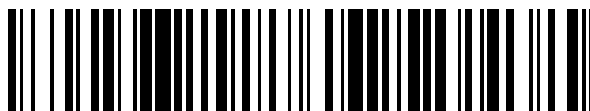


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 407 644**

51 Int. Cl.:

G06F 21/00

(2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **20.08.2009** **E 09778011 (8)**

97 Fecha y número de publicación de la concesión europea: **06.03.2013** **EP 2359300**

54 Título: **Procedimiento para almacenamiento seguro de datos en una memoria de un soporte de datos portátil**

30 Prioridad:

17.11.2008 DE 102008057681

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

13.06.2013

73 Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
Prinzregentenstrasse 159
81677 München , DE

72 Inventor/es:

RANKL, WOLFGANG

74 Agente/Representante:

ARPE FERNÁNDEZ, Manuel

ES 2 407 644 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

Procedimiento para almacenamiento seguro de datos en una memoria de un soporte de datos portátil.

La invención se refiere a un procedimiento para el almacenamiento seguro de datos en una memoria de niveles múltiples de un soporte de datos portátil, incluyendo la memoria de niveles múltiples una o más celdas de memoria de niveles múltiples que pueden adoptar respectivamente, al menos, tres niveles que representan un contenido de datos diferente. Cada nivel de una celda de memoria se puede predefinir como válido o no válido.

En el marco de la presente descripción, por un soporte de datos portátil se entiende por ejemplo una tarjeta chip, una tarjeta SIM (Subscriber Identity Module - módulo de identificación de abonado), un llavero provisto de un microcontrolador (Fob), un testigo o similares. Un microcontrolador de un soporte de datos portátil incluye una memoria no volátil, por ejemplo en forma de celdas de memoria EEPROM o *flash*. El funcionamiento de este tipo de memorias se basa en la medición de la presencia o ausencia de una carga eléctrica en una celda de memoria. Más concretamente se determina la carga contenida en una, así llamada, puerta flotante (*floating gate*) de la celda de memoria. En el caso de las celdas de memoria de niveles múltiples no solo se determina la presencia de una carga, sino también la magnitud de la misma.

Ya se conocen procedimientos que permiten modificar o borrar el contenido de celdas de memoria EEPROM/*flash*. Por ejemplo, la puerta flotante de una celda de memoria se puede borrar mediante radiación de alta energía. La modificación de los contenidos de datos de una celda de memoria se puede llevar a cabo tanto en toda la memoria como selectivamente en determinadas celdas de memoria. Por ello existe la posibilidad de que un atacante pueda manipular grandes áreas de la memoria no volátil.

Para asegurar el contenido de datos de una memoria no volátil contra ataques de manipulación se emplean sumas de control para los datos y/o programas a proteger. Como sumas de control se utilizan, por ejemplo valores de CRC (Cyclic Redundancy Check - prueba de redundancia cíclica) o valores de troceo (*hash*) (comprobación aleatoria). Dado que los contenidos de datos son variables, las sumas de control correspondientes han de ser calculadas y almacenadas de nuevo a intervalos regulares. Sin embargo, este procedimiento implica varias desventajas. Por un lado, el cálculo y almacenamiento de las sumas de control requiere tiempo. Por otro lado, no basta con determinar una única suma de control para toda la memoria, ya que ésta no es necesaria en muchos accesos de escritura. Por consiguiente, la memoria no volátil se protege con numerosas sumas de control para diferentes áreas de memoria que presentan respectivamente una cantidad de celdas de memoria. Además, también existe el peligro de que, en el marco de un ataque, además de los propios datos útiles también se manipule la suma de control correspondiente, con lo que un sistema operativo que gestiona la memoria ya no puede reconocer los datos modificados por el ataque.

Por ello, en el documento US 6.331.946 B1 se propone utilizar una memoria de niveles múltiples para el almacenamiento seguro de información sensible, en la que los dos niveles exteriores (llamados *levels*) se declaran como no válidos con respecto a un contenido de datos almacenado. Para el almacenamiento de información se utilizan únicamente los niveles situados entre los dos niveles exteriores. Este procedimiento se basa en la consideración de que en caso de un intento de manipulación del contenido de datos de una celda de memoria se produce uno de los estados no válidos de la celda de memoria de niveles múltiples, lo que se puede detectar y reconocer fácilmente como manipulación.

