través de la verificación de votos llevada a cabo tanto por el centro de votación como por el tercero de confianza se comparan, respectivamente, entre sí con el fin de garantizar que el centro de votación y el tercero de confianza lleguen a los mismos resultados de votación en las mismas máquinas de votación.
- 10
7. Método de votación electrónica según la reivindicación 1, en el que la evaluación y la verificación de votos se pueden llevar a cabo públicamente en parte o la totalidad de las máquinas de votación siempre que los secretos de estas máquinas de votación sean hechos públicos por el centro de votación, y los secretos junto con los datos almacenados en las máquinas de votación que comprenden la salida del algoritmo y opciones aleatorias de todas las opciones posibles se usan para la verificación de votos.

5 ↙

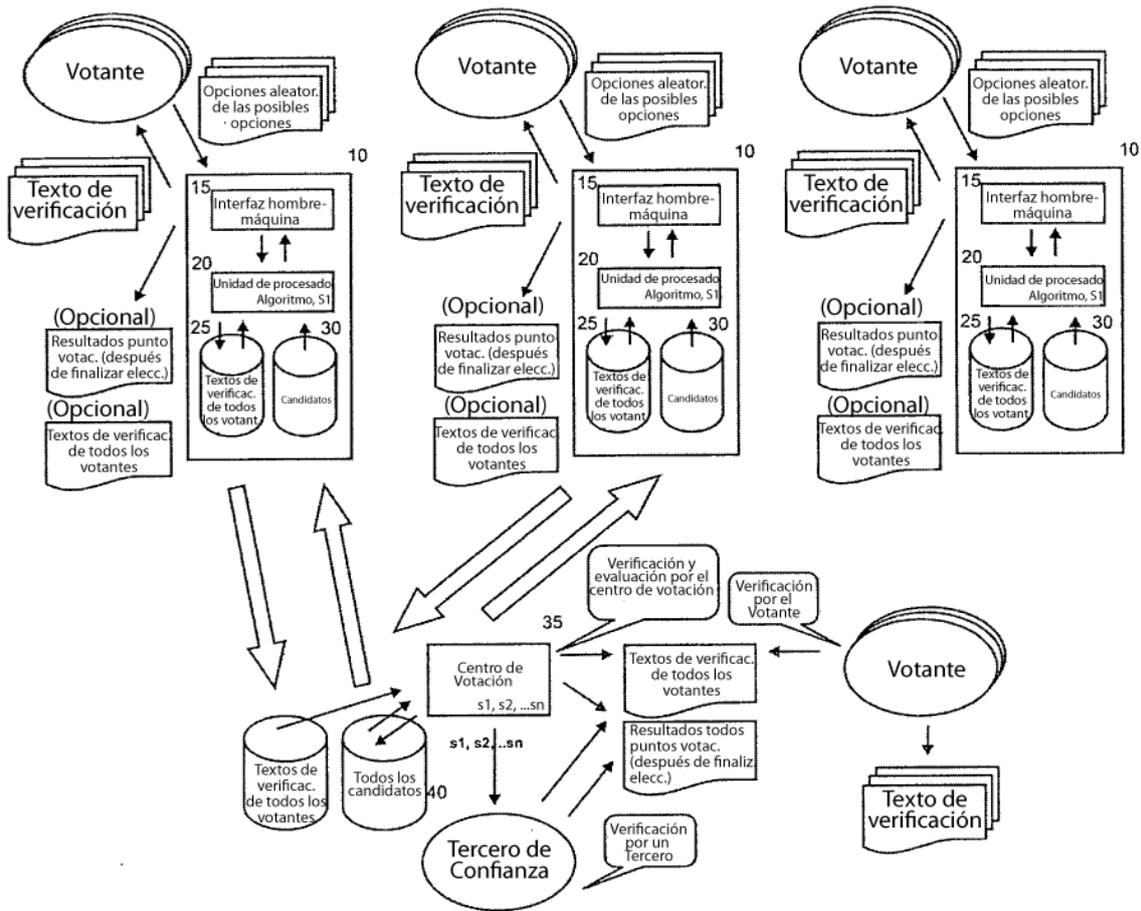


FIGURA 1

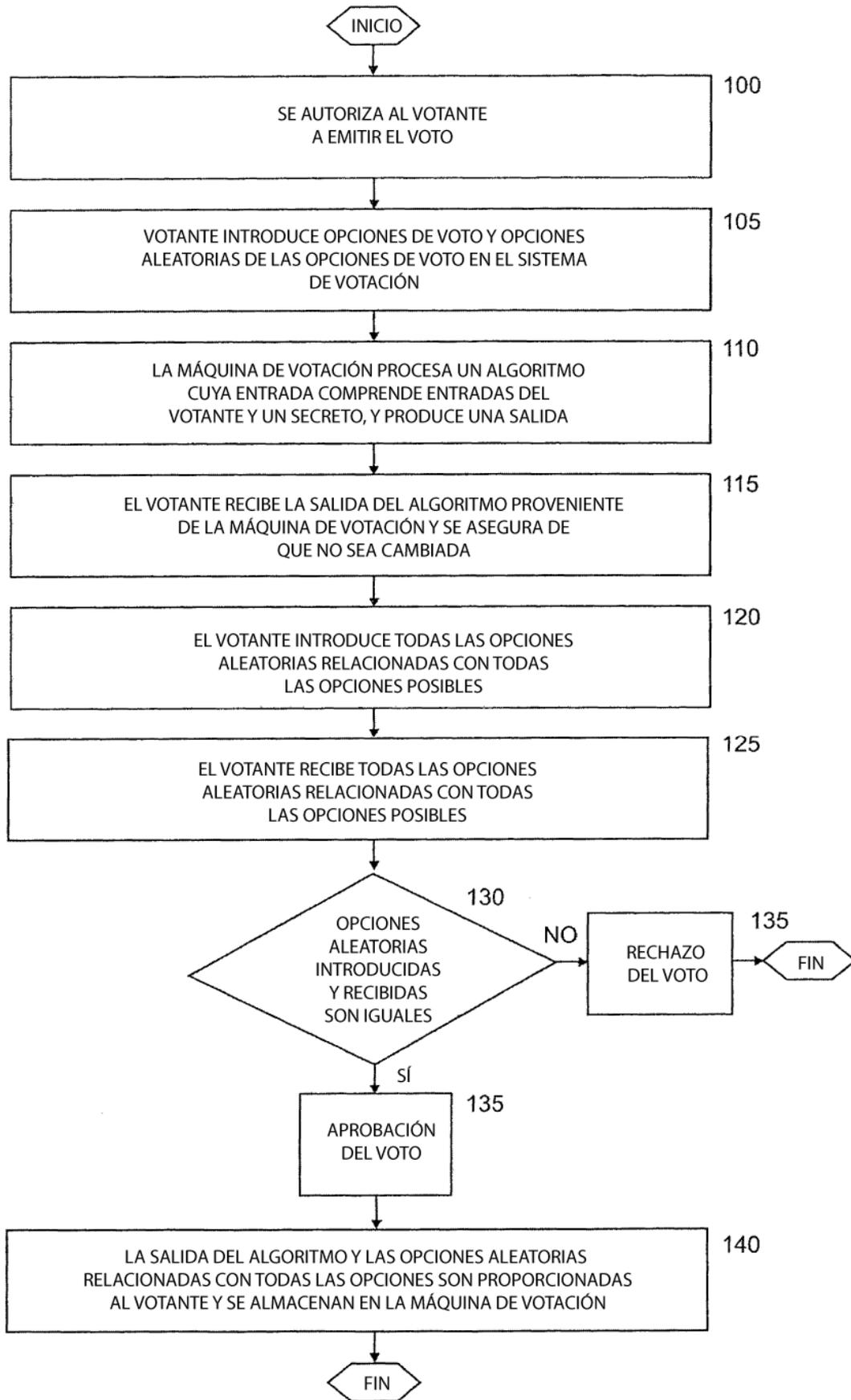


FIGURA 2

**1. Qué candidato selecciona para la circunscripción de Dörtdivan:**

<p>Ahmet Unutulmaz</p> <p>310</p> <p>320</p> <p><input type="radio"/> Rojo</p> <p>320</p> <p><input type="radio"/> Verde</p> <p>320</p> <p><input type="radio"/> Azul</p>	<p>Ali Demirtaş</p> <p>310</p> <p>320</p> <p><input type="radio"/> Rojo</p> <p>320</p> <p><input type="radio"/> Verde</p> <p>320</p> <p><input type="radio"/> Azul</p>	<p>Coskun Karaca</p> <p>310</p> <p>320</p> <p><input type="radio"/> Rojo</p> <p>320</p> <p><input type="radio"/> Verde</p> <p>320</p> <p><input type="radio"/> Azul</p>
