(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 639 061**

(51) Int. CI.:

G06K 19/073 (2006.01)
G06F 21/00 (2013.01)
G07D 7/00 (2006.01)
H04L 9/06 (2006.01)
H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.09.2011 E 11007400 (2)**

(97) Fecha y número de publicación de la concesión europea: **12.07.2017 EP 2428918**

(54) Título: **Soporte de almacenamiento de datos portátil**

(30) Prioridad:

14.09.2010 DE 102010045328

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.10.2017

(73) Titular/es:

GIESECKE+DEVRIENT MOBILE SECURITY GMBH (100.0%)
Prinzregentenstraße 159
81677 München, DE

(72) Inventor/es:

BUTZ, KLAUS;
LAMLA, MICHAEL y
WIRÉN, ARVID

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Soporte de almacenamiento de datos portátil

La presente invención se refiere a un soporte de almacenamiento de datos portátil con al menos una celda de memoria no volátil, a un procedimiento en un soporte de almacenamiento de datos de este tipo y a un sistema que comprende un soporte de almacenamiento de datos de este tipo y un dispositivo de lectura. En particular, la presente invención se refiere a soportes de almacenamiento de datos portátiles en forma de tarjetas de chip, tarjetas de identificación, tarjetas con función de pago, tarjetas inteligentes, tarjetas de telefonía móvil (U)SIM, tarjetas multimedia seguras y similares.

Se conoce que estos soportes de almacenamiento de datos pueden sufrir distintos ataques que provocan fallos de funcionamiento y de procesamiento en los mismos, acarreando, por ejemplo, la lectura no autorizada de datos relevantes para la seguridad o que puedan eludirse consultas de seguridad como, por ejemplo, una consulta de PIN. En este contexto se conocen en particular los ataques que tienen lugar mediante variación de la tensión de suministro, radiación de luz, influencia de calor o frío y similares, así como ataques basados en la radiación del soporte de almacenamiento de datos mediante radiación ionizante y, en particular, con radiación alfa.

En el caso de un componente semiconductor irradiado con radiación ionizante, las zonas que previamente no eran conductoras del componente semiconductor pueden convertirse temporalmente en conductoras debido a la ionización, lo que produce alteraciones en puntos clave de la ejecución de programas o fallos en procesamientos criptográficos del soporte de almacenamiento de datos, a partir de los cuales, mediante un análisis diferencial de fallos (DFA), es posible obtener conclusiones sobre datos secretos del soporte de almacenamiento de datos.

Para detectar este tipo de ataques, el documento DE 103 45 240 A1 propone un circuito integrado con un elemento sensible a la radiación, que presenta una característica de conmutación que se modifica de forma irreversible tras la suficiente dosis de radiación. En ese caso, el circuito integrado, por ejemplo, se desconecta. El elemento sensible a la radiación es en este caso un diodo operado en dirección de bloqueo, cuya corriente de bloqueo aumenta bajo el efecto de la radiación hasta un valor límite predeterminado, desconectándose el circuito integrado al alcanzar dicho valor. Alternativamente también se puede utilizar un transistor o una resistencia de polisilicio como elemento sensible a la radiación.

No obstante, para que tenga lugar la desconexión del circuito integrado a consecuencia de un ataque se requiere una dosis de radiación relativamente elevada, por lo que, debido a la falta de sensibilidad del elemento sensible a la radiación, no es posible detectar de forma efectiva todos los ataques. Debido a que la característica de conmutación del elemento sensible a la radiación se modifica de forma irreversible, la dosis de radiación que actúa durante toda la vida útil del soporte de almacenamiento de datos se mide de forma acumulativa, por lo que la dosis de radiación total para la cual se desconecta el soporte de almacenamiento de datos se debe elegir lo suficientemente grande.

El documento WO 2008/070071 y el documento US 2008/0129504 se refieren a etiquetas RFID con una memoria de datos sensible a la radiación en la que está almacenado un código individual. Cuando actúa una radiación se producen fallos en la memoria de datos sensible a la radiación, de forma que, mediante la lectura del código, se puede determinar si la etiqueta ha recibido anteriormente una radiación elevada. Sin embargo, no está prevista la detección directa de un ataque de radiación y una desactivación lo más rápida posible de la etiqueta RFID.