El objetivo de la presente invención consiste en proponer un procedimiento para el almacenamiento de datos en una memoria de niveles múltiples de un soporte de datos portátil, que posibilite una seguridad aún mayor contra manipulaciones.

Este objetivo se resuelve mediante un procedimiento con las características indicadas en la reivindicación 1. En las reivindicaciones subordinadas se indican configuraciones ventajosas.

El procedimiento según la invención parte del procedimiento descrito en el estado actual de la técnica para el almacenamiento seguro de datos en una memoria de niveles múltiples de un soporte de datos portátil. Correspondientemente, la memoria de niveles múltiples incluye una o más celdas de memoria de niveles múltiples que pueden adoptar respectivamente, al menos, tres niveles (llamados *levels*) que representan un contenido de datos diferente, predefiniéndose cada uno de los niveles de una celda de memoria como válido o no válido. De acuerdo con la invención está previsto predefinir los niveles de cada celda de memoria como válidos o no válidos en función de un nivel de seguridad requerido.

Por consiguiente, la invención se basa en la idea (conocida en el estado actual de la técnica) de no utilizar toda la capacidad de memoria posible de una memoria no volátil en tecnología de niveles múltiples. Más bien, los niveles de cada celda de memoria se predefinen selectivamente como válidos o no válidos en función de un nivel de seguridad requerido, es decir, de un nivel de seguridad predefinido correspondientemente a la protección necesaria para el contenido de datos respectivo. De este modo, la seguridad de la memoria no volátil puede presentar una configuración escalable.

En particular se varía la relación entre el número de niveles válidos y de niveles no válidos de cada celda de memoria en función del nivel de seguridad requerido. En este contexto se puede prever que, si se requiere un nivel de seguridad máximo, la celda de memoria solo presente un nivel válido para el almacenamiento de un contenido de datos, mientras que todos los demás niveles que pueden ser adoptados por la celda de memoria son no válidos. En otra configuración, si se requiere un nivel de seguridad mínimo, todos los niveles de la celda de memoria son válidos para el almacenamiento de contenidos de datos, de modo que se puede aprovechar toda la capacidad de memoria posible de la celda de memoria.

Por consiguiente, el procedimiento según la invención permite variar la relación entre niveles o contenidos de datos de las celdas de memoria de la memoria del soporte de datos portátil autorizados o prohibidos, pudiendo variarse dicha relación en función de la seguridad necesaria. En este contexto, la variación puede tener lugar en particular dentro de la memoria de tal modo que, por ejemplo, se protejan especialmente claves secretas en celdas de memoria definidas, mientras que en otras celdas de memoria se prevén datos que presentan muy poca o ninguna protección y que pueden ser leídos libremente desde fuera del soporte de datos portátil.

De acuerdo con otra forma de realización, la predefinición de niveles válidos y no válidos para la celda o las celdas de la memoria de niveles múltiples tiene lugar de forma dinámica o en el marco de su fabricación. Esto tiene la ventaja de que, incluso cuando un ataque manipula celdas de memoria de tal modo que éstas contienen una carga determinada y en consecuencia un contenido de datos determinado, no se sabe qué niveles, y por consiguiente que contenidos de datos, están autorizados o prohibidos en las celdas de memoria correspondientes.

En una configuración concreta, la predefinición dinámica de niveles válidos y no válidos para la celda o las celdas de memoria se lleva a cabo recurriendo a una tabla, una función o un generador de números pseudoaleatorios cuya salida es determinista, es decir, reproducible a voluntad. En particular, para la lectura de datos de una celda de memoria se comprueba cuáles son los niveles autorizados a través de la tabla, función o generador de números pseudoaleatorios para la celda de memoria en cuestión. Solo después de este proceso es posible leer datos de una dirección determinada. De este modo se logra un aumento de la seguridad en el almacenamiento de datos en una memoria de niveles múltiples de un soporte de datos portátil.

De acuerdo con otra configuración, durante la lectura de una celda de la memoria de niveles múltiples se comprueba si ésta representa un contenido de datos autorizado o no autorizado conforme a los niveles válidos o no válidos predefinidos. Si el contenido de datos está autorizado, éste se facilita para su posterior procesamiento, y si el contenido de datos no está autorizado, se deduce que se ha producido una manipulación de la celda de memoria. De este modo se puede evitar la utilización involuntaria de contenidos de datos manipulados.

