

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 441 370**

51 Int. Cl.:

G06K 19/073 (2006.01)
G08B 21/00 (2006.01)
G06K 19/07 (2006.01)
G06F 1/16 (2006.01)
G06F 21/00 (2013.01)
G06F 3/033 (2013.01)
H04M 1/725 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **10.08.2009 E 09805661 (7)**

97 Fecha y número de publicación de la concesión europea: **02.10.2013 EP 2321809**

54 Título: **Mecanismo de detección direccional y autenticación de comunicaciones**

30 Prioridad:

08.08.2008 US 87633 P

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

04.02.2014

73 Titular/es:

**ASSA ABLOY AB (100.0%)
Klarabergsviadukten 90 P.O. Box 70340
107 23 Stockholm, SE**

72 Inventor/es:

DAVIS, MICHAEL

74 Agente/Representante:

CURELL AGUILÁ, Mireia

ES 2 441 370 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

Mecanismo de detección direccional y autenticación de comunicaciones.

5 **Campo de la invención**

La presente invención se refiere en general a la detección del movimiento de tarjetas y a la utilización de dicha información de detección en relación con el control del funcionamiento de las mismas.

10 **Antecedentes**

Los sistemas de Identificación por Radiofrecuencia (RFID) usan un lector de RFID para detectar inalámbricamente la presencia de una etiqueta de RFID próxima y leer un código de identificación almacenado en la etiqueta. El código de identificación de la etiqueta de RFID se puede usar para controlar el acceso a un recurso protegido al permitir el acceso únicamente cuando se detecte una etiqueta de RFID que tenga un código de identificación autorizado. En general, la etiqueta de RFID autorizada se emite para un usuario autorizado con el fin de garantizar que solamente el usuario autorizado tenga acceso al recurso protegido. No obstante, si la etiqueta de RFID autorizada se pierde o es robada, la misma puede ser presentada por un usuario no autorizado para acceder al recurso protegido.

Los sistemas de RFID instalados disponibles actualmente usan una variedad de diferentes métodos complejos de codificación y señalización, algunos de los cuales son privativos. Las etiquetas de RFID usadas con estos sistemas adoptan dos formas – tarjetas y llaveros. La codificación que estos programadores en *leasing* pueden insertar se limita a ciertos alcances y formatos específicos, permitidos por cada uno de los distribuidores y controlados por unos medios cifrados, que son suministrados por cada una de las empresas.

En un intento por evitar el fraude existen propuestas para integrar dispositivos de RFID en billetes, tarjetas de crédito, tarjetas de débito, tarjetas comerciales de fidelización y otros objetos de alto valor. La idea es que una persona que lleva un objeto con toda la información de autenticación debe ser el verdadero propietario del objeto. En la medida en la que cada vez más objetos están equipados con estos dispositivos de RFID, las probabilidades de que a alguien le roben información personal a partir de los mismos aumenta. Típicamente, los objetos de alto valor con dispositivos de RFID integrados son portadores de información extremadamente sensible (por ejemplo, números de seguridad social, direcciones, números de cuentas bancarias, códigos pin de ATM, nombres, etcétera). Si este tipo de información es robada, puede verse comprometida la identidad completa del titular del objeto. Esto plantea una amenaza muy seria para la población general que es portadora de objetos equipados con un dispositivo de RFID. El documento EP 1607723A1 da a conocer un método de control de un circuito integrado mediante la recepción de una cierta señal de movimiento en un mecanismo de detección direccional.

Un aspecto de la presente invención consiste por lo tanto en proporcionar un dispositivo de RFID que restringe las transmisiones de datos hasta que el mismo ha sido movido de una forma particular por el titular del dispositivo de RFID. Al requerir que el titular del dispositivo mueva el dispositivo de RFID de una cierta forma antes de liberar sus datos sensibles, el dispositivo de RFID limita potencialmente su uso, y por lo tanto la liberación de datos sensibles, a casos en los que realmente un usuario autorizado está presentando la tarjeta resueltamente a un lector (suponiendo que un usuario no autorizado no conoce la secuencia de movimiento predeterminada que desbloquea los datos sensibles del dispositivo de RFID). Esto ayuda a minimizar o a evitar completamente que terceros roben datos del dispositivo de RFID a no ser que el titular del dispositivo de RFID lo esté moviendo en la secuencia predeterminada de movimientos. En otras palabras, se impide que un atacante pase ilícitamente un lector por las proximidades del dispositivo de RFID del usuario para extraer datos del usuario sin su consentimiento.

De acuerdo con por lo menos una forma de realización de la presente invención, un dispositivo de RFID está equipado con un mecanismo de detección direccional tal como un Sistema Micro-electro-mecánico (MEMS) o acelerómetro que tiene la capacidad de detectar el movimiento del dispositivo de RFID en una o más direcciones y/o rotaciones del dispositivo de RFID en una o más direcciones de rotación. La presente invención va dirigida en general a un método, un aparato, y un sistema que utiliza un componente de detección direccional en combinación con un dispositivo de RFID para prohibir sustancialmente la extracción ilícita de datos de dispositivos de RFID. Tal como puede apreciarse, un dispositivo de RFID se puede implementar como parte de una tarjeta de ID/acceso, una tarjeta inteligente, una etiqueta de RF, un teléfono celular, un Asistente Personal Digital (PDA), un llavero, y similares.

De acuerdo con una forma de realización de la presente invención, se proporciona un sistema que evita sustancialmente la extracción ilegítima de datos de un dispositivo de RFID. Los datos pueden presentar grados de sensibilidad. Por ejemplo, los datos altamente sensibles pueden incluir, aunque sin carácter limitativo, números de cuentas bancarias, números de seguridad social, códigos PIN, contraseñas, claves, ID exclusivas de RFID, esquemas de cifrado, etcétera. Los datos menos sensibles pueden incluir, aunque sin carácter limitativo, el nombre de usuario, el ID de fabricante, el puesto de trabajo, y otros.