El documento DE 10 2004 009 622 A1 da a conocer un elemento constructivo semiconductor en el que están previstas conexiones “bulk”, a través de las cuales se detecta una corriente en la dirección de bloqueo de diodos “bulk” entre regiones dopadas y un dopaje básico del cuerpo semiconductor para poder activar una función de alarma o de protección en caso de radiación de luz.

El documento DE 10 2005 058 238 A1 da a conocer un circuito en el que siete transistores están conectados entre sí de forma que se obtiene un circuito de detección digital. En caso de manipulación el estado del circuito de detección se conmuta de manera que se detecta el intento de manipulación. En una realización preferente, varios circuitos de detección están conectados entre sí en cadena, de forma que una señal que indica un intento de manipulación se propaga en cadena. En una aplicación ventajosa, varios circuitos de detección están integrados en un campo de memoria. La invención se refiere además a un procedimiento para operar una disposición de circuito, en la que se detectan manipulaciones externas.

Por lo tanto, la presente invención tiene como objetivo proteger un soporte de almacenamiento de datos portátil de forma fiable y a tiempo contra ataques con radiación ionizante.

Este objetivo se consigue con las características de las reivindicaciones independientes. En las reivindicaciones dependientes se indican configuraciones y perfeccionamientos ventajosos de la invención.

Un soporte de almacenamiento de datos según la invención comprende al menos una celda de memoria no volátil, un dispositivo de supervisión y un dispositivo de control. En un modo de supervisión, el dispositivo de supervisión

supervisa de forma permanente, es decir, esencialmente sin interrupción, un flujo de corriente entre dos conexiones de la al menos una celda de memoria para detectar de este modo una modificación reversible del flujo de corriente que indica que hay un ataque mediante radiación ionizante, especialmente un ataque con radiación alfa. El dispositivo de control conmuta el soporte de almacenamiento de datos a un estado seguro en función de la modificación del flujo de corriente que indica que hay un ataque mediante radiación ionizante.

Mediante la supervisión permanente del flujo de corriente es posible detectar un ataque mediante radiación ionizante de forma fiable y rápida en el modo de supervisión. El soporte de almacenamiento de datos es conmutado entonces inmediatamente al estado seguro, contrarrestando dicho ataque de forma segura. Mediante el uso de una celda de memoria no volátil para la detección de la radiación ionizante se logra una sensibilidad de detección elevada, ya que se detectan las modificaciones del flujo de corriente, que son reversibles, debido a la acción de la radiación ionizante. De este modo se pueden diferenciar y cuantificar por separado los ataques individuales, ya que es posible medir y supervisar la dosis de radiación que actúa sobre el soporte de almacenamiento de datos en el periodo entre el encendido (o más precisamente, la inicialización) y el apagado del soporte de almacenamiento de datos.

El dispositivo de control conmuta el soporte de almacenamiento de datos a un estado seguro en caso de un ataque con radiación ionizante en base a una modificación del flujo de corriente a través de la celda de memoria. Alternativamente, el dispositivo de control u otro componente del soporte de almacenamiento de datos también pueden estar configurados de forma que si ocurre una modificación en el flujo de corriente, ésta vuelva a ser compensada. En este caso, el dispositivo de control puede contar el número de este tipo de modificaciones reversibles del flujo de corriente y conmutar el soporte de almacenamiento de datos al estado seguro cuando se supera un número predeterminado de ataques detectados.

De forma especialmente preferente, el dispositivo de supervisión supervisa el flujo de corriente entre una conexión fuente ("source") y una conexión sumidero ("drain") de una celda de memoria EPROM o una celda de memoria EEPROM del soporte de almacenamiento de datos. Este tipo de celdas de memoria (E)EPROM están compuestas esencialmente por un transistor de efecto campo con una puerta aislada (denominada "floating Gate") sobre la cual se puede aplicar una carga para el almacenamiento de datos.

Habitualmente, el proceso de lectura de una celda de memoria de este tipo tiene lugar mediante selección de dicha celda y aplicación de un potencial a una puerta de control ("control gate") de la celda de memoria. El estado de carga en la "floating gate" influye sobre la corriente entre el sumidero y la fuente, que es interpretada en los amplificadores de lectura por medio de un valor umbral como un 1 ó 0 lógico.

La "floating gate" está aislada de forma que la carga aplicada no se puede perder durante un largo periodo de tiempo (por ejemplo, durante décadas). No obstante, mediante la acción de una radiación ionizante, la carga de la "floating gate" se descarga más rápidamente, por lo que se modifica el flujo de corriente entre la conexión fuente y la conexión sumidero de la celda de memoria (E)EPROM bajo la acción de una radiación ionizante.