En un perfeccionamiento ventajoso del procedimiento según la invención, la predefinición de los niveles válidos se aprovecha para llevar a cabo de forma sencilla un borrado seguro próximo a *hardware* de celdas de memoria declaradas lógicamente como borradas. Para ello, en una operación de borrado, los niveles definidos como válidos se cambian por otros originalmente no válidos. De este modo, el contenido de datos de la celda de memoria no puede ser recuperado, incluso si en un intento de manipulación se consigue evitar la declaración de borrado lógico asignada.

En otro perfeccionamiento ventajoso del procedimiento según la invención, la predefinición selectiva de los niveles como válidos/no válidos se aprovecha para compensar cambios físicos de las celdas de memoria provocados por envejecimiento o por influencias ambientales. Las celdas de memoria envejecen por diferentes condiciones ambientales tales como humedad del aire, calor o radiación. En este caso, algunos niveles ya no se pueden ajustar de forma fiable o cambian por sí solos. Los cambios son permanentes y normalmente siguen un principio fijo determinista. Por ejemplo, las cargas que predefinen los niveles individuales de una celda de memoria disminuyen con el paso del tiempo, de modo que el contenido de datos representado por la carga corresponde aparentemente a otro nivel. Si se detecta un cambio de función de este tipo de una celda de memoria, mediante una copia del principio de cambio subyacente en la predefinición de los niveles como válidos/no válidos se puede restablecer o mantener fácilmente el estado original de la celda de memoria. La detección de un cambio subyacente puede tener lugar mediante una tecnología de sensores independiente, pero también mediante evaluación de las propias celdas de memoria, por ejemplo comprobando si varias celdas de memoria adyacentes presentan cambios similares de sus contenidos de datos. Mediante la compensación de estos cambios es posible hacer funcionar durante más tiempo celdas de memoria "moribundas". Al mismo tiempo, la ejecución de una compensación indica que la celda de memoria ya no está totalmente intacta y que debería ser sustituida.

La invención se explica más detalladamente a continuación por medio de un ejemplo de realización con referencia a los dibujos. En los dibujos:

- la figura 1 muestra una tabla que compara los estados posibles de celdas de memoria convencionales y de niveles múltiples, y

- la figura 2 muestra una tabla que ilustra el procedimiento en que se basa la invención.

Para realizar el procedimiento según la invención se utiliza una memoria de niveles múltiples de un soporte de datos portátil, en particular una tarjeta chip. Como es sabido, la memoria de niveles múltiples incluye una o más celdas de

memoria de niveles múltiples que pueden adoptar respectivamente, al menos, tres niveles, que representan un contenido de datos diferente. Los niveles de una celda de memoria de niveles múltiples también se designan como *levels*. El procedimiento para proporcionar una mejor protección frente a la manipulación se basa en no utilizar toda la capacidad de memoria posible de la memoria de niveles múltiples no volátil. En lugar de ello, para cada celda de memoria se predefinen selectivamente niveles válidos o no válidos en función de un nivel de seguridad requerido. Dicho de otro modo, esto significa que para cada celda de memoria se predefinen selectivamente contenidos de datos autorizados o no autorizados. Durante la lectura de una celda de la memoria de niveles múltiples se comprueba si ésta representa un contenido de datos autorizado o no autorizado conforme a los niveles válidos o no válidos predefinidos. Si el contenido de datos está autorizado, éste se transmite, por ejemplo, a una rutina que lo llama para su posterior procesamiento. Sin embargo, si se trata de un contenido de datos no autorizado, se parte de la base de que el contenido de la celda de memoria ha sido manipulado.

