(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 301 311**

(21) Número de solicitud: 200502919

(51) Int. Cl.:

H04L 9/32 (2006.01)

H02J 7/04 (2006.01)

G06F 3/023 (2006.01)

(12) PATENTE DE INVENCIÓN CON EXAMEN PREVIO B2

(22) Fecha de presentación: **25.11.2005**

(30) Prioridad: **26.11.2004 JP 2004-342945**
26.11.2004 JP 2004-342946
09.09.2005 JP 2005-263010

(43) Fecha de publicación de la solicitud: **16.06.2008**

Fecha de la concesión: **10.03.2009**

Fecha de modificación de las reivindicaciones: **05.03.2009**

(45) Fecha de anuncio de la concesión: **01.04.2009**

(45) Fecha de publicación del folleto de la patente: **01.04.2009**

(73) Titular/es:
SONY COMPUTER ENTERTAINMENT Inc.
2-6-21 Miami-Aoyama
Minato-ku, Tokyo, JP

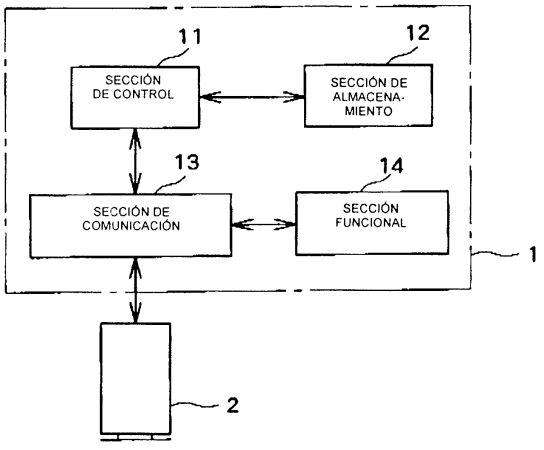
(72) Inventor/es: **Sasaki, Dai y**
Moriai, Shiho

(74) Agente: **Ungría López, Javier**

(54) Título: **Batería y dispositivo de petición de autenticación.**

(57) Resumen:
Batería y dispositivo de petición de autenticación.
Un dispositivo periférico que está conectado a un cuerpo principal como un dispositivo de petición de autenticación opera como un dispositivo a autenticar. Recibiendo información relacionada con código del cuerpo principal, el dispositivo periférico adquiere un código de reto en base a la información relacionada con código recibida, genera información encriptada encriptando el código de reto, y transmite información relacionada con encriptado que se refiere a la información encriptada generada al cuerpo principal. La información relacionada con código es parte del código de reto y/o la información relacionada con encriptado es parte de la información encriptada.

FIG. 1



ES 2 301 311 B2

DESCRIPCIÓN

Batería y dispositivo de petición de autenticación.

Referencia cruzada a solicitudes relacionadas

Se incorporan aquí por referencia las solicitudes de prioridad números JP 2004-342945, JP 2004-342946 y JP 2005-263010 en las que se basa esta solicitud de patente.

Antecedentes de la invención

La presente invención se refiere a una batería como un sujeto de autenticación y un dispositivo de petición de autenticación que está conectado a la batería y envía una petición de autenticación de batería.

En los últimos años, varios aparatos electrónicos de consumo incluyendo máquinas recreativas domésticas han aumentado en funcionalidad y han aumentado los tipos cuyas funciones se pueden ampliar conectando dispositivos periféricos al cuerpo principal del aparato. En tales aparatos, para evitar el problema que resulta de que un usuario conecta erróneamente un producto de otra compañía al cuerpo principal del aparato, se puede producir un caso de que se desee determinar si un dispositivo periférico es auténtico (genuino).

Un método para ello es someter el cuerpo principal del aparato y el dispositivo periférico a procesado de autenticación utilizado en general en sistemas informáticos para comprobar si un dispositivo periférico es auténtico. Por ejemplo, un ejemplo general de autenticación del tipo de respuesta a reto se describe en JP-A-11-163853.

Además, en los últimos años, incluso para baterías, han aparecido fabricantes que suministran productos de imitación (falsificados), que cada vez producen más problemas tales como suministro inestable de potencia a causa de diferencias de regímenes eléctricos. Por lo tanto, incluso para baterías, ahora cada vez es más necesario efectuar procesado de autenticación para comprobar si un producto es auténtico. Para ello, se puede emplear un método de autenticación de batería descrito en JP-T-2000-517487 (el símbolo "JP-T" en el sentido en que se usa aquí significa una traducción al japonés publicada de una Solicitud de Patente PCT).

Sin embargo, en contraposición a los aparatos de información, los aparatos utilizados en viviendas tales como aparatos electrónicos de consumo puede tener el inconveniente de generar una gran cantidad de ruido eléctrico durante el funcionamiento. Una forma de contrarrestarlo es efectuar procesado de autenticación repetidas veces para incrementar la fiabilidad de la autenticación.

Sin embargo, donde el procesado de autenticación se lleva a cabo repetidas veces, la cantidad de datos que se intercambian entre un dispositivo periférico y el cuerpo principal resulta grande y la carga de comunicación aumenta consiguientemente. En aparatos electrónicos de consumo y análogos, tiene prioridad el procesado que se refiere a las funciones del aparato propiamente dicho. Por lo tanto, no es deseable incrementar la carga de comunicaciones que se realizan entre el cuerpo principal y un dispositivo periférico y no se refieren a las funciones del aparato propiamente dicho.

Además, en el método de autenticación convencional anterior, no se consideran problemas específicos de un dispositivo a autenticar tal como un problema de que una batería no está cargada.

Resumen de la invención

La presente invención se ha realizado en vista de las circunstancias anteriores en la técnica, y por lo tanto un objeto de la invención es proporcionar una batería capaz de reducir la cantidad de datos que se intercambian para autenticación y de disminuir por ello la carga de comunicación.

Otro objeto de la invención es proporcionar una batería en la que se consideran problemas específicos de la batería propiamente dicha como un dispositivo a autenticar.

Para resolver los problemas anteriores en la técnica, la invención proporciona un sistema de autenticación que incluye una batería y un dispositivo de petición de autenticación que autentica la batería, conteniendo la batería y el dispositivo de petición de autenticación una clave de encriptado común, donde el dispositivo de petición de autenticación genera primera información relacionada con código y la transmite a la batería, adquiere un primer código de reto de comparación en base a la primera información relacionada con código, y genera primera información de comparación de encriptado encriptando el primer código de reto de comparación usando la clave de encriptado; la batería recibe la primera información relacionada con código, adquiere un primer código de reto en base a la primera información relacionada con código recibida, genera primera información encriptada encriptando el primer código de reto adquirido usando la clave de encriptado, y transmite primera información relacionada con encriptado relativa a la primera información encriptada generada al dispositivo de petición de autenticación; el dispositivo de petición de autenticación determina si autenticar la batería comparando la primera información relacionada con encriptado recibida con primera información relacionada con encriptado de comparación relativa a la primera información de comparación de encriptado generada; y la primera información relacionada con código es parte del primer código de reto y/o la primera información relacionada con encriptado es parte de la primera información encriptada.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques que esboza la configuración de un dispositivo periférico 1.

La figura 2 es diagrama de bloques que esboza la configuración de un cuerpo principal 2.

La figura 3 es diagrama de bloques que representa la configuración ejemplo de una sección de control de potencia del cuerpo principal 2.

La figura 4 es un diagrama de bloques funcionales de un ejemplo del dispositivo periférico 1.

La figura 5 es un diagrama de bloques funcionales de un ejemplo del cuerpo principal 2.

La figura 6 es un diagrama de flujo que representa un flujo de comunicaciones entre el dispositivo periférico 1 y el cuerpo principal 2.

Y la figura 7 es un diagrama de flujo que representa un proceso ejemplar ejecutado por el cuerpo principal 2.

Descripción de la realización preferida

Una realización de la presente invención se describirá a continuación con referencia a los dibujos anexos. Una batería según la realización se implementa como un dispositivo periférico 1. Como se representa en la figura 1, el dispositivo periférico 1 incluye una sección de control 11, una sección de almacenamiento 12, una sección de comunicación 13, y una sección funcional 14, y está conectado a un cuerpo principal 2.

La sección de control 11 es una CPU o análogos y opera según programas almacenados en la sección de almacenamiento 12. La sección de control 11 realiza procesado para realizar las funciones del dispositivo periférico 1. Para un dispositivo de manipulación tal como un controlador como un dispositivo periférico 1, la sección de control 11 realiza procesado consistente en transmitir información referente a una manipulación de instrucción por el usuario al cuerpo principal 2. Para un dispositivo de almacenamiento, tal como una tarjeta de memoria, como un dispositivo periférico 1, la sección de control 11 realiza procesado consistente en guardar información recibida del cuerpo principal 2 y procesado consistente en suministrar información mantenida en ella al cuerpo principal 2 en respuesta a una petición del cuerpo principal 2. Aunque en esta realización el dispositivo a autenticar es la fuente de alimentación (es decir, batería), el dispositivo periférico 1 como el dispositivo a autenticar también puede ser cualquiera de otros varios dispositivos incluyendo un dispositivo de comunicación, un dispositivo de formación de imágenes tal como una cámara, y un dispositivo de sonido tal como un altavoz.