65

5 Los MEMS son la integración de elementos mecánicos, sensores, accionadores, y electrónica en un sustrato común de silicio a través de la tecnología de microfabricación. Mientras que la electrónica se fabrica usando secuencias de procesos de circuitos integrados (IC) (por ejemplo, procesos CMOS, Bipolares, o BICMOS), los componentes micromecánicos se fabrican usando procesos de "micromecanización" compatibles que eliminan selectivamente partes de la oblea de silicio por ataque químico o añaden capas estructurales nuevas para formar los dispositivos mecánicos y electromecánicos).

10 Los MEMS tienen la capacidad de combinar la microelectrónica basada en silicio con la tecnología de micromecanización, posibilitando la realización de sistemas en un chip completos. MEMS es una tecnología habilitadora que permite el desarrollo de productos inteligentes, que potencia la capacidad computacional de la microelectrónica con las capacidades de percepción y control de microsensores y microaccionadores y que amplía el espacio de posibles diseños y aplicaciones.

15 Puesto que los dispositivos MEMS se fabrican usando técnicas de fabricación por lotes, similares a las usadas para circuitos integrados, en un pequeño chip de silicio se pueden aplicar, con un coste relativamente bajo, niveles sin precedentes de funcionalidad, fiabilidad y sofisticación.

20 De acuerdo con por lo menos algunas formas de realización de la presente invención, el dispositivo MEMS se puede proporcionar en forma de una parte integral del chip de procesado que se usa también para controlar la funcionalidad de comunicación de RF del dispositivo de RFID. Más específicamente, un solo chip puede ser responsable de ejecutar el procesado tradicional del dispositivo de RFID así como de controlar si se permite que el dispositivo de RFID responda a una solicitud de datos de un lector (o incluso habilitar a la antena para que responda a cualquier tipo de campo de RF). A no ser que el dispositivo MEMS detecte la secuencia correcta de movimientos (por ejemplo, rotaciones, movimientos deslizantes, etcétera), al procesador no se le permitirá revelar ningún dato sensible de su ubicación de almacenamiento en el dispositivo de RFID. De acuerdo con por lo menos una forma de realización de la presente invención, en el dispositivo de RFID se puede proporcionar un conmutador (por ejemplo, un conmutador lógico, un conmutador mecánico, un conmutador electromecánico, un conmutador eléctrico, o similares) que inhiba al dispositivo de RFID para que no responda a ninguna energización por parte de un lector o similar a no ser que se detecte el movimiento o secuencia de movimientos predeterminados en el dispositivo de RFID. De este modo, el dispositivo de RFID está habilitado para controlar unilateralmente si proporciona cualesquiera datos a una fuente solicitante, sobre la base de si se ha detectado el movimiento predeterminado.

35 De acuerdo con por lo menos algunas formas de realización de la presente invención, un usuario del dispositivo de RFID también podría introducir contraseñas usando un símil de cerradura con combinación. Por ejemplo, una contraseña se podría corresponder con el giro del dispositivo de RFID a la derecha, a continuación de vuelta a la posición original, a continuación a la derecha, etcétera. Así, aunque la combinación de contraseña se usa para permitir que el dispositivo de RFID transmita datos a un lector, el dispositivo de RFID también puede enviar los resultados del movimiento detectado (es decir, el dispositivo de RFID puede enviar al lector la combinación de derecha-inicio-derecha, probablemente en forma de datos binarios). A continuación, el lector puede analizar la información de movimiento como una contraseña adicional para verificar la identidad del dispositivo de RFID y el titular del dispositivo de RFID. Si o bien la información de la tarjeta o bien la contraseña basada en el movimiento no es válida, entonces el lector puede determinar que al dispositivo de RFID no se le concede acceso al recurso protegido por el lector. De este modo, la contraseña proporcionada al lector como consecuencia de detectar movimiento se puede usar para representar algo que el usuario conoce además del objeto (dispositivo de RFID) que está llevando el usuario, proporcionándose así dos capas de seguridad.

50 Este paradigma de seguridad de dos capas se puede implementar con un lector tradicional que no disponga necesariamente de un teclado. Si la tarjeta de un usuario se pierde o se ve comprometida, la misma no será utilizable por ningún otro usuario que no conozca la contraseña basada en el movimiento.

55 De acuerdo con otras formas de realización de la presente invención, la "información de movimiento" capturada por el mecanismo de detección direccional también se puede corresponder con ciertos mensajes (por ejemplo, se puede proporcionar una tabla que establezca correspondencias de ciertas secuencias de movimiento con ciertos mensajes). Por consiguiente, el dispositivo de RFID puede enviar o bien el mensaje correspondiente o bien la información de movimiento capturada al lector, en donde la misma es analizada. El mensaje puede indicar, por ejemplo, que el titular del dispositivo de RFID se encuentra bajo coacción. Tal como pueden apreciar los expertos en la materia, se pueden establecer correspondencias de otras secuencias de movimientos con diferentes mensajes para proporcionar otras indicaciones sobre el titular del dispositivo de RFID. En algunas formas de realización, la tabla se puede mantener en el dispositivo de RFID. En algunas formas de realización, la tabla se puede mantener en el lector. En algunas formas de realización, la tabla se puede mantener en una combinación del dispositivo de RFID y el lector.

65 De acuerdo con todavía otras formas de realización de la presente invención, la integración de un mecanismo de detección direccional en un chip se puede aprovechar en otras aplicaciones, tales como en aplicaciones de comunicación de móviles y de teléfonos celulares. Más específicamente, una tarjeta SIM o plataforma de procesado similar se puede adaptar para incluir un mecanismo de detección direccional que actúe como una entrada a la

5 tarjeta. De este modo, se puede permitir que un usuario del dispositivo de comunicación móvil controle el funcionamiento del dispositivo de comunicación móvil (por ejemplo, hacer una llamada, responder a una llamada, rechazar una llamada, etcétera) simplemente agitando el dispositivo de comunicación móvil o moviendo el dispositivo de comunicación móvil en un patrón predeterminado de movimiento. Todavía en otras formas de realización, un usuario puede simplemente agitar o dar golpecitos a su dispositivo móvil cuando se encuentre ocupado en una llamada con otro usuario o cuando se encuentre ocupado haciendo otra cosa (por ejemplo, durante una reunión). El agitado o el golpeteo en el dispositivo móvil puede provocar que este último genere un mensaje de texto predeterminado que se transmite de vuelta al llamante, informando a este último de que el destinatario deseado del mensaje está ocupado y devolverá la llamada más tarde. En otras formas de realización, se puede permitir que un usuario localice el menú de servicios y aplicaciones proporcionado en el dispositivo móvil simplemente agitando o dando golpecitos al dispositivo móvil.