La protección en comparación con una tecnología de memoria convencional cuyas celdas de memoria solo pueden adoptar dos niveles (estados) se basa en que para un atacante es infinitamente más difícil llegar durante una manipulación a estados intermedios de una celda de memoria de niveles múltiples que al estado de una celda de memoria convencional vacía o llena. La figura 1 muestra una tabla en la que están representados ejemplos de contenidos y una respectiva carga eléctrica correspondiente de una celda de memoria convencional y una celda de memoria de niveles múltiples con cuatro niveles posibles. Con ADR se designan ejemplos de direcciones 0x8000, 0x8001, 0x8002 y 0x8003 de una celda de memoria. INH1 representa por ejemplo el contenido de datos de celdas convencionales en representación lógica. LAD1 representa el contenido de datos de las celdas de memoria convencionales en lo que respecta a su carga eléctrica. Un círculo vacío representa por ejemplo una puerta flotante no cargada y un círculo lleno representa una puerta flotante cargada. INH2 representa por ejemplo el contenido de datos de celdas de memoria múltiples de niveles múltiples en representación lógica. LAD2 representa el contenido de datos de las celdas de memoria múltiples de niveles múltiples en lo que respecta a la carga eléctrica correspondiente. Cuanto mayor es la relación de la superficie negra con respecto a la superficie blanca, mayor es por ejemplo la carga de la puerta flotante. En el ejemplo de realización mostrado, una celda de memoria multicapa puede adoptar en total cuatro cargas diferentes.

Las celdas de memoria SZ con las direcciones 0x8000 y 0x8002 en tecnología de memoria convencional presentan un "0" lógico. En cambio, las celdas de memoria SZ con las direcciones 0x8001 y 0x8003 presentan un "1" lógico. El "0" lógico se representa por ejemplo mediante una puerta flotante no cargada. Correspondientemente, un "1" lógico se representa mediante una puerta flotante cargada. No obstante, esto también puede ser a la inversa dependiendo de la lógica utilizada en la memoria.

A diferencia de ello, las celdas de memoria SZ de una memoria de niveles múltiples puede adoptar no solo dos, sino en total cuatro estados diferentes ("0", "1", "2" y "3"), siendo representados estos estados diferentes por cargas de diferente magnitud en la puerta flotante. Por ejemplo, un "0" lógico de la celda de memoria SZ con la dirección 0x8000 se representa mediante una puerta flotante no cargada. Una puerta flotante completamente cargada representa un "3" lógico, lo que está representado por ejemplo en la celda de memoria SZ con la dirección 0x8003. Las celdas de memoria SZ con las direcciones 0x8001 y 0x8002 presentan niveles situados entre estos dos estados exteriores. No obstante, esto también puede ser a la inversa dependiendo de la lógica utilizada en la memoria.

Para aumentar la seguridad de los datos contenidos en una memoria de niveles múltiples, por ejemplo únicamente se definen como autorizados los contenidos de datos "1" y "2" o sus niveles correspondientes, lo que se identifica con "E" en la tabla de la figura 2. En cambio, los contenidos de datos "0" y "3" representan contenidos de datos o niveles no autorizados. Esto significa que, si durante la lectura de una celda de memoria se determinan los contenidos de datos "0" y "3", se parte de la base de que se ha producido una manipulación con éxito de la celda de memoria SZ correspondiente (en la tabla 1 las celdas de memoria con las direcciones 0x8000 y 0x8003). La figura 2 también muestra que un nivel autorizado, que representa un contenido de datos autorizado, puede ser leído, mientras que un nivel no autorizado no es transferido para su procesamiento posterior. Esto se encuentra representado esquemáticamente en la última línea de la tabla, en la que una acción AKT a ejecutar respectivamente, está identificada con M o con R. M representa una celda de memoria manipulada, cuyo contenido de datos no es procesado posteriormente, sino que es tratado especialmente por un sistema operativo del soporte de datos portátil. R representa una celda de memoria no manipulada, cuyo contenido puede ser leído y procesado posteriormente.

La limitación de la utilización de determinados niveles o contenidos de datos conduce a una reducción de la memoria disponible. En cambio, también implica un considerable aumento de la seguridad. Además, la invención permite en particular configurar la seguridad de la memoria no volátil de forma escalable. Si se requiere un nivel de seguridad máximo, se puede predefinir por ejemplo que la celda de memoria solo presente un único nivel válido. En cambio, si se requiere un nivel de seguridad mínimo, se puede predefinir que sean válidos todos los niveles de la celda de memoria para los contenidos de datos correspondientes. Esta variación se puede llevar a cabo dentro de la memoria de niveles múltiples completa, lo que permite proteger especialmente claves secretas u otra información sensible. Por el contrario, los datos que se pueden leer libremente desde fuera de la memoria de niveles múltiples del soporte de datos portátil se pueden almacenar de tal modo que presenten muy poca o ninguna protección.