Para realizar una función de autenticación, la sección de control 11 también realiza procesado consistente en recibir primera información relacionada con código, adquirir un primer código de reto en base a la primera información relacionada con código recibida, y generar primera información encriptada encriptando el primer código de reto. El procesado para realizar la función de autenticación del controlador 11 se describirá con detalle más adelante.

La sección de almacenamiento 12 incluye un elemento de almacenamiento tal como una ROM flash y una RAM, y guarda programas a ejecutar por la sección de control 11. La sección de almacenamiento 12 también opera como una memoria de trabajo para guardar varios datos que son necesarios durante el procesado de la sección de control 11.

La sección de comunicación 13 es un puerto serie de comunicaciones, por ejemplo, y está conectado al cuerpo principal 2. La sección de comunicación 13 transmite información al cuerpo principal 2 según una instrucción que se introduce desde la sección de control 11. Además, la sección de comunicación 13 envía, a la sección de control 11, información recibida del cuerpo principal 2.

La sección funcional 14 realiza las funciones del dispositivo periférico 1. Puesto que en esta realización el dispositivo periférico 1 es la batería, la sección funcional 14 incluye una batería secundaria para suministrar potencia eléctrica. Como se representa en la figura 2, el cuerpo principal 2, que es una máquina recreativa doméstica, por ejemplo, incluye una sección de control 21 tal como una CPU, una sección de almacenamiento 22, una sección de manipulación 23, una sección de control de pantalla 24, una sección de comunicación 25, una unidad de disco óptico 26, y una sección de control de potencia 27.

La sección de control 21 opera según programas almacenados en la sección de almacenamiento 22. Por ejemplo, la sección de control 21 realiza procesado que se refiere a un juego. En esta realización, la sección de control 21 también realiza operaciones de un dispositivo de petición de autenticación. El procesado detallado que se lleva a cabo por el aspecto de dispositivo de petición de autenticación de la sección de control 21 se describirá más adelante.

La sección de almacenamiento 22, que incluye una RAM, por ejemplo, guarda programas recreativos que son leídos por la unidad de disco óptico 26. La sección de almacenamiento 22 también incluye un elemento de almacenamiento no volátil, donde se almacenan programas para el dispositivo de petición de autenticación. La sección de almacenamiento 22 también opera como una memoria de trabajo para la sección de control 21.

La sección de manipulación 23, que es un controlador de juego, envía el contenido de una manipulación de instrucción de un jugador a la sección de control 21. La sección de control de pantalla 24, que es un circuito gráfico, visualiza una imagen de juego en un dispositivo de visualización tal como un receptor de TV doméstico según una instrucción introducida desde la sección de control 21. La sección de comunicación 25, que es un puerto serie de comunicaciones, por ejemplo, está conectada a la sección de comunicación 13 del dispositivo periférico 1 e intercambia información con ella. En esta realización, la sección de comunicación 25 transmite información al dispositivo periférico 1 según una instrucción introducida desde la sección de control 21, y envía, a la sección de control 21, información recibida del dispositivo periférico 1.

La unidad de disco óptico 26, que es una unidad de DVD-ROM o una unidad de disco Blu-ray, por ejemplo, lee información, tal como programas, de un medio de grabación, tal como un DVD, un disco Blu-ray, o análogos, y la envía a la sección de control 21.

Como se representa en la figura 3, la sección de control de potencia 27, que está conectada a la batería como el dispositivo periférico 1, incluye un circuito de control de potencia 31, un circuito de carga 32, y un circuito de suministro de potencia 33. El circuito de control de potencia 31 controla el suministro de potencia de la batería o el circuito de suministro de potencia 33 a las secciones individuales tal como la sección de control 21. Por ejemplo, si un jugador conecta la potencia, el circuito de control de potencia 31 comienza a suministrar potencia a las secciones individuales. Si un jugador apaga la potencia o llega una instrucción de apagar la potencia (instrucción de apagado de potencia) de la sección de control 21, el circuito de control de potencia 31 interrumpe el suministro de potencia a las secciones individuales.

El circuito de carga 32 carga la batería si la batería está conectada a él en un estado en el que se le suministra potencia desde el circuito de suministro de potencia 33. El circuito de suministro de potencia 33 es un regulador, por ejemplo, y está conectado a una fuente de alimentación externa (por ejemplo, enchufe de pared doméstico). El circuito de suministro de potencia 33 recibe voltaje de suministro de potencia CC que se genera en base a la potencia de la fuente de alimentación externa, y lo envía al circuito de control de potencia 31 y el circuito de carga 32. El circuito de suministro de potencia 33 corresponde a una “sección de recepción de potencia” de la invención.

La sección de control de potencia 27 suministra a las secciones individuales potencia que se suministra desde la batería si la batería está conectada a ella en un estado en el que el circuito de suministro de potencia 33 no recibe potencia de ninguna fuente de alimentación externa. Si el circuito de suministro de potencia 33 recibe potencia de una fuente de alimentación externa, la sección de control de potencia 27 suministra a las secciones individuales potencia que se suministra desde la fuente de alimentación externa. Además, la sección de control de potencia 27 carga la batería si la batería está conectada a ella en un estado en el que el circuito de suministro de potencia 33 recibe potencia de una fuente de alimentación externa.

Ahora se describirá el procesado para realizar la función de autenticación que lleva a cabo la sección de control 11 del dispositivo periférico 1. En esta realización, múltiples claves de encriptado candidatas k0, k1, ..., se almacenan con anterioridad en la sección de almacenamiento 12 del dispositivo periférico 1.

Expresado en términos funcionales, como se representa en la figura 4, la sección de control 11 incluye una sección de procesado de petición de autenticación 41 y una sección de autenticación de cuerpo principal 42.

La sección de procesado de petición de autenticación 41 recibe del cuerpo principal 2 (dispositivo de petición de autenticación), mediante la sección de comunicación 13, primera información relacionada con código a partir de la que se ha de generar un primer código de reto. Además, la sección de procesado de petición de autenticación 41 recibe del cuerpo principal 2 información de identificación de clave de encriptado a usar para identificar una clave de encriptado, y lee, de la sección de almacenamiento 12, una clave de encriptado kN que se identifica por la información de identificación de clave de encriptado (por ejemplo, una tecla N).

Se supone aquí que la primera información relacionada con código es parte de un primer código de reto. Por ejemplo, donde se utiliza un primer código de reto de 128 bits, el cuerpo principal 2 envía, como la primera información relacionada con código, información de 64 bits que ha de corresponder a la primera mitad (mitad superior) de la información de 128 bits. La sección de procesado de petición de autenticación 41 genera un primer código de reto en base a la primera información relacionada con código y la adquiere.

En esta realización, se almacena con anterioridad una pluralidad de primeras constantes C10, C11, ..., en la sección de almacenamiento 12. Se genera un primer código de reto leyendo, de la sección de almacenamiento 12, una primera constante C1N correspondiente a un número de tecla N que se recibe como información de identificación de clave de encriptado y poniendo la primera constante C1N leída después de la primera información relacionada con código recibida. Donde, como se ha descrito anteriormente, la primera información relacionada con código es de 64 bits para el primer código de reto de 128 bits, cada una de las primeras constantes C10, C11, ..., es una constante de 64 bits. La primera constante es “información de parte común” de la invención.

La sección de procesado de petición de autenticación 41 genera primera información encriptada encriptando el primer código de reto que se ha generado utilizando la clave de encriptado kN leída de la sección de almacenamiento 12.

Además, la sección de procesado de petición de autenticación 41 extrae, como primera información relacionada con encriptado, una parte predeterminada (por ejemplo, segunda mitad (mitad inferior)) de la primera información encriptada, y transmite la primera información relacionada con encriptado extraída al cuerpo principal 2. Por ejemplo, si el primer código de reto es de 128 bits y el algoritmo del encriptado anterior es de un método de codificación que no cambia la longitud de código de la información objeto de encriptado, la primera información encriptada también tiene 128 bits. La sección de procesado de petición de autenticación 41 transmite la parte predeterminada (por ejemplo, 64 bits de la segunda mitad) de la primera información encriptada de 128 bits al cuerpo principal 2.

Para autenticar el cuerpo principal 2 (dispositivo de petición de autenticación), la sección de autenticación de cuerpo principal 42 genera segunda información relacionada con código que se refiere a un segundo código de reto de comparación (segundo código de reto para comparación) a usar para autenticar el cuerpo principal 2. Por ejemplo, la sección de autenticación de cuerpo principal 42 genera un valor numérico que tiene un número preestablecido de bits mediante una rutina de número aleatorio y transmite el número aleatorio generado como segunda información relacionada con código al cuerpo principal 2 mediante la sección de comunicación 13.

Además, la sección de autenticación de cuerpo principal 42 genera un segundo código de reto de comparación en base a la segunda información relacionada con código generada. En esta realización, múltiples segundas constantes C20, C21, ..., se almacenan con anterioridad en la sección de almacenamiento 12. Una segunda constante C2N correspondiente al número de tecla N que se recibió previamente como la información de identificación de clave de encriptado se lee de la sección de almacenamiento 12. Se genera un segundo código de reto de comparación colocando la segunda constante C2N después de la segunda información relacionada con código generada. La cantidad de datos de comunicaciones (transmisión y recepción) de un segundo código de reto se puede reducir, como se ha descrito anteriormente, determinando aleatoriamente parte del segundo código de reto y convirtiendo la parte restante en una constante.