15 Todavía en otras formas de realización se proporciona una unidad combinada de acelerómetro y giróscopo que comprende en general: una masa de prueba; medios de accionamiento primarios que pueden funcionar para accionar la masa de prueba a lo largo de un eje primario; medios de accionamiento secundarios que pueden funcionar para accionar la masa de prueba a lo largo de un eje secundario; medios sensores secundarios que pueden funcionar para detectar la posición de la masa de prueba a lo largo del eje secundario; y medios sensores primarios que pueden funcionar para detectar la posición de la masa de prueba a lo largo del eje primario, en donde se establecen bucles de realimentación-fuerza $\Sigma\Delta$ tanto para el eje secundario como para el eje primario.

20 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde la unidad de acelerómetro y giróscopo es una unidad MEMS de acelerómetro y giróscopo.

25 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde tanto los medios de accionamiento primarios como los medios sensores primarios son condensadores de tipo *comb-drive*.

30 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde se proporcionan condensadores independientes de tipo *comb-drive* para el accionamiento y para la lectura.

35 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo, en donde se usa el multiplexado en el tiempo para permitir el uso de los mismos condensadores de tipo *comb-drive* tanto para el accionamiento como para la lectura.

Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde tanto los medios de accionamiento secundarios como los medios sensores secundarios son condensadores diferenciales de placas paralelas.

40 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde se proporcionan condensadores diferenciales independientes de placas paralelas para el accionamiento y para la lectura.

45 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde se usa el multiplexado en el tiempo para permitir la utilización de los mismos condensadores diferenciales de placas paralelas tanto para el accionamiento como para la lectura.

50 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde se proporcionan bucles independientes de realimentación-fuerza $\Sigma\Delta$ para el modo primario y el modo secundario.

Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde el bucle primario tiene una entrada extra V_{jn} .

55 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde cada bucle incorpora un filtro eléctrico.

Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde al final de cada bucle, se proporciona un cuantificador para entregar valores de salida digitales.

60 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde cada bucle contiene un trayecto de realimentación mecánica.

Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde se proporciona también un trayecto de realimentación eléctrica.

65

Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo según la reivindicación 14, en donde los bucles de realimentación eléctrica están provistos de filtros eléctricos adicionales.

5 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde cada filtro adicional tiene los mismos polos que los primeros filtros.

Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde cada filtro adicional tiene ceros diferentes a los primeros filtros.

10 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde se proporciona un filtro de controlador adicional para estabilizar el bucle.

15 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde la unidad está provista además de medios de accionamiento terciarios que pueden funcionar para accionar la masa de prueba a lo largo de un eje terciario y/o medios sensores terciarios que pueden funcionar para detectar la posición de la masa de prueba a lo largo del eje terciario.

20 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde el eje terciario es sustancialmente perpendicular al plano que contiene los ejes primario y secundario.

Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde tanto los medios de accionamiento terciarios como los medios sensores terciarios son condensadores de tipo *comb-drive*.

25 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde se pueden proporcionar condensadores independientes de tipo *comb-drive* para el accionamiento y para la lectura.

30 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo, en donde se puede usar el multiplexado en el tiempo para permitir la utilización de los mismos condensadores de tipo *comb-drive* tanto para el accionamiento como para la lectura.

35 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde los dos conjuntos de ramas que comprenden los condensadores de tipo *comb-drive* pueden ser de dimensiones diferentes a lo largo del eje terciario.

40 Otro aspecto de la presente invención consiste en proporcionar una unidad combinada de acelerómetro y giróscopo en donde la unidad se hace funcionar en un modo en el que se establece un bucle de realimentación-fuerza $\Sigma\Delta$ para solamente uno del eje secundario y el eje primario.

Otro aspecto de la presente invención consiste en proporcionar un grupo sensor que comprende una o más unidades combinadas de acelerómetro y giróscopo.

45 Otro aspecto de la presente invención consiste en proporcionar un grupo sensor en el que el grupo puede comprender adicionalmente uno o más acelerómetros dedicados de un solo eje o de múltiples ejes y/o uno o más giróscopos dedicados de un solo eje o de múltiples ejes.

50 Otro aspecto de la presente invención consiste en proporcionar un método de funcionamiento de una unidad combinada de acelerómetro y giróscopo que tiene una masa de prueba; medios de accionamiento primarios que pueden funcionar para accionar la masa de prueba a lo largo de un eje primario; medios de accionamiento secundarios que pueden funcionar para accionar la masa de prueba a lo largo de un eje secundario; medios sensores secundarios que pueden funcionar para detectar la posición de la masa de prueba a lo largo del eje secundario; y medios sensores primarios que pueden funcionar para detectar la posición de la masa de prueba a lo largo del eje primario, comprendiendo el método las etapas de: establecer bucles de realimentación-fuerza $\Sigma\Delta$ tanto para el eje secundario como para el eje primario con el fin de medir tanto un componente de rotación como dos componentes de aceleración.

60 A partir de la exposición de la(s) invención(es) contenida(s) en la presente se pondrán de manifiesto estas y otras ventajas. Las formas de realización y configuraciones antes descritas no son ni completas ni exhaustivas. Tal como se apreciará, son posibles otras formas de realización de la invención usando, de forma individual o en combinación, una o más de las características expuestas anteriormente o que se describen de forma detallada posteriormente.