Este efecto se utiliza en este caso para la detección altamente sensible de la radiación con el fin de detectar, en función de ésta, una modificación del flujo de corriente. De ello resulta una modificación del estado lógico al quedar el valor por encima o por debajo de un valor umbral en los amplificadores de lectura. En este caso, el soporte de almacenamiento de datos es conmutado al estado seguro.

Para volver a aplicar o aplicar inicialmente una carga en la "floating gate" de la celda de memoria (E)EPROM, el soporte de almacenamiento de datos comprende preferentemente un dispositivo de carga correspondiente. La carga puede aplicarse, por ejemplo, mediante control simultáneo de una conexión denominada conexión de control y de la conexión sumidero de la celda de memoria (E)EPROM. De este modo se puede volver a compensar una modificación reversible del flujo de corriente entre la conexión fuente y la conexión sumidero de la celda de memoria, causada por un ataque de radiación.

El flujo de corriente de la celda de memoria es supervisado preferentemente tras la aplicación de la carga. Es decir que la supervisión o el modo de supervisión comienza cuando en la "floating gate" de la celda de memoria se encuentra una carga suficiente. Alternativamente, el modo de supervisión puede activarse también antes de aplicar la carga. No obstante, en este caso, mientras no se haya aplicado ninguna carga en la "floating gate" de la celda de memoria, se producirá un flujo de corriente en la celda de memoria, que podría ser detectado (erróneamente) como ataque de radiación. En este caso, el dispositivo de control está configurado preferentemente para ignorar aumentos del flujo de corriente mientras no se haya aplicado la suficiente carga en la "floating gate".

El soporte de almacenamiento de datos o su dispositivo de supervisión están configurados preferentemente de forma que el modo de supervisión siempre está activado cuando un ataque de radiación pudiera ser, en principio, exitoso, es decir, cuando pudiera poner en riesgo la seguridad del soporte de almacenamiento de datos. Por lo tanto, el modo de supervisión se activa preferentemente inmediatamente después de la inicialización del soporte de almacenamiento de datos. La inicialización puede consistir, por ejemplo, únicamente en aplicar una carga en la puerta de la celda de memoria. Preferentemente, durante la inicialización no se realiza en el soporte de almacenamiento de datos ningún tipo de operación de procesamiento u operación de almacenamiento que, en caso

de un ataque mediante radiación ionizante, podría poner en riesgo la seguridad del soporte de almacenamiento de datos y de los datos almacenados en el mismo. De forma especialmente preferente, el soporte de almacenamiento de datos no realiza ningún tipo de operación de procesamiento y/u otro tipo de operaciones durante la inicialización. El modo de supervisión finaliza preferentemente al finalizar el apagado del soporte de almacenamiento de datos.

Preferentemente, el dispositivo de supervisión comprende al menos un comparador de tensión analógico, por ejemplo, un amplificador operacional, para la supervisión permanente del flujo de corriente de una celda de memoria.

El dispositivo de control conmuta el soporte de almacenamiento de datos preferentemente al estado seguro desactivando funcionalidades específicas del soporte de almacenamiento de datos. En este sentido, se puede tratar de cualquier funcionalidad. Preferentemente, no obstante, en el estado seguro están desactivadas funcionalidades relevantes para la seguridad, por ejemplo, aquellas que comprenden operaciones criptográficas, operaciones en relación con datos relevantes para la seguridad, como por ejemplo contraseñas o claves criptográficas, o similares. En principio, en el estado seguro se puede desactivar cualquier funcionalidad que se conoce o se sospecha que puede ser probablemente atacada mediante radiación ionizante. Por ejemplo, se pueden desactivar todas las funcionalidades. En función de los requisitos de seguridad y del tipo de soporte de almacenamiento de datos también se pueden desactivar todas las funcionalidades del soporte de almacenamiento de datos de forma duradera o temporal.

Según un modo de realización preferente, el dispositivo de control conmuta el soporte de almacenamiento de datos de forma duradera al estado seguro para excluir que la seguridad del soporte de almacenamiento de datos finalmente se pueda ver afectada por otros ataques. También es posible que en el estado seguro determinadas funciones críticas estén desactivadas de forma duradera y otras únicamente por un periodo de tiempo predeterminado para que el soporte de almacenamiento de datos permanezca utilizable para funciones menos críticas o básicas.