La sección de autenticación de cuerpo principal 42 genera segunda información de comparación de encriptado encriptando el segundo código de reto de comparación almacenado en la sección de almacenamiento 12 usando la clave de encriptado kN que se identifica utilizando la información de identificación de clave de encriptado que se recibió al realizar el procesado de función de autenticación.

Además, la sección de autenticación de cuerpo principal 42 compara una parte predeterminada de la segunda información de comparación de encriptado con parte de la información obtenida encriptando el segundo código de reto en el cuerpo principal 2. Donde los 64 bits de la segunda mitad se extrae como la parte predeterminada como en el ejemplo antes descrito, la sección de autenticación de cuerpo principal 42 extrae los 64 bits de la segunda mitad de la segunda información de comparación de encriptado y compara la información de 64 bits extraída con la segunda información de encriptado (64 bits) recibida del cuerpo principal 2.

Si coinciden entre sí, la sección de autenticación de cuerpo principal 42 (es decir, el dispositivo periférico 1) juzga que el cuerpo principal 2 es uno autorizado (por ejemplo, auténtico) y refiere el resultado del juicio al cuerpo principal 2. Si la sección de autenticación de cuerpo principal 42 juzga que la parte predeterminada de la segunda información de comparación de encriptado no coincide con la segunda información relacionada con encriptado recibida del cuerpo principal 2, es decir, el cuerpo principal 2 no es uno autorizado, la sección de autenticación de cuerpo principal 42 refiere el resultado del juicio al cuerpo principal 2.

A continuación se describirá la operación de la sección de control 21 del cuerpo principal 2 que opera como el dispositivo de petición de autenticación. Una clave de encriptado kN se almacena con anterioridad en la sección de almacenamiento 22 del cuerpo principal 2. La clave de encriptado kN es la misma que una de las múltiples claves de encriptado almacenadas en la sección de almacenamiento 12 del dispositivo periférico 1 como el dispositivo a autenticar. Además, información de identificación de clave de encriptado (por ejemplo, número de tecla N) que es información necesaria para identificar la clave de encriptado en el dispositivo periférico 1 se almacena con anterioridad en la sección de almacenamiento 22.

La sección de control 21 del cuerpo principal 2 realiza funciones representadas en la figura 5. Expresado en términos funcionales, como se representa en la figura 5, la sección de control 21 incluye una sección de autenticación de dispositivo periférico 45 y una sección de procesado de petición de autenticación 46.

La sección de autenticación de dispositivo periférico 45 genera primera información relacionada con código de la que se ha de generar un primer código de reto de comparación. Por ejemplo, la sección de autenticación de dispositivo periférico 45 genera un número aleatorio por una rutina de número aleatorio, y transmite el número aleatorio generado como primera información relacionada con código al dispositivo periférico 1 mediante la sección de comunicación 25. La sección de autenticación de dispositivo periférico 45 también transmite la información de identificación de clave de encriptado (por ejemplo, número de tecla N) a usar para identificar la clave de encriptado kN.

Además, la sección de autenticación de dispositivo periférico 45 genera un primer código de reto de comparación en base a la primera información relacionada con código generada. En esta realización, una primera constante Cli a usar en el dispositivo periférico 1 se almacena con anterioridad en la sección de almacenamiento 22. En este ejemplo, dado que la primera constante C1N que se identifica utilizando la información de identificación de clave de encriptado (número de tecla N) es utilizada en el dispositivo periférico 1, la primera constante C1N se almacena en la sección de almacenamiento 22.

La sección de autenticación de dispositivo periférico 45 genera un primer código de reto de comparación poniendo la primera constante C1N almacenada en la sección de almacenamiento 22 después de la información relacionada con código generada. La cantidad de datos de comunicaciones (transmisión y recepción) de un código de reto se puede reducir, como se ha descrito anteriormente, determinando parte del código de reto aleatoriamente y convirtiendo la parte restante en una constante.

La sección de autenticación de dispositivo periférico 45 genera primera información de comparación de encriptado encriptando el primer código de reto de comparación generado por la clave de encriptado kN almacenada en la sección de almacenamiento 22.

Además, la sección de autenticación de dispositivo periférico 45 recibe, del dispositivo periférico 1, como primera información relacionada con encriptado, parte de un resultado de encriptado de un primer código de reto realizado en el dispositivo periférico 1 utilizando la clave de encriptado kN. Y la sección de autenticación de dispositivo periférico 45 compara una parte predeterminada de la primera información de comparación de encriptado con la primera información relacionada con encriptado recibida del dispositivo periférico 1. Donde los 64 bits de la segunda mitad se extraen como la parte predeterminada como en el ejemplo antes descrito, la sección de autenticación de dispositivo periférico 45 extrae los 64 bits de la segunda mitad de la primera información de comparación de encriptado y compara la información de 64 bits extraída con la primera información relacionada con encriptado (64 bits) recibida del dispositivo periférico 1.

Si coinciden entre sí, la sección de autenticación de dispositivo periférico 45 juzga que el dispositivo periférico 1 es un dispositivo autorizado (por ejemplo, genuino).

Además, el cuerpo principal 2 mantiene, con anterioridad, la segunda constante C2N que es utilizada en el dispositivo periférico 1. La sección de procesado de petición de autenticación 46 genera un segundo código de reto poniendo la segunda constante C2N después de la segunda información relacionada con código que se recibe de la sección de autenticación de cuerpo principal 42 del dispositivo periférico 1.

La sección de procesado de petición de autenticación 46 genera segunda información encriptada leyendo el código de encriptado kN de la sección de almacenamiento 22 y encriptando el segundo código de reto generado usando el código de encriptado kN. Además, la sección de procesado de petición de autenticación 46 extrae, como segunda información relacionada con encriptado, una parte predeterminada (por ejemplo, segunda mitad) de la segunda información encriptada y transmite la segunda información relacionada con encriptado extraída al dispositivo periférico 1.

Aunque la descripción anterior se dirige al caso de que se realiza el procesado de autenticar el dispositivo periférico 1 y el procesado de autenticar el cuerpo principal 2 por el dispositivo periférico 1, solamente el procesado de que el cuerpo principal 2 autentica el dispositivo periférico 1 se puede realizar si es suficiente. En este caso, la sección de autenticación de cuerpo principal 42 del dispositivo periférico 1 y la sección de petición de autenticación 46 del cuerpo principal 2 no siempre son necesarias.

Una característica importante de esta realización es que se refiere si autenticación ha tenido éxito o fallado usando datos que incluyen una parte predeterminada de la segunda información de comparación de encriptado. En esta realización, se hace un informe al efecto de que el cuerpo principal 2 ha sido autenticado transmitiendo una parte preestablecida propiamente dicha de la segunda información de comparación de encriptado al cuerpo principal 2 como datos de éxito de autenticación. Un informe al efecto de que el cuerpo principal 2 no ha sido autenticado se hace transmitiendo, al cuerpo principal 2, como datos de fallo de autenticación, datos obtenidos negando los bits individuales de la parte preestablecida de la segunda información de comparación de encriptado. La negación significa una operación de cambiar el bit “1” a “0” y el bit “0” a “1”. Una operación lógica de dejar cada bit de datos tal como está, corresponde a una “segunda operación lógica” de la invención, y una operación lógica de negar cada bit de datos corresponde a una “primera operación lógica” de la invención. Correspondientemente, cuando el cuerpo principal 2 refiere cuándo ha sido autenticado el dispositivo periférico 1, el cuerpo principal 2 transmite una parte preestablecida propiamente dicha de la primera información de comparación de encriptado. Un informe al efecto de que el dispositivo periférico 1 no ha sido autenticado se realiza transmitiendo, al dispositivo periférico 1, como datos de fallo de autenticación, datos obtenidos negando los bits individuales de la parte preestablecida de la primera información de comparación de encriptado.

El cuerpo principal 2 compara los datos de éxito de autenticación recibidos con la segunda información relacionada con encriptado que transmitió antes. Si se halla coincidencia, el cuerpo principal 2 juzga que ha sido autenticado.

Los datos de éxito de autenticación y los datos de fallo de autenticación pueden ser una constante predeterminada tal como datos cuyos bits son “1” o “0”. Sin embargo, donde se utiliza una constante para ello, por ejemplo, la información al efecto de que el cuerpo principal 2 ha sido autenticado puede ser enviada transmitiendo la constante como datos de éxito de autenticación usando un chip MOD fabricado ilegalmente. Para evitar dicho punto débil de la seguridad, en esta realización, los datos de éxito de autenticación o los datos de fallo de autenticación se generan utilizando, en lugar de una constante, la parte predeterminada de información de comparación de encriptado que toma un valor diferente cada vez que se lleva a cabo un procesado de autenticación.

En esta realización, el (los) código(s) de reto primero y/o segundo y la primera y/o segunda información encriptada obtenida encriptando el (los) código(s) de reto primero y/o segundo no se transmiten y reciben en su totalidad y, en cambio, se reciben y transmiten parte de ellos. Esto hace posible reducir la cantidad de datos que se intercambian para procesado de autenticación y por lo tanto contribuye a la reducción de la carga de comunicación.