Breve descripción de los dibujos

La Fig. 1 es un diagrama de bloques que representa un sistema de control de acceso de acuerdo con por lo menos algunas formas de realización de la presente invención;

la Fig. 2 es un diagrama de bloques que representa un dispositivo de RFID de acuerdo con por lo menos algunas formas de realización de la presente invención;

la Fig. 3 es un diagrama de bloques que representa una configuración alternativa de un soporte de un dispositivo de RFID de acuerdo con por lo menos algunas formas de realización de la presente invención;

la Fig. 4 es un diagrama de bloques que representa una vista en sección transversal de un dispositivo de RFID contenido en un soporte que cancela de manera activa comunicaciones de RF a no ser que el soporte detecte un movimiento o secuencia de movimientos predeterminados de acuerdo con por lo menos algunas formas de realización de la presente invención; y

la Fig. 5 es una tabla que representa movimientos ejemplificativos y sus acciones asociadas de acuerdo con por lo menos algunas formas de realización de la presente invención.

Descripción detallada

En referencia inicialmente a la Fig. 1, se representa un sistema de control de acceso 100 ejemplificativo de acuerdo con por lo menos algunas formas de realización de la presente invención. El sistema de control de acceso 100 puede comprender un lector 104 y un dispositivo de RFID 108. El RFID 108 puede ser un dispositivo pasivo que no requiera alimentación suministrada desde una fuente de alimentación interna. La alimentación eléctrica requerida para hacer funcionar una etiqueta pasiva se suministra a esta última por medio de energía electromagnética transmitida desde el lector 104. La energía electromagnética se puede generar en una antena 112 del lector 104 y se puede recibir en una antena 116 del dispositivo de RFID 108. De acuerdo con por lo menos algunas formas de realización de la presente invención, puede que a la antena 116 (o al circuito completo de antena) no se le permita responder a la energía electromagnética generada por el lector 104 si el dispositivo de RFID 108 no se ha movido con un movimiento predefinido de secuencia predefinida de movimientos.

Por consiguiente, un dispositivo de RFID pasivo 108 está operativo cuando recibe ondas electromagnéticas desde el lector 104 y ha sido movido con un movimiento predefinido. No obstante, tal como puede apreciarse, el dispositivo de RFID 108 puede ser alternativamente un dispositivo activo que disponga de alguna forma de fuente de alimentación interna (por ejemplo, una batería o un dispositivo similar de almacenamiento de energía). En esta forma de realización particular, la batería se puede desconectar de la antena o de alguna otra parte del dispositivo de RFID 108 a no ser que el dispositivo de RFID 108 se haya movido con un movimiento predefinido.

En referencia a continuación a la Fig. 2, el dispositivo de RFID 108 puede comprender una serie de elementos funcionales que incluyen un circuito integrado (IC) 204 que está conectado a la antena 116 del dispositivo. El IC 204 materializa las capacidades de procesado y memoria del dispositivo de RFID 108. La antena 116 del dispositivo de RFID 108 está acoplada típicamente al IC 204 y puede ser una bobina convencional denominada "bobina de antena de función dual" que tiene la capacidad de llevar a cabo las funciones tanto de recepción como de transmisión del dispositivo de RFID 108. Alternativamente, dos bobinas de antena independientes de recepción y transmisión pueden sustituir a la "bobina de antena de función dual" única en el dispositivo de RFID 108. El dispositivo de RFID 108 también puede incluir opcionalmente un condensador sintonizador de transpondedor, externo, acoplado al IC y a cada bobina de antena de la antena 116 de la etiqueta. Se describen otros detalles de la circuitería del dispositivo de RFID en la solicitud de patente U.S. n.º 10/874.542 concedida a Lowe, cuyo contenido completo se incorpora por la presente aquí a título de referencia.

La antena 116 del dispositivo de RFID, en cooperación con el condensador sintonizador de transpondedor, si estuviera presente, se puede usar para determinar la frecuencia portadora del dispositivo de RFID 108. De acuerdo con por lo menos algunas formas de realización de la presente invención, el dispositivo de RFID 108 puede estar equipado para comunicarse en una serie de frecuencias portadoras diferentes incluyendo, sin carácter limitativo, 125 kHz, 13,56 MHz, etcétera.

El dispositivo de RFID 108 mostrado y descrito en la presente no es más que un ejemplo de un tipo de transpondedor que tiene utilidad en el sistema de RFID 100. Se entiende que la práctica de la presente invención no se limita a ningún tipo específico de etiqueta, sino que en general es aplicable a la mayoría de tipos convencionales de etiqueta que tienen utilidad en sistemas de RFID. Así, por ejemplo, la etiqueta se puede seleccionar de entre tarjetas de proximidad, etiquetas de proximidad, tarjetas inteligentes, dispositivos de NFC, o similares. Se entiende además que la práctica de la presente invención no se limita a sistemas de RFID que dispongan de solamente una etiqueta y un lector según se ha mostrado y descrito, sino que en general es aplicable a sistemas de RFID que disponen de un número cualquiera de etiquetas/credenciales legibles por máquina y lectores compatibles.

Además, el dispositivo de RFID 108 se puede proporcionar en varios factores de forma diferentes. Por ejemplo, el dispositivo de RFID 108 se puede proporcionar en o dentro de una tarjeta según se ha descrito anteriormente. Adicionalmente, el dispositivo de RFID 108 se puede proporcionar en o dentro de un llavero, un dispositivo electrónico portátil (por ejemplo, ordenador portátil, Asistente Personal Digital (PDA), dispositivo portátil de recuperación de correos electrónicos, teléfono celular, etcétera), cualquier otro dispositivo incluyendo una tarjeta SIM que contenga uno de sus ICs, un ordenador, un teléfono, o cualquier otro dispositivo en general portátil.