<p>Ekrem Albayrak</p> <p>310</p> <p>320</p> <p><input type="radio"/> Rojo</p> <p>320</p> <p><input type="radio"/> Verde</p> <p>320</p> <p><input type="radio"/> Azul</p>	<p>Hüsniddin Charyyev</p> <p>310</p> <p>320</p> <p><input type="radio"/> Rojo</p> <p>320</p> <p><input type="radio"/> Verde</p> <p>320</p> <p><input type="radio"/> Azul</p>	<p><b><i>Mehmet Çamlıbel</i></b></p> <p>310</p> <p>320</p> <p><input checked="" type="radio"/> Rojo</p> <p>320</p> <p><input type="radio"/> Verde</p> <p>320</p> <p><input type="radio"/> Azul</p>

**2. ¿Debe elegirse el presidente de Turquía en elecciones nacionales?**

<p>310</p> <p><i>SÍ</i></p> <p>320</p> <p><input type="radio"/> Rojo</p> <p>320</p> <p><input checked="" type="radio"/> Verde</p> <p>320</p> <p><input type="radio"/> Azul</p>	<p>310</p> <p>NO</p> <p>320</p> <p><input type="radio"/> Rojo</p> <p>320</p> <p><input type="radio"/> Verde</p> <p>320</p> <p><input type="radio"/> Azul</p>
--	--

EMISIÓN

FIGURA 3

400

Se recomienda llenar uno de entre ROJO, VERDE O AZUL para cada fila.

**1. Candidatos a alcalde para la circunscripción de Dörtdivan:**

	420 ROJO	420 VERDE	420 AZUL