A continuación, las operaciones del dispositivo periférico 1 y el cuerpo principal 2 como el dispositivo a autenticar y el dispositivo de petición de autenticación, respectivamente, se describirán con referencia a la figura 6. La figura 6 es un diagrama de flujo que representa un flujo de comunicaciones entre el dispositivo periférico 1 y el cuerpo principal 2. Al comienzo, una clave de encriptado k0, una primera constante C10, y una segunda constante C20 que corresponden a información de identificación de clave de encriptado N = 0 se almacenan en la sección de almacenamiento 22 del cuerpo principal 2.

Cuando el dispositivo periférico 1 es conectado al cuerpo principal 2, el cuerpo principal 2 genera un número aleatorio de 64 bits R1 en el paso S1 y transmite la información de identificación de clave de encriptado (en este ejemplo, el número de tecla "0") a usar para identificar la clave de encriptado k0 y el número aleatorio R1 que servirá como primera información relacionada con código al dispositivo periférico 1 en el paso S2.

En el paso S3, el cuerpo principal 2 genera un primer código de reto de comparación poniendo la primera constante C10 después del número aleatorio R1 que es la primera información relacionada con código generada en el paso S1. En la descripción siguiente, poner dos fragmentos de información uno junto a otro se denotará con el símbolo "H". Por consiguiente, el primer código de reto de comparación se representa con "R1||C10".

En el paso S4, el cuerpo principal 2 genera primera información de comparación de encriptado encriptando el primer código de reto de comparación generado R1||C10 usando la clave de encriptado k0. Una regla es ahora establecer que la información obtenida encriptando datos de sujeto d usando una clave de encriptado k deberá ser representada por ENC(k, d). La primera información de comparación de encriptado generada está representada por ENC(k0, (R1||C10)).

El dispositivo periférico 1 recibe la primera información relacionada con código R1 y el número de tecla "0" (información de identificación de clave de encriptado) del cuerpo principal 2, y lee una clave de encriptado k0 y una primera constante C10 que se identifican por la información de identificación de clave de encriptado "0" de la sección de almacenamiento 12. En el paso S5, el dispositivo periférico 1 genera un primer código de reto R1||C10 poniendo la primera información relacionada con código R1 y la primera constante C10 una junto a otra.

En el paso S6, el dispositivo periférico 1 genera primera información encriptada ENC(k0, (R1||C10)) encriptando el primer código de reto generado R1||C10 usando la clave de encriptado k0 y extrae una parte preestablecida (por ejemplo, 64 bits inferiores) de la primera información encriptada generada ENC(k0, (R1||C10)) para producir primera información relacionada con encriptado. En el paso S7, el dispositivo periférico 1 transmite la primera información relacionada con encriptado extraída al cuerpo principal 2.

El cuerpo principal 2 recibe la primera información relacionada con encriptado. En el paso S8, el cuerpo principal 2 verifica si la parte preestablecida (64 bits inferiores) de la primera información de comparación de encriptado generada en el paso S4 coincide con la primera información relacionada con encriptado recibida y por lo tanto autentica el dispositivo periférico 1.

En general, una parte quien pretenda fabricar ilegalmente un dispositivo periférico no conoce la clave de encriptado k0 o la primera constante C10 y por lo tanto no puede generar el primer código de reto o la primera información encriptada. Por lo tanto, en este caso, en general, en el paso S8 la parte preestablecida (64 bits inferiores) de la primera información de comparación de encriptado no coincide con la primera información relacionada con encriptado recibida. El dispositivo periférico 1 puede ser considerado así ilegal.

El dispositivo periférico 1 puede generar, en el paso S9, segunda información relacionada con código que se refiere a un código de reto (segundo código de reto) a usar para autenticar el cuerpo principal 2. En esta realización, el dispositivo periférico 1 genera un número aleatorio de 64 bits R2 por una rutina de número aleatorio en el paso y transmite el número aleatorio generado R2 como segunda información relacionada con código al cuerpo principal 2 junto con la primera información relacionada con encriptado en el paso S7.

El dispositivo periférico 1 genera un segundo código de reto de comparación en base a la segunda información relacionada con código R2. En este caso, el dispositivo periférico 1 lee, de la sección de almacenamiento 12, una segunda constante C20 correspondiente al número de tecla "0" como la información de identificación de clave de encriptado que se recibió en el paso S2. En el paso S10 el dispositivo periférico 1 genera un segundo código de reto de comparación R2||C20 colocando la segunda constante S20 después de la segunda información relacionada con código R2.

En el paso S11, el dispositivo periférico 1 genera segunda información de comparación de encriptado ENC(k0, (R2||C20)) encriptando el segundo código de reto de comparación R2||C20 usando la clave de encriptado k0 que se identifica utilizando el número de tecla "0" como la información de identificación de clave de encriptado.

En el paso S12, el cuerpo principal 2 genera un segundo código de reto R2||C20 colocando la segunda constante C20 después de la segunda información relacionada con código R2 que se recibió en el paso S7 y adquiere el segundo código de reto R2||C20. En el paso S13, el cuerpo principal 2 genera segunda información encriptada ENC(k0, (R2||C20)) encriptando el segundo código de reto generado R2||C20 usando la clave de encriptado k0, y extrae una parte preestablecida (64 bits inferiores) de la segunda información encriptada ENC(k0,(R2||C20)) para producir segunda información relacionada con encriptado. En el paso S14, el cuerpo principal 2 transmite la segunda información relacionada con encriptado extraída al dispositivo periférico 1.

Recibiendo la segunda información relacionada con encriptado del cuerpo principal 2, en el paso S15 el dispositivo periférico 1 juzga si la parte preestablecida (64 bits inferiores) de la segunda información de comparación de encriptado que se generó en el paso S11 coincide con la segunda información relacionada con encriptado recibida del cuerpo principal 2. En el paso S16, el dispositivo periférico 1 transmite un resultado del juicio al cuerpo principal 2.

Como se ha descrito anteriormente, si la parte preestablecida (64 bits inferiores) de la segunda información de comparación de encriptado que se generó en el paso S11 coincide con la segunda información relacionada con encriptado recibida del cuerpo principal 2, el dispositivo periférico 1 transmite la parte preestablecida propiamente dicha de la segunda información de comparación de encriptado que se generó en el paso S11 al cuerpo principal 2 como datos de éxito de autenticación.

Si la parte preestablecida (64 bits inferiores) de la segunda información de comparación de encriptado que se generó en el paso S11 no coincide con la segunda información relacionada con encriptado recibida del cuerpo principal 2, el dispositivo periférico 1 genera datos de fallo de autenticación negando cada bit de la parte preestablecida de la segunda información de comparación de encriptado que se generó en el paso S11 y transmite los datos de fallo de autenticación generados al cuerpo principal 2.

En el paso S17, el cuerpo principal 2 juzga si el cuerpo principal 2 propiamente dicho ha sido autenticado con éxito en base al resultado del juicio que se recibió en el paso S16. En esta realización, el cuerpo principal 2 compara la parte preestablecida de la segunda información encriptada que se transmitió en el paso S13 con la información del resultado del juicio que se recibió en el paso S16. Si coinciden entre sí, el cuerpo principal 2 juzga que ha sido autenticado con éxito. Si la clave de encriptado k0, por ejemplo, tiene escapado, el cuerpo principal 2 se recupera y la clave de encriptado, etc, almacenada en la sección de almacenamiento 22 se sustituyen (sobreescriben), por ejemplo, por una clave de encriptado k1 una primera constante C11, y una segunda constante C21 (cada una de las cuales se almacena en el dispositivo periférico 1 con anterioridad) que se identifican utilizando un número de tecla “1”. La información de identificación de clave de encriptado se cambia después a “1”. Esto hace posible actualizar la clave de encriptado, etc, sin necesidad de recoger dispositivos periféricos 1 (en el mercado hay muchos más dispositivos periféricos 1 que cuerpos principales 2).

Aunque el cuerpo principal 2 y el dispositivo periférico 1 están conectados entre sí, las comunicaciones representadas en la figura 6 se pueden realizar repetidas veces, es decir, cada vez que llega un tiempo preestablecido. Si el dispositivo periférico 1 no es autenticado en el paso S8, el cuerpo principal 2 puede volver al paso S1 y realizar de nuevo el proceso de la figura 6. Igualmente, si se halla en el paso S17 que el cuerpo principal 2 propiamente dicho no ha sido autenticado, el cuerpo principal 2 puede volver al paso S1 y realizar de nuevo el proceso de la figura 6.

Aunque la descripción anterior es tal que se transmiten partes de un primer o segundo código de reto y primera o segunda información encriptada que se utilizan para procesado de autenticación, uno de ellos se puede transmitir en su totalidad. Donde uno de ellos se puede transmitir en su totalidad, la carga de comunicación aumenta consiguientemente, pero el nivel de seguridad se puede incrementar haciendo un juicio de coincidencia/no coincidencia transmitiendo toda la primera o segunda información encriptada, por ejemplo.

Donde se transmite parte de un primer o segundo código de reto como primera o segunda información relacionada con código, el orden de la conexión de la primera o segunda información relacionada con código y la constante C no se limita al antes descrito “R||C” y puede ser “C||R”. Además, su orden de conexión en el proceso para autenticar el dispositivo periférico 1 por el cuerpo principal 2 (pasos S1-S8 en la figura 6) y el del proceso para autenticar el cuerpo principal 2 por el dispositivo periférico 1 (pasos S9-S17 en la figura 6) pueden ser diferentes uno de otro.