La celda de memoria está dispuesta preferentemente en una zona de componentes electrónicos relevantes para la seguridad del soporte de almacenamiento de datos o en un chip del soporte de almacenamiento de datos con componentes electrónicos relevantes para la seguridad. De este modo se pueden detectar de forma segura los ataques específicos a estos componentes mediante radiación ionizante. Técnicamente no es posible determinar con una precisión específica el objetivo de un ataque con radiación ionizante, por ejemplo, mediante apantallamiento. No obstante, mediante la disposición de una celda de memoria según la invención o una pluralidad de las mismas en una zona con componentes electrónicos relevantes para la seguridad o distribuidas por una zona de este tipo se puede detectar con suficiente precisión un ataque inespecífico a los componentes relevantes para la seguridad. Preferentemente, el soporte de almacenamiento de datos también se puede conmutar al estado seguro cuando no solo se constata una modificación significativa del flujo de corriente en una celda de memoria individual, sino cuando se detectan modificaciones de los respectivos flujos de corriente en una pluralidad de celdas de memoria, cuya suma indica que hay a un ataque con radiación ionizante.

Según un modo de realización preferente, los componentes electrónicos relevantes para la seguridad comprenden al menos una celda de memoria de datos, en la que están almacenados los datos relevantes para la seguridad. En cuanto a los componentes relevantes para la seguridad éstos pueden ser también procesadores o chips criptográficos, procesadores o chips de seguridad, o similares.

Preferentemente, la al menos una celda de memoria según la invención está dispuesta oculta sobre el soporte de almacenamiento de datos o dentro de componentes relevantes para la seguridad o del chip de seguridad. Esto significa que las celdas de memoria no pueden ser reconocidas y localizadas en el soporte de almacenamiento de datos por un atacante mediante los métodos de inspección habituales, por ejemplo, mediante inspección visual, inspección con rayos X, inspección microscópica o similares. Para ello, un componente de memoria u otro componente relevante para la seguridad del soporte de almacenamiento de datos puede comprender tanto celdas de memoria según la invención para la detección de ataques como también celdas de memoria de datos tradicionales para el almacenamiento de datos de forma que las celdas de memoria según la invención no puedan o prácticamente no puedan ser diferenciadas de las celdas de memoria de datos mediante métodos de inspección habituales, especialmente no puedan serlo debido a una disposición especial y/o configuración reconocible de las celdas de memoria según la invención en el componente de memoria.

La al menos una celda de memoria está configurada preferentemente de manera que el flujo de corriente de la celda de memoria reacciona de forma sensible a un ataque con radiación ionizante. Para ello, la curva característica de la celda de memoria se puede especificar de forma que el flujo de corriente de la celda de memoria se modifique lo menos posible para una dosis de radiación que sea muy baja para un ataque con radiación ionizante, por ejemplo, para una radiación de fondo habitual en el entorno. Sin embargo, ante una dosis de radiación que indique que hay un ataque con radiación ionizante, el flujo de corriente de la celda de memoria reacciona con una modificación significativa. Preferentemente, en la zona de las celdas de memoria según la invención no se realiza ningún tipo de medida de protección o solo medidas de protección limitadas contra la radiación ionizante mediante

apantallamientos o similares, aunque está prevista una protección contra otros tipos de interferencias, especialmente por radiación de luz.

Según un modo de realización preferente, el soporte de almacenamiento de datos comprende una pluralidad de celdas de memoria según la invención, controlando el dispositivo de control los flujos de corriente entre las respectivas conexiones de la pluralidad de celdas de memoria y conmutando el dispositivo de control el soporte de almacenamiento de datos al estado seguro en caso de una modificación del flujo de corriente, que indique que hay una radiación ionizante, en al menos una cantidad predeterminada de celdas de memoria. También es posible que el dispositivo de control conmute el soporte de almacenamiento de datos al estado seguro cuando la modificación total de todos los flujos de corriente en la pluralidad de celdas de memoria supere un valor predeterminado.

De este modo se puede evitar una conmutación demasiado pronta del soporte de almacenamiento de datos al estado seguro aunque en celdas de memoria individuales se detecten modificaciones significativas del flujo de corriente que, en comparación con los otros flujos de corriente en todas las otras celdas de memoria según la invención, probablemente no se deban a un ataque mediante radiación ionizante, sino, por ejemplo, más bien indiquen que hay celdas de memoria defectuosas. Tomando esto como base, para hacer posible una detección segura y robusta de un ataque de radiación, preferentemente se alojan una pluralidad de celdas de memoria, opcionalmente contiguas, en una zona de un componente relevante para la seguridad del soporte de almacenamiento de datos.