En una variante de configuración alternativa a una predefinición fija de niveles válidos y no válidos de una celda de memoria está previsto realizar dicha predefinición de forma dinámica para determinadas áreas, es decir celdas, de la

memoria no volátil. Aunque un atacante logre manipular celdas de memoria para que éstas contengan una carga determinada y en consecuencia un contenido de datos determinado, el atacante no sabe qué contenidos de datos están autorizados o prohibidos en las celdas de memoria correspondientes.

En otra variante está previsto predefinir individualmente niveles o contenidos de datos de celdas de memoria válidos y no válidos. Esta predefinición se puede llevar a cabo mediante una tabla, una función o un generador de números pseudoaleatorios cuya salida es determinista y, por consiguiente, reproducible a voluntad. Para la lectura de datos de una memoria protegida de este modo se han de determinar, por ejemplo a través del generador de números pseudoaleatorios, los contenidos de datos autorizados para una celda de memoria correspondiente, es decir, la dirección de memoria respectiva. Solo después es posible leer el contenido de datos de la celda de memoria perteneciente a la dirección de memoria.

La predefinición dinámica e individual para las celdas de memoria de niveles válidos y no válidos también se puede llevar a cabo adicionalmente de forma individual para cada chip. Por ejemplo, antes de introducir contenidos de datos durante la fabricación del soporte de datos portátil se puede parametrizar aleatoriamente el generador de números pseudoaleatorios individualmente para cada chip. Después se pueden introducir datos en la memoria no volátil utilizando los valores producidos por el generador de números pseudoaleatorios.

Un algoritmo posible para el proceso de lectura de una celda de memoria puede tener el siguiente aspecto:

1. En primer lugar se lee el contenido de datos DI de una celda de memoria con la dirección X.
2. Después se determinan los contenidos de datos autorizados eDI de la celda de memoria con la dirección X.
3. A continuación se comprueba si el contenido de datos DI está en el área del contenido de datos autorizado eDI. En caso afirmativo, el contenido de datos DI se considera como no manipulados y se transfiere a la rutina que lo llama. Si el contenido de datos no se encuentra en el área del contenido de datos autorizado eDI, se parte de la base de que el contenido de datos DI ha sido manipulado. El sistema operativo puede iniciar las medidas correspondientes.

El procedimiento anteriormente descrito, consistente en definir como válidos únicamente determinados niveles de una celda de memoria de niveles múltiples, también puede ser utilizado para llevar a cabo un borrado seguro, próximo a *hardware*, de celdas de memoria de niveles múltiples. Para ello, en una operación de borrado, los niveles definidos hasta entonces como válidos se cambian por otros no válidos. Por ejemplo, los estados autorizados identificados con "E" en la tabla mostrada en la figura 2 se transforman en estados no autorizados identificados con "NE", y los estados no autorizados se transforman en estados autorizados mediante la sustitución de "E" por "NE". En este caso, la celda de memoria todavía puede ser leída, pero proporciona contenidos de datos inservibles. La redefinición de niveles para simular un borrado es tanto más eficaz cuanto mayor es la cantidad de estados posibles de una celda de memoria.

Dado que los niveles representan diferentes estados físicos de una celda de memoria, también pueden ser aprovechados para compensar cambios físicos típicos de las celdas de memoria debidos al paso del tiempo. Las celdas de memoria envejecen por diferentes condiciones ambientales, tales como humedad del aire, calor o radiación, entre otras causas. Con el tiempo esto conduce a una degradación de la función. Por regla general, en algún momento ciertos niveles ya no se pueden ajustar de forma fiable o cambian por sí solos. Pero el cambio en la funcionalidad normalmente es permanente y sigue un principio fijo determinista. Por ejemplo, con el paso del tiempo disminuye la capacidad de una celda de memoria para almacenar cargas correspondientes a los niveles individuales, de modo que un nivel representado por una carga corresponde aparentemente a otro contenido de datos. Mediante una definición adecuada de una tabla de validez, tal como se muestra en la figura 2, se puede compensar la función modificada de una o más celdas de memoria. Por ejemplo, una tabla de validez de este tipo podría presentar en cada caso entre dos estados autorizados "E" al menos un estado no autorizado "NE". Teniendo en cuenta la funcionalidad modificada previsible se puede llevar a cabo una compensación de la siguiente manera: por ejemplo, en caso de presencia de un estado no autorizado "NE" se adopta como valor real el siguiente estado autorizado "E" más alto, para tener en cuenta que el nivel de la celda de memoria ha disminuido. Evidentemente, la transformación de la compensación puede tener lugar mediante mecanismos más complejos. Gracias a la compensación, una celda de memoria puede seguir siendo utilizada al menos durante cierto tiempo aunque ya no esté totalmente intacta. Convenientemente, la ejecución de una compensación se indica a través de medios de salida adecuados, para que la celda de memoria pueda ser sustituida o desactivada.