En la mayoría de sistemas de RFID convencionales, la posición de lector 104 es fija (es decir, constante) con respecto al entorno circundante, mientras que la posición del dispositivo de RFID 108 es portátil (es decir, variable) dentro del entorno circundante. En tales casos, el usuario del sistema de RFID mueve el dispositivo portátil de RFID 108 de manera que se sitúe en una proximidad relativa con el lector fijo 104 para posibilitar un funcionamiento simultáneo tanto del dispositivo de RFID 108 como del lector 104. No obstante, en algunos sistemas de RFID convencionales, la posición del lector 104 puede ser portátil con respecto al entorno circundante, mientras que la posición del dispositivo de RFID 108 es o bien portátil o bien fija. En el caso de un lector portátil 104 y un dispositivo de RFID fijo 108, el usuario mueve el lector portátil 104 de manera que se sitúe en proximidad relativa con el dispositivo de RFID fijo 108 para posibilitar el funcionamiento simultáneo tanto del dispositivo de RFID 108 como del lector 104. En el caso de un lector portátil 104 y un dispositivo de RFID portátil 108, el usuario puede mover tanto el lector portátil 104 como el dispositivo de RFID portátil 108 para que se sitúen en proximidad relativa mutua con el fin de posibilitar un funcionamiento simultáneo tanto del dispositivo de RFID 108 como del lector 104. Formas de realización de la presente invención no se limitan a ninguna de las configuraciones antes mencionadas del sistema de RFID.

Tal como puede observarse en la Fig. 2, el dispositivo de RFID 108 puede incluir además un mecanismo de detección direccional 208 que está acoplado a un conmutador 212. El conmutador 212 puede controlar las capacidades operativas globales del dispositivo de RFID 108. Más específicamente, el conmutador 212 se puede habilitar para desconectar el IC 204 del dispositivo de RFID 108 con respecto a la antena 116. Alternativamente, el conmutador 212 se puede habilitar para desconectar el IC 204 con respecto a una memoria externa que contenga datos sensibles. Todavía en otra forma de realización alternativa, el conmutador 212 se puede habilitar para deshabilitar en su totalidad la antena 116. Todavía en otra forma de realización alternativa, el conmutador 212 se puede habilitar para deshabilitar o, si no, controlar directamente el funcionamiento del IC 204 (es decir, el conmutador 212 puede ser solidario con el IC 204). En otras palabras, el conmutador 212 puede comprender un conmutador lógico que sea simplemente un conjunto de reglas implementado por el IC 204 cuando se reciba una señal particular en el IC 204 desde el mecanismo de detección direccional 208.

Tal como puede observarse en la Fig. 2, el IC 204, el mecanismo de detección 208, y/o el conmutador 212 se pueden proporcionar en un único trozo de silicio 216 residente en el dispositivo de RFID 108. Alternativamente, solamente el IC 204 y el mecanismo de detección 208 se pueden proporcionar en el trozo único de silicio 216. Todavía adicionalmente en la opción alternativa, cada componente se puede proporcionar en trozos independientes de silicio.

Como estado por defecto, puede que el conmutador 212 no permita que el dispositivo de RFID 108 transmita ningún dato (incluyendo datos sensibles) desde la antena 116. Cuando se detecta un movimiento o secuencia de movimientos predeterminados "de activación" en el mecanismo de detección 208, el conmutador 212 se puede cambiar desde su estado por defecto y a continuación se puede permitir que el dispositivo de RFID 108 transmita datos sensibles.

Una vez que se ha habilitado el dispositivo de RFID 108 para transmitir datos, se puede habilitar al IC 204 para recuperar datos sensibles desde su ubicación de almacenamiento, generar un mensaje que contenga dichos datos, y a continuación transmitir dicho mensaje al lector 104 por medio de su antena 116.

De acuerdo con por lo menos algunas formas de realización y según se ha indicado anteriormente, la presente invención no se limita a su uso en tecnologías de RFID o al control de dichas tecnologías. Por el contrario, formas de realización de la presente invención se pueden aplicar a tarjetas SIM que contengan uno o más ICs u otros ICs que residan en un dispositivo de comunicación móvil. Se puede utilizar un mecanismo de detección direccional 208 para controlar el funcionamiento de la tarjeta SIM o del IC del dispositivo de comunicación móvil. Como ejemplo, el mecanismo de detección direccional 208 se puede utilizar para limitar el funcionamiento de la tarjeta SIM o del IC. Como otro ejemplo, el mecanismo de detección direccional 208 se puede usar para proporcionar una entrada de control a la tarjeta SIM o al IC, de tal manera que operaciones de la tarjeta SIM o del IC se basen en movimientos del dispositivo de comunicación móvil detectados por el mecanismo de detección direccional 208. Esto puede permitir que un usuario del dispositivo de comunicación móvil controle el funcionamiento del dispositivo de comunicación móvil simplemente agitando este último o moviéndolo de una manera predeterminada o de acuerdo con una secuencia predeterminada de movimientos. En calidad de diferentes entradas de control para la tarjeta SIM o el IC se puede usar un conjunto de movimientos o secuencia de movimientos diferentes. Como ejemplo, una rotación del dispositivo móvil a la izquierda se puede corresponder con una entrada que provoca que la tarjeta SIM o el IC ejecute una acción, mientras que una rotación del dispositivo móvil a la derecha se puede corresponder con una entrada diferente que provoque que la tarjeta SIM o el IC ejecute otra acción diferente.

Como ejemplo alternativo, un usuario puede dar origen a una llamada por medio de la antena 116 hacia un destino remoto (por ejemplo, por medio de tecnologías de comunicación celular) y un número de teléfono predeterminado simplemente agitando o dando golpecitos al dispositivo móvil. Esto permite que el usuario controle las operaciones del dispositivo móvil y ciertas aplicaciones que residen en el mismo, simplemente moviendo o agitando el dispositivo móvil. Esto puede permitir la creación de un dispositivo de comunicación móvil que no requiere necesariamente un conjunto telefónico de mano o un teclado. En otras palabras, la tarjeta SIM del dispositivo móvil puede ser independiente del conjunto telefónico de mano y se puede controlar simplemente mediante el agitado o el golpeteo del dispositivo móvil y la posterior detección de movimiento por parte del mecanismo de detección direccional 208.