Otras características y ventajas de la invención resultan de la siguiente descripción de los ejemplos de realización según la invención, así como de otras alternativas de realización en relación a los dibujos, que muestran esquemáticamente:

Figura 1: un soporte de almacenamiento de datos portátil según la invención; y

Figura 2: un circuito integrado del soporte de almacenamiento de datos con celdas de memoria según la invención, un dispositivo de supervisión, un dispositivo de control y un dispositivo de carga.

La figura 1 muestra esquemáticamente un soporte de almacenamiento de datos portátil según la invención en forma de una tarjeta de chip -1-. La tarjeta de chip -1- comprende un chip de tarjeta de chip -10- que está conectado a través de un conductor de datos -3- a las superficies de contacto -2- de la tarjeta de chip -1-. Para una visualización más clara, la figura 1 muestra una tarjeta de chip -1- cuyo chip de tarjeta de chip -10- está dispuesto lateralmente junto a las superficies de contacto -2-. Naturalmente, y de forma preferente en la práctica, el chip de tarjeta de chip -10- también puede encontrarse directamente debajo de las superficies de contacto -2-. En el presente ejemplo, el chip de tarjeta de chip -10- comprende una memoria de datos no volátil -11-, en este caso una memoria EPROM o una memoria EEPROM, un procesador -12- y una memoria de datos volátil -13-, por ejemplo, una memoria de trabajo RAM. En principio, la tarjeta de chip -1- y el chip de tarjeta de chip -10- están dotados además con todos los demás componentes habituales y necesarios en la práctica cuya explicación, no obstante, se omite en adelante, siempre y cuando no sean relevantes para la invención.

La memoria (E)EPROM -11- comprende, además de la pluralidad de celdas de memoria de datos para el almacenamiento de datos (no mostradas), también una pluralidad de celdas de memoria -20- especialmente configuradas para detectar ataques mediante radiación ionizante a la tarjeta de chip -1- y sus componentes. Las celdas de memoria -20- están conectadas a un dispositivo de supervisión -30- (las conexiones no están representadas) que, en el modo de realización según la figura 1, forma parte del chip de tarjeta de chip -10- y supervisa de forma permanente un flujo de corriente entre las conexiones fuente -S- y sumidero -D- de las celdas de memoria -20- en un modo de supervisión. El chip -10- comprende además un dispositivo de control -40- que, en función de la modificación del flujo de corriente detectada por el dispositivo de supervisión en las celdas de memoria -20- respectivas, conmuta la tarjeta de chip -1- a un estado seguro. Un dispositivo de carga -50- sirve para aplicar una carga en las celdas de memoria -20-.

La figura 2 muestra un circuito integrado del chip -10- de la tarjeta de chip -1-, que comprende una pluralidad de celdas de memoria -20-, un dispositivo de supervisión -30-, un dispositivo de control -40- y un dispositivo de carga -50-. Para lograr mayor claridad, la figura 2 solo muestra dos celdas de memoria -20'- y -20"- de la pluralidad de celdas de memoria -20- de la figura 1.

Para detectar un ataque mediante radiación ionizante, en primer lugar, antes de cada uso de la tarjeta de chip -1- se aplica en cada celda de memoria -20- una carga en una puerta de la celda de memoria -20- mediante un dispositivo de carga -50- o se recarga una carga parcial existente previamente en la puerta, es decir, se eleva a un valor de carga predeterminado. La carga tiene lugar mediante control de la conexión de control -SG- y la conexión sumidero -D- de la celda de memoria -20- respectiva.

La puerta de la celda de memoria -20- está aislada de forma que la carga aplicada no se pierde durante un largo periodo de tiempo. Sin embargo, bajo la acción de radiación ionizante, la puerta se descarga de forma

esencialmente más rápida, lo que se constata debido a un flujo de corriente creciente entre la conexión fuente -S- y la conexión sumidero -D- de la celda de memoria (E)EPROM -20- respectiva.