Para averiguar si una celda de memoria presenta cambios compensables debidos al paso del tiempo o a influencias ambientales se pueden comprobar fácilmente si bloques de celdas de memoria adyacentes presentan cambios similares o que sigan un patrón determinado puro. Alternativamente, la comprobación de cambios debidos al paso del tiempo o a influencias ambientales se puede llevar a cabo mediante sensores especiales.

El procedimiento según la invención permite almacenar datos a prueba de manipulación en memorias de niveles múltiples de un soporte de datos, sin que sea necesario utilizar sumas de control adicionales. El procedimiento se basa en la utilización de una tecnología de memoria disponible con celdas de memoria de niveles múltiples. El procedimiento se puede emplear de forma sencilla y con poco gasto en un sistema operativo utilizado.

REIVINDICACIONES

1. Procedimiento para almacenamiento seguro de datos en una memoria de niveles múltiples de un soporte de datos portátil, incluyendo la memoria de niveles múltiples una o más celdas de memoria de niveles múltiples (SZ) que pueden adoptar respectivamente al menos tres niveles (E, NE) que representan un contenido de datos diferente, en el que los respectivos niveles (E, NE) de una celda de memoria (SZ) se predefinen como válidos o no válidos, caracterizado porque, los niveles (E, NE) de una respectiva celda de memoria (SZ) se predefinen selectivamente como válidos o no válidos en función de un nivel de seguridad requerido.
2. Procedimiento según la reivindicación 1, caracterizado porque la relación entre el número de niveles válidos y el número de niveles no válidos de una respectiva celda de memoria (SZ) varía en función del nivel de seguridad requerido.
3. Procedimiento según la reivindicación 1 o 2, caracterizado porque, si se requiere un nivel de seguridad máximo, la celda de memoria solo presenta un nivel válido (E, NE).
4. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque, si se requiere un nivel de seguridad mínimo, todos los niveles (E, NE) de la celda de memoria (SZ) son válidos.
5. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque la predefinición de niveles válidos y no válidos para la celda o las celdas de memoria (SZ) de la memoria de niveles múltiples tiene lugar de forma dinámica o en el marco de su fabricación.
6. Procedimiento según la reivindicación 5, caracterizado porque la predefinición dinámica de niveles válidos y no válidos para la celda o las celdas de memoria (SZ) se lleva a cabo recurriendo a una tabla, una función o un generador de números pseudoaleatorios cuya salida es determinista.
7. Procedimiento según la reivindicación 6, caracterizado porque durante la lectura de datos de una celda de memoria (SZ) se determinan los niveles autorizados (E, NE) a través de la tabla, función o generador de números pseudoaleatorios para la celda de memoria (SZ) correspondiente.
8. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque durante la lectura de una celda de memoria (SZ) de la memoria de niveles múltiples se comprueba si ésta representa un contenido de datos autorizado o no autorizado conforme a los niveles (E, NE) válidos o no válidos predefinidos; si el contenido de datos está autorizado, éste se facilita para su posterior procesamiento, y si el contenido de datos no está autorizado, se deduce que se ha producido una manipulación de la celda de memoria (SZ).
9. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque, si se ha detectado un cambio en una celda de memoria (SZ) debido al paso del tiempo o a influencias ambientales, en caso de presencia de un nivel no válido (NE) en dicha celda de memoria se considera que el siguiente nivel autorizado (E) más alto es el nivel real.

	SZ	SZ	SZ	SZ
ADR	0x8000	0x8001	0x8002	0x8003
INH1	0	1	0	1
LAD1				
INH2	0	1	2	3
LAD2				

Fig. 1

	SZ	SZ	SZ	SZ
ADR	0x8000	0x8001	0x8002	0x8003
INH	0	1	2	3
	NE	E	E	NE
AKT	M	R	R	M

Fig. 2

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

5 La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citados en la descripción

- US 6331946 B1 [0005]