La sección de control 21 guarda un señalizador que indica un resultado de autenticación en la sección de almacenamiento 22. Por ejemplo, el señalizador se pone a “0” cuando el procesado de autenticación tiene éxito y a “1” cuando el procesado de autenticación ha fallado.

En esta realización, cada una de la sección de control 21 del cuerpo principal 2 y la sección de control 11 de la batería como el dispositivo periférico 1 realiza procesado de autenticación de nuevo si el procesado de autenticación recién realizado ha dado lugar a un fallo. Aunque el procesado de autenticación tenga éxito, cada una de las secciones de control 21 y 11 puede realizar procesado de autenticación de nuevo después de un lapso de tiempo preestablecido.

Otra característica importante de esta realización es que el proceso de autenticación realizado por la sección de control 21 depende de si la sección de control de potencia 27 recibe potencia de una fuente de alimentación externa. Por ejemplo, cuando se activa la potencia, la sección de control 21 verifica si la batería como el dispositivo periférico 1 está conectada o no a la sección de control de potencia 27. Si la batería está conectada a la sección de control de

potencia 27, la sección de control 21 comienza un proceso representado en la figura 7. Aunque la descripción siguiente se hará con el supuesto de que una zona de almacenamiento que servirá como un contador de fallos para retener el número de veces de fallos de autenticación consecutivos está fijada en la sección de almacenamiento 22, se puede disponer un contador de fallos en un registro de la CPU que opera como la sección de control 21.

En el paso S21, la sección de control 21 realiza procesado de autenticación de batería. En el paso S22, la sección de control 21 verifica si el procesado de autenticación de batería ha tenido éxito o no (es decir, si la batería ha sido considerada auténtica). Es decir, la sección de control 21 verifica si el señalizador relacionado con autenticación está o no puesto a "1" (es decir, el valor que indica que el procesado de autenticación realizado ha dado lugar a un fallo). Si se juzga que el procesado de autenticación ha fallado, en el paso S23 el contador de fallos se incrementa en uno. En el paso S24, la sección de control 21 juzga si la sección de control de potencia 27 recibe potencia o no de una fuente de alimentación externa. Si la sección de control de potencia 27 no recibe potencia de una fuente de alimentación externa, en el paso S25 la sección de control 21 establece el intervalo de repetición de procesado de autenticación a un primer valor de intervalo preestablecido (por ejemplo, 100 ms) y establece el valor umbral del número de veces de fallos de autenticación a un primer valor umbral (por ejemplo, 30). En el paso S26, la sección de control 21 verifica si el valor del contador de fallos supera o no el valor umbral. Si el valor del contador de fallos supera el valor umbral, en el paso S27 la sección de control 21 ejecuta un proceso de tiempo de fallo y el proceso termina. Es decir, la sección de control 21 ejecuta el proceso de tiempo de fallo si el procesado de autenticación ha fallado consecutivamente más del número de veces que es igual al valor umbral establecido y después corta la potencia del cuerpo principal 2.

Por otra parte, si se juzga en el paso S26 que el número de veces de fallos no ha excedido el valor umbral establecido, en el paso S28 la sección de control 21 suspende el proceso durante un tiempo que es igual al intervalo de repetición de procesado de autenticación. Después del transcurso de dicho tiempo, el proceso se vuelve al paso S21 y reinicia.

Si se juzga en el paso S24 que la sección de control de potencia 27 recibe potencia de una fuente de alimentación externa, en el paso S29 la sección de control 21 establece el intervalo de repetición de procesado de autenticación a un segundo valor de intervalo preestablecido (por ejemplo, 500 ms) y establece el valor umbral del número de veces de fallos de autenticación a un segundo valor umbral (por ejemplo, 600). Después, el proceso pasa al paso S26 y se sigue ejecutando.

Como se ha descrito anteriormente, el valor de intervalo de repetición preestablecido y el valor umbral del número de veces de fallos se cambian y el período durante el que el procesado de autenticación se repite se cambia por lo tanto dependiendo de si la sección de control de potencia 27 recibe o no potencia de una fuente de alimentación externa. Esta medida toma en consideración los casos en los que, por ejemplo, la sección de control 11 no puede operar si la batería secundaria de la sección funcional 14 casi no tiene energía residual aunque la batería sea auténtica. Si la sección de control 11 no está operando, aunque el cuerpo principal 2 (dispositivo de petición de autenticación) transmita un número aleatorio a la batería, la batería no puede transmitir información relacionada con encriptado y por lo tanto el cuerpo principal 2 juzga que la batería no ha sido autenticada. En vista de esto, en esta realización, aunque la sección de control de potencia 27 esté recibiendo potencia de una fuente de alimentación externa y la batería se esté cargando, el intervalo de procesado de autenticación se establece más largo y el número de veces de repeticiones de procesado de autenticación se hace más grande. Como resultado, si la batería está vacía al comienzo, el período de repetición de procesado de autenticación se prolonga de manera que la batería se cargue de manera que la sección de control 11 sea operativa.

Además, si se juzga en el paso S22 que la batería ha sido autenticada con éxito, en el paso S30 la sección de control 21 pone el contador de fallos a "0". Entonces, la sección de control 21 establece el intervalo de repetición de procesado de autenticación a un tercer valor de intervalo preestablecido (por ejemplo, 30 s) en el paso S31 y ejecuta un proceso de tiempo de éxito en el paso S32. El proceso 1 pasa al paso S28 y continúa ejecutándose.

Por ejemplo, el proceso de tiempo de fallo (paso S27) puede ser un proceso de ordenar a la sección de control de potencia 27 que corte la potencia para apagar por lo tanto el cuerpo principal 2 o un proceso de hacer que la sección de control de pantalla 24 produzca una visualización "Inutilizable" y detenga el procesado relacionado con juego.

Por ejemplo, el proceso de tiempo de éxito (paso S32) puede ser un proceso de comenzar un procesado relacionado con juego. Si el procesado relacionado con juego ya ha iniciado, no siempre es necesario realizar ningún procesado en el proceso de tiempo de éxito.

La zona de almacenamiento como el contador de fallos se puede fijar en una memoria no volátil de la sección de almacenamiento 22 de manera que su contenido se mantenga incluso después de un corte de potencia. Esto evita el hecho de continuar jugando a un juego intermitentemente poniendo a cero el contador de fallos a la mitad, por ejemplo, conectando y desconectando una fuente de alimentación externa al cuerpo principal 2 o suspendiendo regularmente un juego y conectando de nuevo la potencia.

Como se ha descrito anteriormente, la realización proporciona un proceso en el que se consideran problemas específicos de la autenticación de una batería, tal como un problema de que la autenticación de una batería como una unidad principal para suministrar potencia se inhabilita porque la batería no todavía ha sido cargada suficientemente.

Aunque la descripción anterior se dirige al caso de que el cuerpo principal 2 es una máquina recreativa doméstica, la invención no se limita a tal caso. Por ejemplo, es posible que el dispositivo periférico 1 sea una batería y el cuerpo principal 2 sea su cargador. En este caso, el cuerpo principal 2 no siempre tiene que estar equipado con la sección de manipulación 23 y la sección de control de pantalla 24. Y el proceso de tiempo de fallo y el proceso de tiempo de éxito que se ejecutan por la sección de control 21 pueden ser, por ejemplo, suspensión de carga e inicio de carga, respectivamente.

Aunque la presente invención se describe en términos de realizaciones preferidas o ejemplares, no se limita a ellas.

REIVINDICACIONES

1. Un sistema de autenticación que incluye una batería y un dispositivo de petición de autenticación para autenticar la batería, conteniendo la batería y el dispositivo de petición de autenticación una clave común de encriptado, donde:

el dispositivo de petición de autenticación genera primera información relacionada con código para transmisión a la batería, adquiere un primer código de reto de comparación en base a la primera información relacionada con código, y genera primera información de comparación de encriptado encriptando el primer código de reto de comparación usando la clave de encriptado;

la batería recibe la primera información relacionada con código, adquiere un primer código de reto en base a la primera información relacionada con código recibida, genera primera información encriptada encriptando el primer código de reto adquirido usando la clave de encriptado, y transmite primera información relacionada con encriptado relativa a la primera información encriptada generada al dispositivo de petición de autenticación;

el dispositivo de petición de autenticación determina si autenticar la batería comparando la primera información relacionada con encriptado recibida con la primera información de comparación relacionada con encriptado relativa a la primera información de comparación de encriptado generada; y

la primera información relacionada con código es parte del primer código de reto y/o la primera información relacionada con encriptado es parte de la primera información encriptada.

2. El sistema de autenticación según la reivindicación 1, donde:

el dispositivo de petición de autenticación incluye una sección de conexión de batería conectada a la batería y una sección de recepción de potencia para recibir potencia de una fuente de alimentación externa cuando está conectada a la fuente de alimentación externa; y

el dispositivo de petición de autenticación ejecuta un proceso de autenticación para autenticar la batería conectada a la sección de conexión de batería de manera que cambie el proceso de autenticación dependiendo de si la sección de recepción de potencia está recibiendo potencia o no de la fuente de alimentación externa.

3. El sistema de autenticación según la reivindicación 1, donde:

el dispositivo de petición de autenticación opera para transmitir un resultado de autenticación a la batería, mediante una instrucción almacenada en un circuito de memoria.