Tras haber aplicado o recargado la carga de la puerta se inicia el modo de supervisión, en el que el dispositivo de supervisión -30- supervisa de forma permanente los flujos de corriente en las celdas de memoria -20-. El flujo de corriente es supervisado para cada celda de memoria -20- individualmente mediante los comparadores de tensión -30a- o amplificadores operacionales respectivos Para ello, la entrada (+) del comparador de tensión -30a- está conectada a una fuente de tensión fija -30b-. Una segunda entrada (-) del comparador de tensión -30a- está conectada a la conexión sumidero -D- de la celda de memoria -20- y conectada a una tensión de entrada -Uo- a través de una resistencia previa -30c-. La conexión fuente -S- de la celda de memoria -20- está conectada a masa. Mientras en la puerta de la celda de memoria -20- hay una carga, el flujo de corriente $-I_3-$ a través de la celda de memoria es reducido y, por tanto, el flujo de corriente $-I_1-$ a través de la resistencia -30c- es bajo, ya que éste se compone del flujo de corriente $-I_3-$ y el flujo de corriente $-I_2-$ (también bajo) hacia la entrada (-) del comparador de tensión -30a-. Correspondientemente, a través de la resistencia -30c- solo se produce una caída de tensión reducida y la tensión en la entrada (-) del comparador de tensión -30a- es sólo un poco más baja que la tensión -Uo-. Cuando la carga de la puerta de la celda de memoria se reduce debido a la acción de radiación ionizante, entonces aumenta el flujo de corriente $-I_3-$ a través de la celda de memoria -20- y, por tanto, aumenta el flujo de corriente -h-, en la resistencia -30c- la caída de tensión es mayor, es decir, la tensión $-U_1-$ baja al aumentar el flujo de corriente por la celda de memoria -20-.

La tensión de la fuente de tensión fija -30b- se elige de forma que ésta sea inferior a la tensión $-U_1-$ inicialmente, es decir, para una carga completa de la puerta. Mientras éste sea el caso, el comparador -30a- emite una señal de salida negativa. Sin embargo, si debido a la acción de radiación ionizante la tensión $-U_1-$ baja por debajo de la tensión -Uc- de la fuente de tensión fija -30b-, la señal de salida del comparador -30a- cambia de negativa a positiva. De forma correspondiente, en el presente ejemplo de realización se fija un valor umbral a través de la tensión -Uc- de la fuente de tensión fija -30b- (en relación con la tensión de entrada -Uo-, también fija, y el valor de resistencia de la resistencia -30c-), a partir del cual el flujo de corriente $-I_3-$ a través de la celda de memoria -20- y, por tanto, la dosis de radiación medida son considerados críticos, es decir, son interpretados como un ataque mediante radiación ionizante.

El dispositivo de control -40- recibe la señal de salida del dispositivo de supervisión -30-. Si el dispositivo de supervisión -30- constata una modificación del flujo de corriente $-I_3-$ que indica que hay un ataque mediante radiación ionizante en una cantidad predeterminada de celdas de memoria -20-, por ejemplo, en ambas celdas de memoria -20´- y -20"- en la figura 2, el dispositivo de control -40- desactiva todas las funcionalidades de la tarjeta de chip -1- de forma irreversible. Esto tiene lugar en el ejemplo de realización mostrado decrementando un contador en el chip -10- cuando el dispositivo de supervisión -30- informa de una modificación significativa del flujo de corriente de una celda de memoria -20- y el dispositivo de control -40- bloquea todas las funcionalidades de la tarjeta de chip -1- de forma irreversible al alcanzar el valor de contador "cero". Alternativamente, el dispositivo de control -40- también puede comprender exclusivamente componentes analógicos y desactivar las funcionalidades de la tarjeta de chip -1- destruyendo partes del chip -10- mediante aplicación de una tensión.

De igual forma, tras constatar una modificación reversible del flujo de corriente $-I_3-$ en una de las celdas de memoria -20-, que indica que hay un ataque mediante radiación ionizante, se puede volver a aplicar una carga en la puerta de esta celda de memoria -20- o recargar la carga. Entonces se cuentan las veces en que se ha modificado reversiblemente el flujo de corriente y tras alcanzar un número predeterminado de veces en que se ha modificado significativamente se desactivan las funcionalidades de la tarjeta de chip -1-.

En el presente ejemplo de realización, las operaciones relevantes para la seguridad en la tarjeta de chip -1- tienen lugar exclusivamente cuando la tarjeta de chip -1- se encuentra en el modo de supervisión.