Las Figs. 3 y 4 representan un mecanismo alternativo que se puede usar para proteger datos sensibles almacenados en un dispositivo de RFID 108. Más específicamente, en lugar de "habilitar" el dispositivo de RFID 108 para transmitir datos sensibles únicamente cuando un mecanismo de detección 208 detecta un movimiento o secuencia predeterminados de movimientos, puede haber la posibilidad de utilizar un dispositivo portador de tarjetas 304 que genere un campo de cancelación activo 308 el cual está destinado a distorsionar cualquier transmisión de datos del dispositivo de RFID 108. Más específicamente, el soporte 304 puede comprender una antena y un IC independientes que están adaptados para activarse cuando se llevan dentro de un campo de RF. Si en el soporte se encuentra también un dispositivo de RFID 108 cuando se aplica un campo de RF al mismo, tanto las antenas del soporte como una antena incluida en el dispositivo de RFID 108 intentarán transmitir mensajes. La señal transmitida por el soporte 304 se usa para crear ruido haciendo así que resulte difícil o imposible recuperar los datos transmitidos por el dispositivo de RFID 108. Si un usuario desea hacer que su dispositivo de RFID sea leído por un lector, tradicionalmente se requiere que el usuario extraiga el dispositivo de RFID 108 del soporte 304 de manera que no se genere el campo de cancelación 308.

Formas de realización de la presente invención proponen la incorporación de un mecanismo de detección 208 en el soporte 304, mejor que en el dispositivo de RFID 108, de manera que puedan usarse técnicas de protección de la privacidad aquí descritas para proteger datos en dispositivos de RFID 108 heredados, más antiguos, que no poseen un mecanismo de detección direccional 208. De acuerdo con por lo menos algunas formas de realización de la presente invención, un usuario puede permitir que se lean datos del dispositivo de RFID 108 moviendo el soporte 304 con un movimiento o secuencia predeterminados de movimientos para desactivar temporalmente el campo de cancelación 308. Esto permite que el dispositivo de RFID 108 sea la única antena que responde al lector. Todo esto se puede lograr sin necesidad de que ningún usuario extraiga el dispositivo de RFID 108 del soporte 304.

Tal como puede observarse en la Fig. 4, el soporte 304 puede tener una geometría preferida para afianzar físicamente el dispositivo de RFID 108. El mecanismo de detección direccional 208 se puede proporcionar en una placa de circuito impreso o similar que resida en la cara posterior del soporte de tarjeta 304. El mecanismo de detección direccional 208 puede funcionar de una manera normal, aunque en lugar de habilitar operaciones del soporte 304 cuando se detecte un movimiento o secuencia predeterminados de movimientos, el mecanismo de detección direccional 208 puede deshabilitar operaciones del soporte 304 durante una cantidad de tiempo predeterminada.

En referencia a continuación a la Fig. 5, se describirá de acuerdo con por lo menos algunas formas de realización de la presente invención una tabla de movimientos 500 ejemplificativa usada para traducir movimientos en acciones. Tal como puede observarse, se pueden usar movimientos de rotación por uno, dos, o tres ejes para proteger datos en un dispositivo de RFID 108 ó por lo menos controlar el funcionamiento del dispositivo RFID 108. Adicionalmente, como entrada de movimiento también pueden considerarse movimientos deslizantes. Cuando se detecta un movimiento o secuencia de movimientos predeterminados, se lleva a cabo una acción en concordancia con las acciones enumeradas en la tabla 500. Como ejemplo, el movimiento o secuencia de movimientos puede dar como resultado una acción que permita que el dispositivo de RFID 108 transmita datos sensibles a un lector. Como ejemplo alternativo, el movimiento o secuencia de movimientos puede dar como resultado la generación y la transmisión de un mensaje predeterminado. Todavía como otro ejemplo, el movimiento o secuencia de movimientos puede provocar que el IC 204 traduzca los movimientos en datos binarios los cuales pueden ser transmitidos en calidad de contraseña al lector 104 de forma individual o adicionalmente con respecto a otros datos sensibles almacenados en el dispositivo de RFID 108. A continuación, el lector 104 puede analizar la contraseña para determinar si se permite el acceso al usuario. La contraseña se puede usar como símil o sustitución de una entrada de usuario que, en caso contrario, necesitaría ser proporcionada en un teclado en el lector 104. Por consiguiente, un lector 104 sin ningún teclado puede comprobar qué es lo que está llevando el usuario así como qué es lo que sabe el usuario, dando como resultado de este modo un servicio sustancialmente más seguro.

De acuerdo con por lo menos algunas formas de realización de la presente invención, se proporciona un proceso de inscripción por el cual se permite que un usuario defina su movimiento o secuencia personal de movimientos que se usarán para proteger los datos en el dispositivo de RFID 108. En una forma de realización, se puede permitir que el usuario se sienta delante de un lector conectado a un ordenador que proporciona al usuario una Interfaz Gráfica de Usuario. El lector puede invitar al usuario a introducir su contraseña basada en el movimiento y a continuación esperará la detección de un movimiento o serie de movimientos. Una vez que el usuario ha llevado a cabo el(los)

5 movimiento(s) deseado(s), el usuario puede indicar que ya ha acabado y el lector/ordenador repetirá el movimiento o secuencia de movimientos detectados y preguntará al usuario si esa es su contraseña deseada. Si el usuario selecciona sí, entonces las entradas de la tabla 500 se pueden actualizar de forma correspondiente. Además, los datos de la contraseña se pueden proporcionar de vuelta al dispositivo de RFID 108 ó se envía por lo menos una afirmación al dispositivo de RFID 108 indicando que el último movimiento o secuencia de movimientos se corresponde con una contraseña introducida y reconocida por el lector.

10 De acuerdo con por lo menos algunas formas de realización alternativas de la presente invención, la contraseña basada en movimiento también se puede usar para proteger dispositivos que no sean de RF. Como ejemplo, una tarjeta RSA se puede proteger con un mecanismo de detección direccional 208 que lleva a cabo operaciones según se ha descrito en la presente. A no ser que en la tarjeta RSA se detecte un movimiento o secuencia de movimientos predeterminados, se puede prohibir entonces a la tarjeta RSA que genere un código para el usuario.