4. El sistema de autenticación según la reivindicación 1, donde:

la batería opera para autenticar el dispositivo de petición de autenticación, y para transmitir el resultado de autenticación al dispositivo de petición de autenticación, mediante una instrucción almacenada en un circuito de memoria.

5. Una batería a conectar a un dispositivo de petición de autenticación y para transmitir información referente a autenticación en respuesta a una petición de autenticación del dispositivo de petición de autenticación, incluyendo:

una porción que recibe primera información relacionada con código del dispositivo de petición de autenticación;

una porción de adquisición de código que adquiere un primer código de reto en base a la primera información relacionada con código recibida;

una porción que genera primera información encriptada encriptando el primer código de reto; y una porción que transmite primera información relacionada con encriptidado relativa a la primera información encriptada generada al dispositivo de petición de autenticación,

donde la primera información relacionada con código es parte del primer código de reto y/o la primera información relacionada con encriptado es parte de la primera información encriptada.

6. La batería según la reivindicación 5, donde:

la primera información relacionada con código es parte del primer código de reto; y

la porción de adquisición de código genera y adquiere un primer código de reto conectando la primera información relacionada con código a información de parte común mantenida por la batería y el dispositivo de petición de encriptado.

7. La batería según la reivindicación 5, incluyendo además:

una porción que genera segunda información relacionada con código y transmite la información al dispositivo de petición de autenticación para autenticar el dispositivo de petición de autenticación;

una porción que recibe, del dispositivo de petición de autenticación, parte de información encriptada obtenida encriptando un segundo código de reto;

una porción que adquiere un segundo código de reto de comparación en base a la segunda información relacionada con código;

una porción que genera segunda información de comparación de encriptado encriptando el segundo código de reto de comparación generado; y

una porción que extrae parte, correspondiente a la parte de la segunda información encriptada recibida, de la segunda información de comparación de encriptado para producir segunda información parcial de comparación, y para comparar la segunda información parcial de comparación con la parte de la segunda información encriptada recibida, donde:

si la segunda información parcial de comparación difiere de la parte de la segunda información encriptada recibida, la batería transmite un valor correspondiente a un resultado de una primera operación lógica preestablecida realizada en la segunda información parcial de comparación; y

si la segunda información parcial de comparación coincide con la parte de la segunda información encriptada recibida, la batería transmite un valor correspondiente a un resultado de una segunda operación lógica preestablecida realizada en la segunda información parcial de comparación.

8. La batería según la reivindicación 5, donde:

la batería opera para recibir un resultado de autenticación del dispositivo de petición de autenticación, mediante una instrucción almacenada en un circuito de memoria.

9. la batería según la reivindicación 5, donde:

la batería opera para autenticar el dispositivo de petición de autenticación, y para transmitir el resultado de autenticación al dispositivo de petición de autenticación mediante una instrucción almacenada en un circuito de memoria.

10. Un método de autenticación ejecutado en una batería conectada a un dispositivo de petición de autenticación, incluyendo los pasos de:

recibir primera información relacionada con código del dispositivo de petición de autenticación;

adquirir un primer código de reto en base a la primera información relacionada con código recibida;

generar primera información encriptada encriptando el primer código de reto; y

transmitir primera información relacionada con encriptado relativa a la primera información encriptada generada al dispositivo de petición de autenticación,

donde la primera información relacionada con código es parte del primer código de reto y/o la primera información relacionada con encriptado es parte de la primera información encriptada.

11. El método de autenticación según la reivindicación 10, donde:

el dispositivo de petición de autenticación incluye una sección de conexión de batería conectada a la batería y una sección de recepción de potencia que recibirá potencia de una fuente de alimentación externa cuando esté conectada a la fuente de alimentación externa; y

el dispositivo de petición de autenticación cambia un proceso de autenticación dependiendo de si la sección de recepción de potencia está recibiendo potencia o no de la fuente de alimentación externa.

FIG. 1

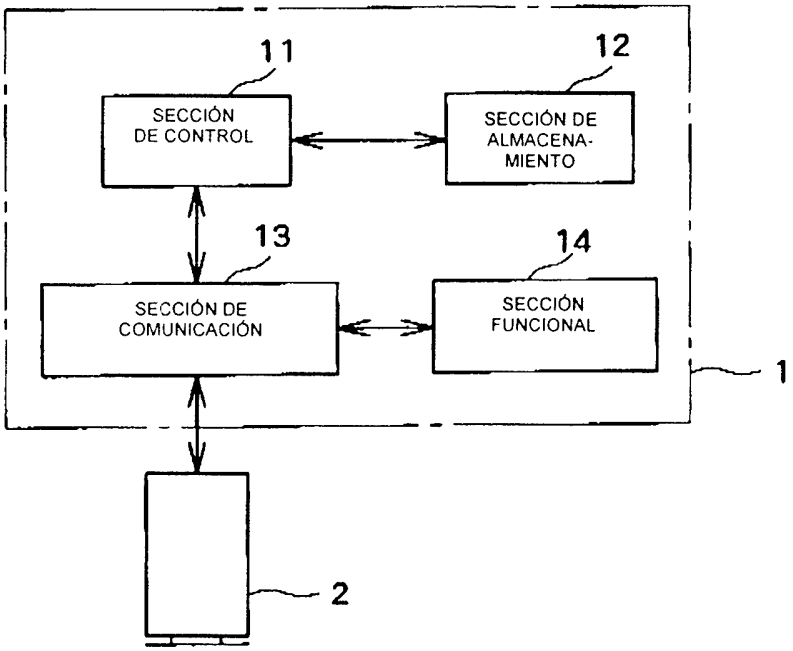

11
SECCIÓN DE CONTROL
12
SECCIÓN DE ALMACENA-MIENTO
13
SECCIÓN DE COMUNICACIÓN
14
SECCIÓN FUNCIONAL
1
2

FIG. 2

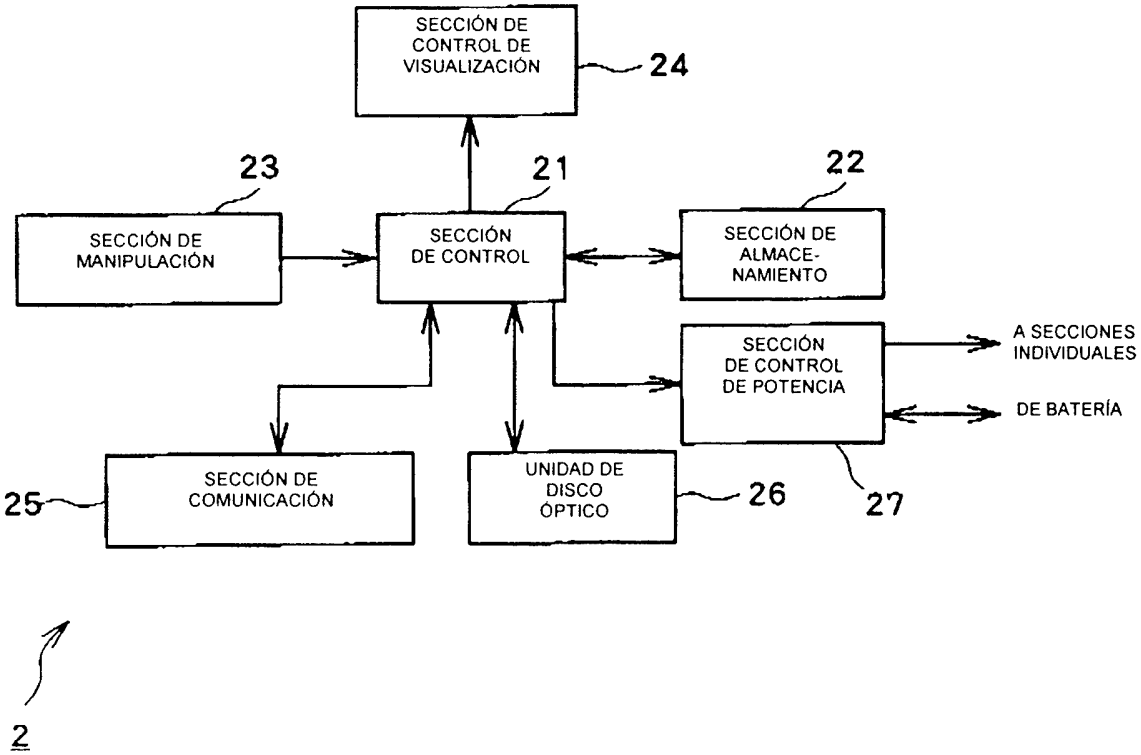

SECCIÓN DE CONTROL DE VISUALIZACIÓN
24
23
SECCIÓN DE MANIPULACIÓN
21
SECCIÓN DE CONTROL
22
SECCIÓN DE ALMACE-NAMIENTO
SECCIÓN DE CONTROL DE POTENCIA
A SECCIONES INDIVIDUALES
DE BATERÍA
25
SECCIÓN DE COMUNICACIÓN
UNIDAD DE DISCO ÓPTICO
26
27
2