En el ejemplo de realización representado en la figura 1, las celdas de memoria no volátil -20- utilizadas para determinar un ataque mediante radiación ionizante están distribuidas según un patrón irregular en la memoria (E)EPROM -11-. Además, las celdas de memoria -20- están configuradas de forma que apenas se diferencian en sus características reconocibles (especialmente en el caso de una inspección microscópica del chip -10-) de otras celdas de memoria de datos de la memoria (E)EPROM -11-, que sirven para el almacenamiento de datos. Esto dificulta a un atacante la localización y la manipulación o el apantallamiento de las celdas de memoria -20-. El dispositivo de supervisión -30-, el dispositivo de control -40- y el dispositivo de carga -50- también están dispuestos en el chip de tarjeta de chip -10- de forma difícilmente localizable.

Además, las celdas de memoria -20- están distribuidas en el chip -10- de forma que, en la zona de los componentes relevantes para la seguridad de la tarjeta de chip -1- está prevista una cantidad suficiente de celdas de memoria -20- para que un ataque de radiación sobre uno de los componentes relevantes para la seguridad siempre provoque una modificación significativa del flujo de corriente en al menos una cantidad predeterminada de celdas de memoria -20-. La disposición de las celdas de memoria -20- en o cerca de los componentes relevantes para la seguridad se configura de forma que un ataque sea detectado por una cantidad suficiente de celdas de memoria -20- incluso si el atacante irradia precisamente solo una zona muy pequeña del chip -10- mediante apantallamiento del chip -10-. En

el presente ejemplo de realización, todas las celdas de memoria de datos que sirven para el almacenamiento de datos de la memoria (E)EPROM -11-, el procesador -12-, la memoria de datos volátil -13-, el dispositivo de supervisión -30-, el dispositivo de control -40- y el dispositivo de carga -50- son componentes electrónicos relevantes para la seguridad de la tarjeta de chip -1-.

Aunque las celdas de memoria -20- que sirven para detectar ataques mediante radiación ionizante están configuradas de forma que resulten difíciles de localizar y difíciles de diferenciar de las celdas de memoria de datos tradicionales para un atacante, las celdas de memoria -20- están optimizadas adicionalmente para que el flujo de corriente de cada una de las celdas de memoria -20- reaccione de forma sensible a un ataque con radiación ionizante. Para ello, las celdas de memoria -20- están protegidas lo menos posible (mediante apantallamiento o similares) contra la radiación ionizante a detectar, mientras que están lo suficientemente protegidas contra otros tipos de interferencias que afectan el flujo de corriente -I_3- pero no se deben a radiación ionizante, por ejemplo, radiación de luz o similares. De este modo se evita que la incidencia de luz diurna normal sea interpretada erróneamente como ataque mediante radiación ionizante.

La tarjeta de chip -1- según la invención está protegida contra todos los ataques mediante radiación ionizante, especialmente contra radiación alfa, radiación beta y radiación gamma. No obstante, la invención ofrece una protección especialmente buena contra ataques mediante radiación alfa.

REIVINDICACIONES

1. Soporte de almacenamiento de datos portátil (1) que comprende
al menos una celda de memoria no volátil (20) y
un dispositivo de supervisión (30) configurado para supervisar de forma permanente un flujo de corriente (I_3) entre una conexión fuente (S) y una conexión sumidero (D) de la celda de memoria (20) en un modo de supervisión con el fin de detectar una modificación del flujo de corriente (I_3), **caracterizado por**
un dispositivo de control (40) configurado para conmutar el soporte de almacenamiento de datos (1) a un estado seguro en función de la modificación detectada del flujo de corriente (I_3) desactivando funcionalidades específicas del soporte de almacenamiento de datos (1), tal que la celda de memoria (20) es una celda de memoria EPROM (20) o una celda de memoria EEPROM (20),
tal que el soporte de almacenamiento de datos incluye un dispositivo de carga configurado para aplicar una carga en una puerta de la celda de memoria (20) antes de cada uso del soporte de almacenamiento de datos (1) con el fin de detectar un ataque mediante radiación ionizante a través de una descarga de la puerta, considerándose un aumento del flujo de corriente como consecuencia de la descarga de la puerta como indicio de un ataque de este tipo.

2. Soporte de almacenamiento de datos portátil (1), según la reivindicación 1, **caracterizado por que** el modo de supervisión se inicia inmediatamente después de inicializar el soporte de almacenamiento de datos (1).

3. Soporte de almacenamiento de datos portátil (1), según cualquiera de las reivindicaciones 1 a 2, **caracterizado por que** el dispositivo de control (40) está configurado para conmutar el soporte de almacenamiento de datos (1) de forma irreversible al estado seguro.