15 En varias formas de realización, la presente invención incluye componentes, métodos, procesos, sistemas y/o aparatos sustancialmente según se ha representado y descrito en la presente, incluyendo varias formas de realización, subcombinaciones y subconjuntos de los mismos. Aquellos expertos en la materia entenderán cómo materializar y hacer uso de la presente invención después de asimilar la presente exposición. En varias formas de realización, la presente invención incluye la provisión de dispositivos y procesos en ausencia de elementos no representados y/o descritos en la presente o en varias realizaciones de los mismos, incluyendo en ausencia de
20 elementos tales como los que se pueden haber usado en dispositivos o procesos previos, por ejemplo, para mejorar el rendimiento, proporcionar comodidad y/o reducir el coste de implementación.

25 La anterior exposición de la invención se presentado con fines ilustrativos y descriptivos. Lo anterior no pretende limitar la invención a la forma o formas dadas a conocer en la presente. En la anterior Descripción Detallada por ejemplo, varias características de la invención se agrupan conjuntamente en una o más formas de realización con la finalidad de racionalizar la exposición. Este método de exposición no debe interpretarse de manera que refleje una intención de que la invención reivindicada requiera más características de las que se mencionan expresamente en cada reivindicación. Por el contrario, tal como reflejan las siguientes reivindicaciones, los aspectos de la invención residen en menos características que todas las pertenecientes a una única forma de realización dada a conocer
30 anteriormente.

35 Por otra parte, aunque la descripción de la invención ha incluido la descripción de una o más formas de realización y ciertas variaciones y modificaciones, dentro del alcance de la invención se sitúan otras variaciones y modificaciones, por ejemplo, como las que pueden darse con las habilidades y los conocimientos de los profesionales en la materia, después de asimilar la presente exposición.

REIVINDICACIONES

1. Método de control del funcionamiento de un Circuito Integrado (204), que comprende:

5 recibir una primera entrada de movimiento en un mecanismo de detección direccional (208), siendo el mecanismo de detección direccional solidario con el Circuito Integrado;

traducir la primera entrada de movimiento recibida en una primera señal eléctrica; y

10 proporcionar la primera señal eléctrica al Circuito Integrado para controlar el funcionamiento del Circuito Integrado;

comprendiendo además el método:

15 recibir una segunda entrada de movimiento en el mecanismo de detección direccional, siendo la segunda entrada de movimiento diferente con respecto a la primera entrada de movimiento;

traducir la segunda entrada de movimiento recibida en una segunda señal eléctrica que es diferente de la primera señal eléctrica;

20 proporcionar la segunda señal eléctrica al Circuito Integrado;

en el que el primer y segundo movimientos se corresponden con una secuencia predeterminada de movimientos y en el que la primera y segunda señales eléctricas se analizan juntas y antes de llevar a cabo una operación de control del Circuito Integrado.

2. Método según la reivindicación 1, en el que el Circuito Integrado controla operaciones de un dispositivo de RFID.

30 3. Método según la reivindicación 2, en el que el dispositivo de RFID se incorpora en un dispositivo de comunicación móvil.

4. Método según la reivindicación 2, en el que el funcionamiento del Circuito Integrado depende de la primera señal eléctrica recibida del mecanismo de detección direccional.

35 5. Método según la reivindicación 1, en el que se impide al Circuito Integrado transmitir una señal eléctrica a una fuente externa en ausencia de por lo menos una de entre la primera y segunda señales eléctricas o en ausencia de la recepción de la primera señal eléctrica antes de la segunda señal eléctrica.

40 6. Método según la reivindicación 1, en el que el Circuito Integrado y el mecanismo de detección direccional residen en un soporte del dispositivo de RFID, y el Circuito Integrado se usa para generar un campo de cancelación transmitido por una antena del soporte del dispositivo de RFID con el fin de confundir una señal eléctrica transmitida por un dispositivo de RFID contenido en el soporte de dispositivo de RFID, y en el que se permite que el Circuito Integrado transmita una señal eléctrica a una fuente externa a no ser que se reciba por lo menos una de entre la primera y segunda señales eléctricas.

45 7. Dispositivo de comunicación (108) para llevar a cabo el método según una de las reivindicaciones anteriores, que comprende:

50 un Circuito Integrado (204); y

un mecanismo de detección direccional (208) configurado para detectar por lo menos un primer movimiento y un segundo movimiento del dispositivo de comunicación, siendo dicho primer y segundo movimientos diferentes, y estando configurado para traducir el primer y segundo movimientos detectados en señales eléctricas diferentes que posteriormente se transmiten a un conmutador (212) que controla el funcionamiento del Circuito Integrado, correspondiéndose el primer y segundo movimientos con una secuencia predeterminada de movimientos y siendo la primera y segunda señales eléctricas analizadas juntas y antes de llevar a cabo una operación de control del Circuito Integrado.

60 8. Dispositivo de comunicación según la reivindicación 7, en el que el mecanismo de detección direccional es solidario con el Circuito Integrado.

9. Dispositivo de comunicación según la reivindicación 8, en el que el mecanismo de detección direccional y el Circuito Integrado se proporcionan en un sistema micro-electromecánico común.

10. Dispositivo de comunicación según la reivindicación 7, en el que el conmutador comprende un conmutador lógico o en el que el conmutador comprende uno o más de entre un conmutador eléctrico, un conmutador mecánico, y un conmutador electromecánico.
- 5 11. Dispositivo de comunicación según la reivindicación 7, que comprende además:
una antena (116), en la que el mecanismo de detección direccional controla la capacidad del Circuito Integrado para transmitir mensajes por medio de la antena.
- 10 12. Dispositivo de comunicación según la reivindicación 11, en el que el Circuito Integrado no transmite un mensaje por medio de la antena, a menos que el mecanismo de detección direccional detecte la secuencia predeterminada de movimientos.
- 15 13. Dispositivo de comunicación según la reivindicación 7, en el que el mecanismo de detección direccional comprende un acelerómetro.
14. Dispositivo de comunicación según la reivindicación 7, en el que el mecanismo de detección direccional comprende dos acelerómetros para detectar movimiento a través de dos ejes diferentes no paralelos.