410 Ahmet Unutulmaz	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
410 Ali Demirtaş	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
410 Coskun Karaca	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
410 Ekrem Albayrak	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
410 Hüsniiddin Charyyev	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
410 Mehmet Çamlıbel	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

**2. ¿Debe elegirse el presidente en las elecciones nacionales?**

	420 ROJO	420 VERDE	420 AZUL
410 SÍ	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
410 NO	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

FIGURA 4

Id Punto Votación: 140206

530 540

Id Votante: Broken Toy

----- Salida Algoritmo -----

87A7D63BF33910FF 510

----- Opciones Aleatorias ----- 520

Opciones Aleatorias 1: Rojo-Verde-Verde-Rojo-Azul-Verde

Opciones Aleatorias 2: Verde-Azul

----- Verificación -----

OK

FIGURA 5

600

Id Punto Votación:140206			
Id Votante	Salida Algoritmo	Opciones Aleatorias n.º 1	Opciones Aleatorias n.º 2
610 Broken Toy	87A7D63BF33910FF	Rojo-Verde-Verde-Rojo-Azul-Verde	Verde-Azul
610 Ceylan	E549B326C224490A	Verde-Azul-Verde-Azul-Azul-Rojo	Rojo-Azul
610 Mercan	92981614C39DAA70	Rojo-Rojo-Verde-Verde-Azul-Rojo	Azul-Azul
610 Nilüfer	5765F9887A34557D	Azul-Rojo-Verde-Rojo-Azul-Azul	Verde-Rojo
...	...	...	...

FIGURA 6