FIG. 3

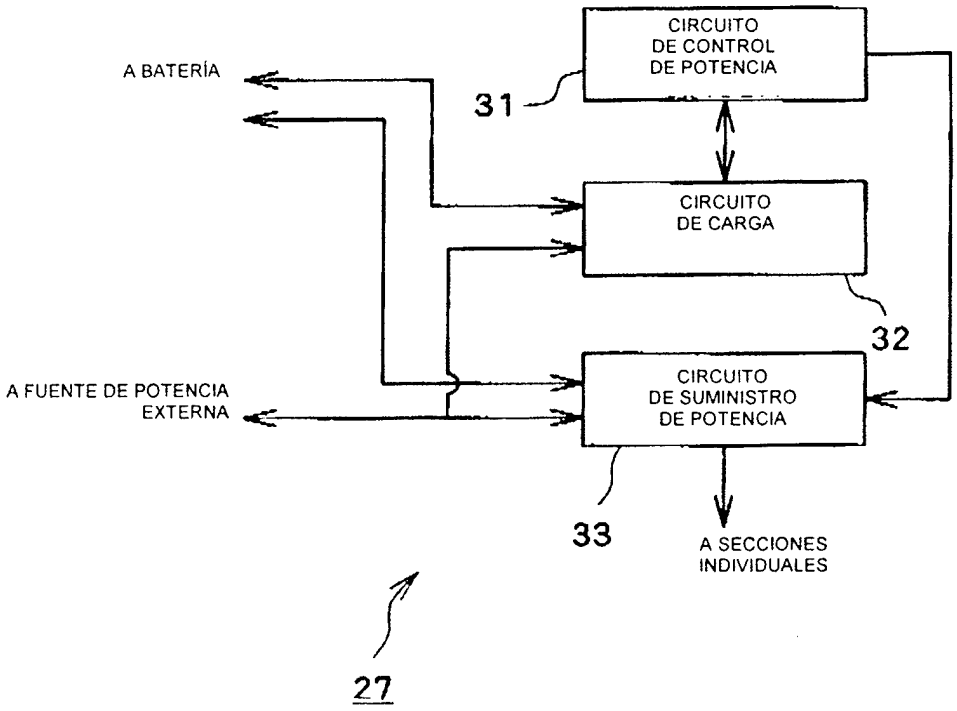

A BATERÍA
CIRCUITO DE CONTROL DE POTENCIA
31
CIRCUITO DE CARGA
32
A FUENTE DE POTENCIA EXTERNA
CIRCUITO DE SUMINISTRO DE POTENCIA
33
A SECCIONES INDIVIDUALES
27

FIG. 4

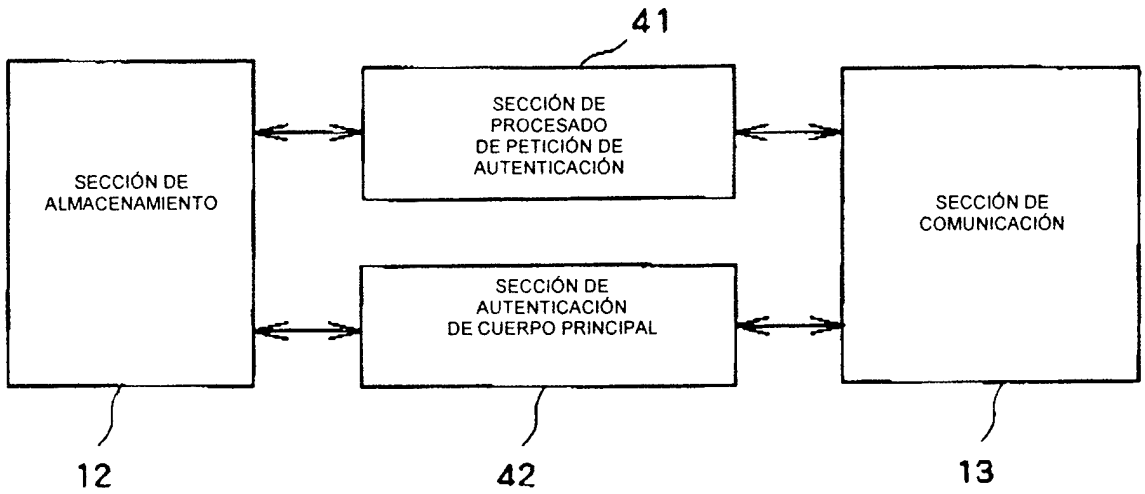

41
SECCIÓN DE ALMACENAMIENTO
SECCIÓN DE PROCESADO DE PETICIÓN DE AUTENTICACIÓN
SECCIÓN DE AUTENTICACIÓN DE CUERPO PRINCIPAL
SECCIÓN DE COMUNICACIÓN
12
42
13

FIG. 5

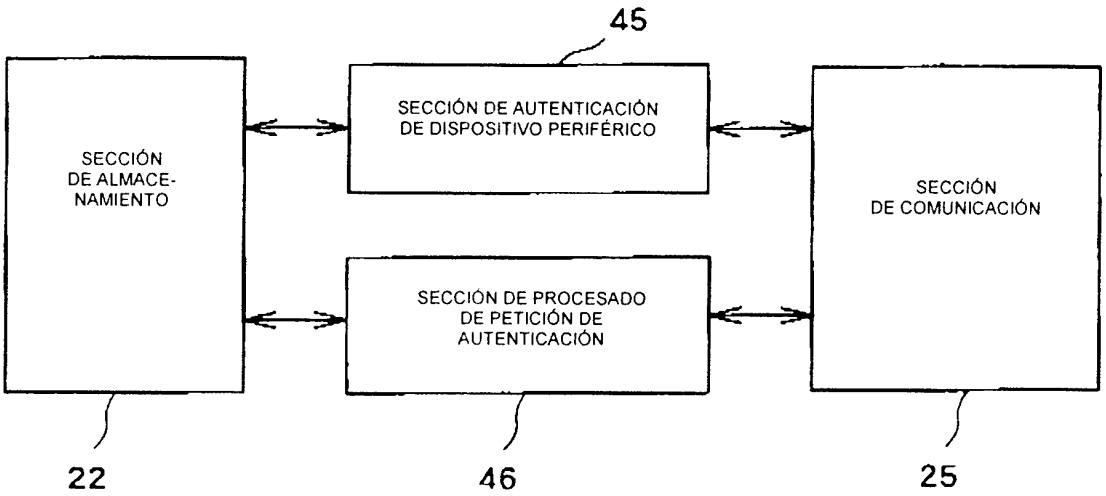

45
SECCIÓN DE AUTENTICACIÓN DE DISPOSITIVO PERIFÉRICO
SECCIÓN DE ALMACE-NAMIENTO
SECCIÓN DE COMUNICACIÓN
SECCIÓN DE PROCESADO DE PETICIÓN DE AUTENTICACIÓN
22
46
25