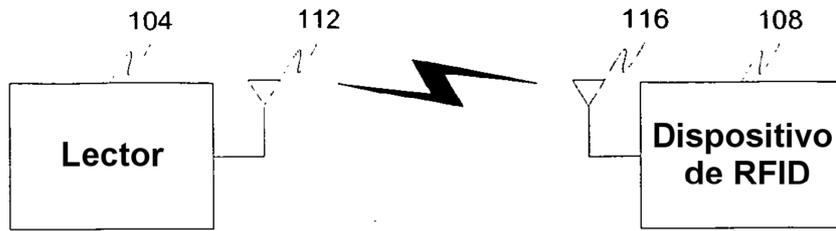


Fig. 1

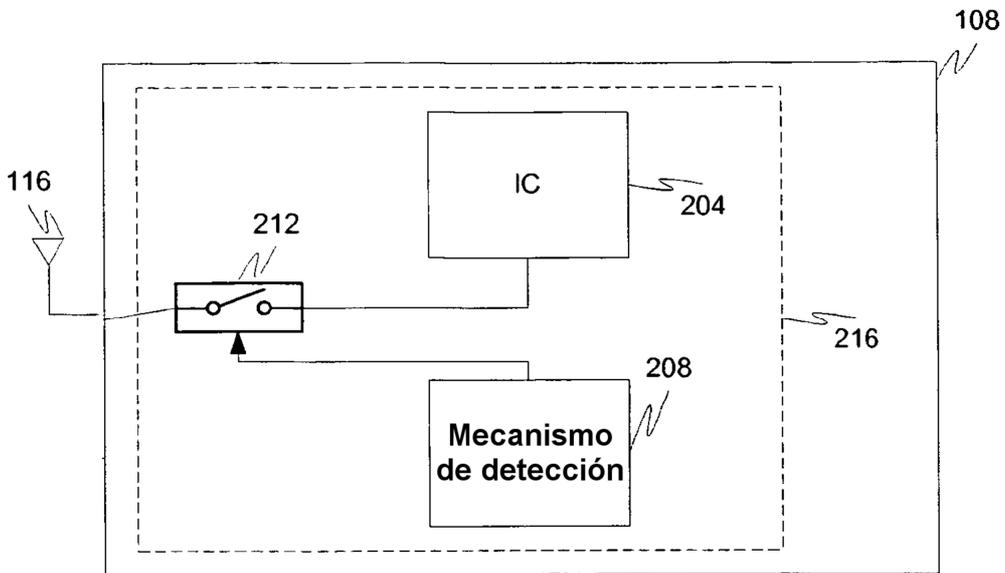


Fig. 2

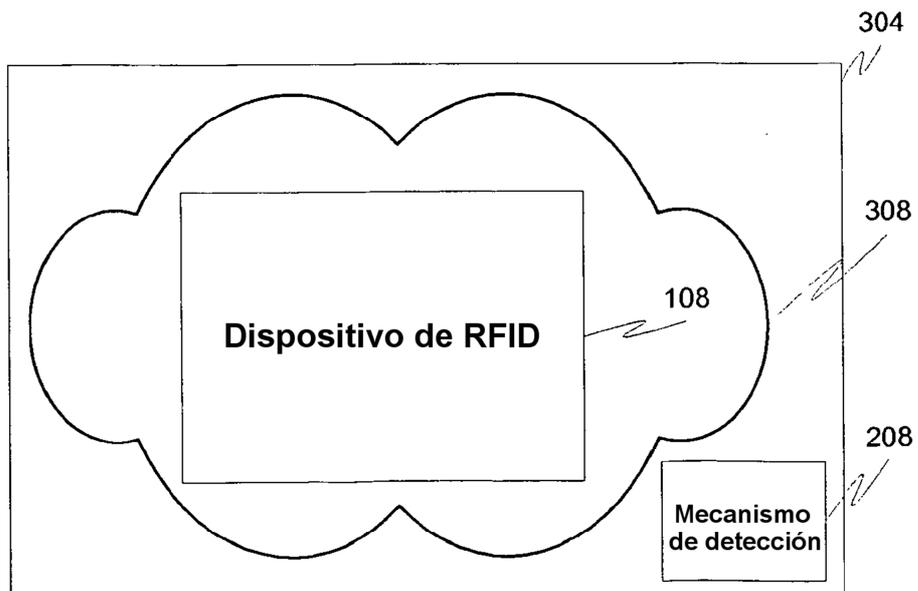


Fig. 3

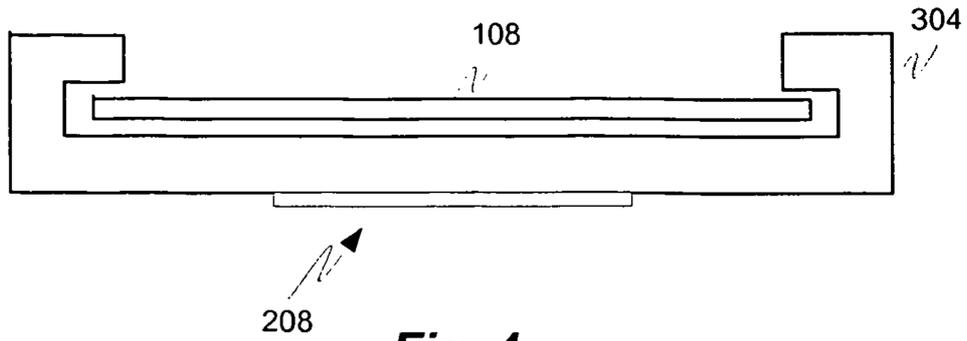


Fig. 4



Movimiento 1	Movimiento 2	Movimiento 3	Acción
↓	←	↓	Permitir Lectura de Datos
↑	<div style="text-align: center;">90 ↻</div>		Permitir Lectura de Datos
<div style="text-align: center;">90 ↻</div>			Permitir Lectura de Datos
<div style="text-align: center;">90 ↻ X-eje</div>	<div style="text-align: center;">180 ↻ Y-eje</div>	<div style="text-align: center;">180 ↻ Z-eje</div>	Transmitir Mensaje Preestablecido n.º 1 de N
↑	→	↑	Proporcionar Secuencia Como Contraseña

Fig. 5