FIG. 6

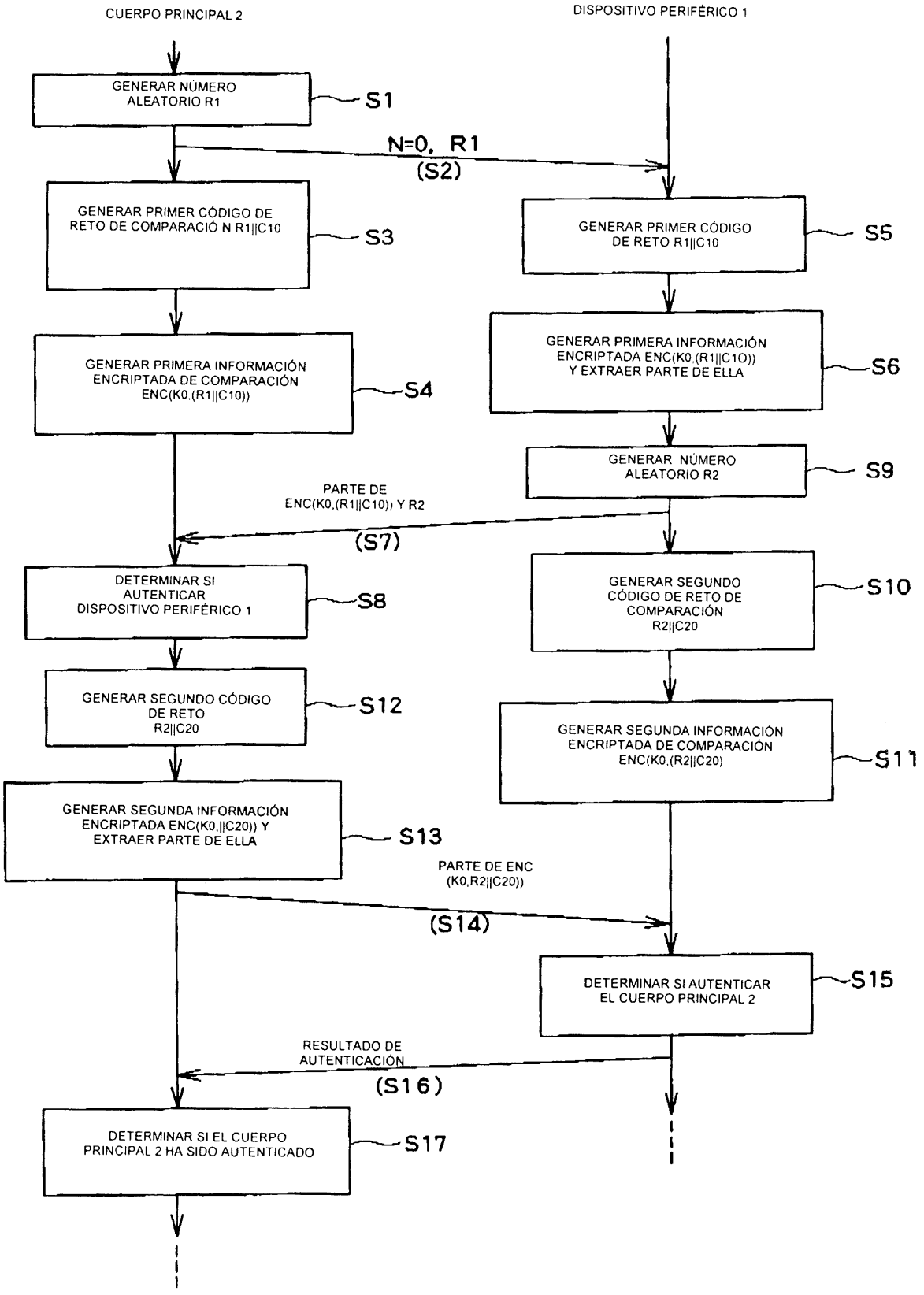
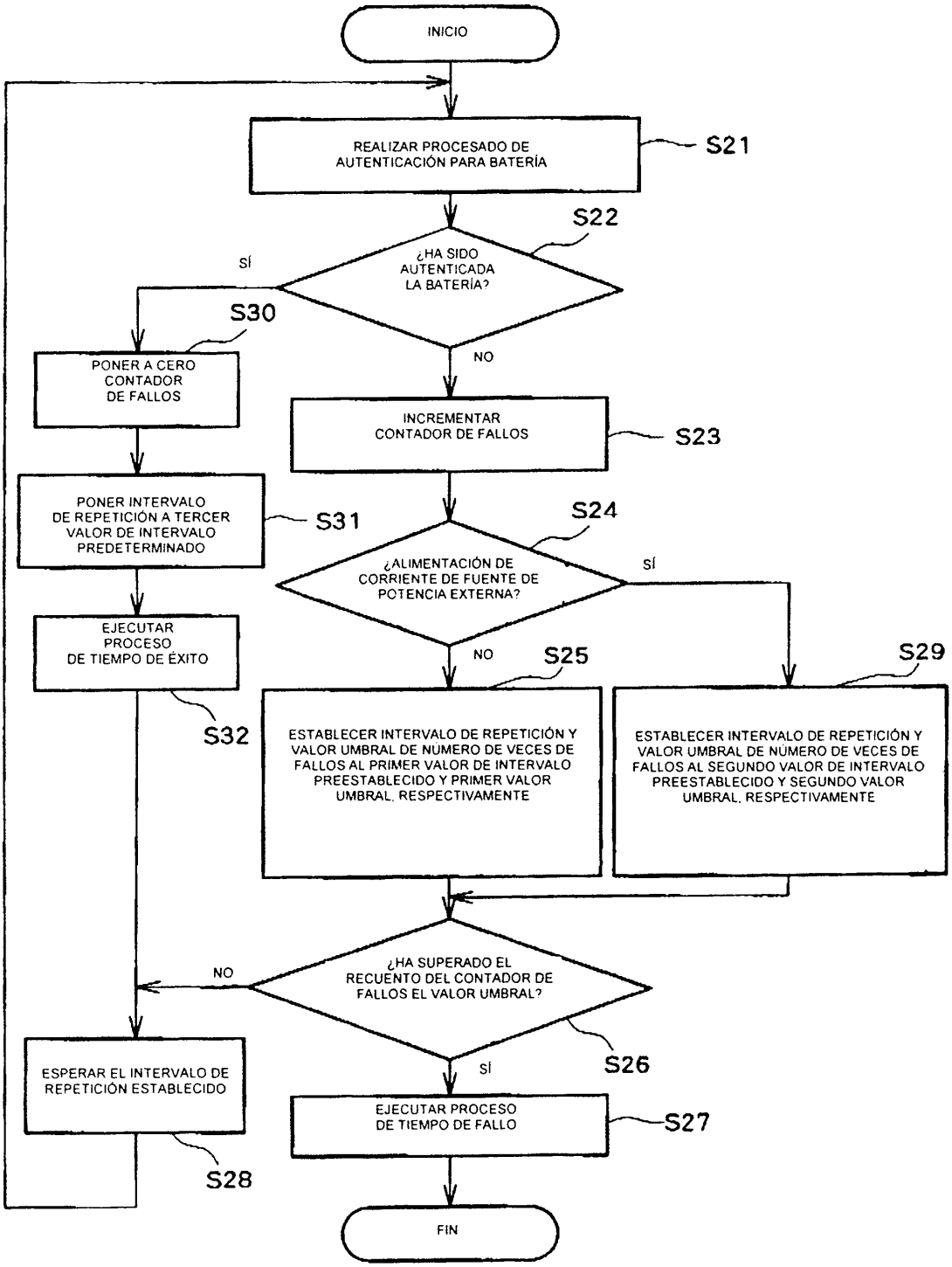

CUERPO PRINCIPAL 2
DISPOSITIVO PERIFÉRICO 1
GENERAR NÚMERO ALEATORIO R1
S1
N=0, R1
(S2)
GENERAR PRIMER CÓDIGO DE RETO DE COMPARACIÓ N R1||C10
S3
GENERAR PRIMERA INFORMACIÓN ENCRIPTADA DE COMPARACIÓN ENC(K0,(R1||C10))
S4
GENERAR PRIMER CÓDIGO DE RETO R1||C10
S5
GENERAR PRIMERA INFORMACIÓN ENCRIPTADA ENC(K0,(R1||C1O)) Y EXTRAER PARTE DE ELLA
S6
GENERAR NÚMERO ALEATORIO R2
S9
PARTE DE ENC(K0,(R1||C10)) Y R2
(S7)
DETERMINAR SI AUTENTICAR DISPOSITIVO PERIFÉRICO 1
S8
GENERAR SEGUNDO CÓDIGO DE RETO DE COMPARACIÓN R2||C20
S10
GENERAR SEGUNDO CÓDIGO DE RETO R2||C20
S12
GENERAR SEGUNDA INFORMACIÓN ENCRIPTADA DE COMPARACIÓN ENC(K0,(R2||C20)
S11
GENERAR SEGUNDA INFORMACIÓN ENCRIPTADA ENC(K0,||C20)) Y EXTRAER PARTE DE ELLA
S13
PARTE DE ENC (K0,R2||C20))
(S14)
DETERMINAR SI AUTENTICAR EL CUERPO PRINCIPAL 2
S15
RESULTADO DE AUTENTICACIÓN
(S16)
DETERMINAR SI EL CUERPO PRINCIPAL 2 HA SIDO AUTENTICADO
S17

FIG. 7


INICIO
REALIZAR PROCESADO DE AUTENTICACIÓN PARA BATERÍA
S21
S22
¿HA SIDO AUTENTICADA LA BATERÍA?
SÍ
NO
S30
PONER A CERO CONTADOR DE FALLOS
INCREMENTAR CONTADOR DE FALLOS
S23
PONER INTERVALO DE REPETICIÓN A TERCER VALOR DE INTERVALO PREDETERMINADO
S31
S24
¿ALIMENTACIÓN DE CORRIENTE DE FUENTE DE POTENCIA EXTERNA?
SÍ
NO
EJECUTAR PROCESO DE TIEMPO DE ÉXITO
S25
S29
S32
ESTABLECER INTERVALO DE REPETICIÓN Y VALOR UMBRAL DE NÚMERO DE VECES DE FALLOS AL PRIMER VALOR DE INTERVALO PREESTABLECIDO Y PRIMER VALOR UMBRAL, RESPECTIVAMENTE
ESTABLECER INTERVALO DE REPETICIÓN Y VALOR UMBRAL DE NÚMERO DE VECES DE FALLOS AL SEGUNDO VALOR DE INTERVALO PREESTABLECIDO Y SEGUNDO VALOR UMBRAL, RESPECTIVAMENTE
¿HA SUPERADO EL RECUENTO DEL CONTADOR DE FALLOS EL VALOR UMBRAL?
NO
SÍ
S26
ESPERAR EL INTERVALO DE REPETICIÓN ESTABLECIDO
EJECUTAR PROCESO DE TIEMPO DE FALLO
S27
S28
FIN

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 301 311

(21) Nº de solicitud: 200502919

(22) Fecha de presentación de la solicitud: **25.11.2005**

(32) Fecha de prioridad: **26.11.2004**
26.11.2004
09.09.2005

INFORME SOBRE EL ESTADO DE LA TÉCNICA

(51) **Int. Cl.:** Ver hoja adicional

DOCUMENTOS RELEVANTES

Categoría	Documentos citados	Reivindicaciones afectadas
A	EP 0809379 A2 (MATSUSHITA ELECTRIC IND CO LTD) 26.11.1997	1,3,6
A	US 6769060 B1 (DENT et al.) 27.07.2004	1,3,6
A	WO 9958987 A1 (TAK SEUNG HO) 18.11.1999	1,3,6
A	US 2002025046 A1 (LIN et al.) 28.02.2002	1,3,6

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
30.05.2008	Mª C. González Vasserot	1/2

CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD

H04L 9/32 (2006.01)
H02J 7/04 (2006.01)
G06F 3/023 (2006.01)