4. Soporte de almacenamiento de datos portátil (1), según cualquiera de las reivindicaciones 1 a 3, **caracterizado por que** la celda de memoria (20) está dispuesta en una zona de componentes electrónicos relevantes para la seguridad del soporte de almacenamiento de datos (1) o en un chip (10) del soporte de almacenamiento de datos (1) con componentes electrónicos relevantes para la seguridad.

5. Soporte de almacenamiento de datos portátil (1), según la reivindicación 4, **caracterizado por que** los componentes electrónicos relevantes para la seguridad comprenden al menos una celda de memoria de datos, en la que están almacenados datos relevantes para la seguridad.

6. Soporte de almacenamiento de datos portátil (1), según cualquiera de las reivindicaciones 4 o 5, **caracterizado por que** la celda de memoria (20) está dispuesta en una zona de componentes electrónicos relevantes para la seguridad o en un chip (10).

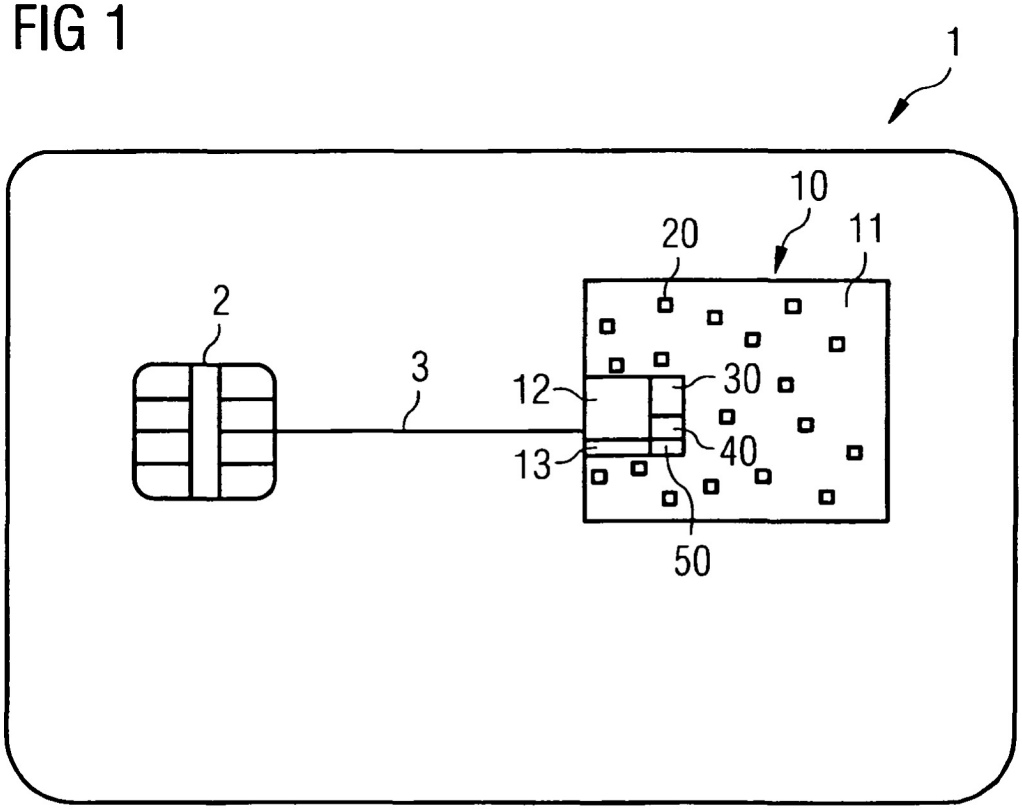
7. Soporte de almacenamiento de datos portátil (1), según cualquiera de las reivindicaciones 1 a 6, **caracterizado por que** el dispositivo de supervisión (30) comprende al menos un comparador de tensión analógico para la supervisión permanente del flujo de corriente (I_3).

8. Soporte de almacenamiento de datos portátil (1), según cualquiera de las reivindicaciones 1 a 7, **caracterizado por que** el soporte de almacenamiento de datos portátil (1) es una tarjeta de chip, una tarjeta de identificación, una tarjeta con función de pago, una tarjeta inteligente, una tarjeta de telefonía móvil (U)SIM o una tarjeta multimedia segura.

9. Procedimiento en un soporte de almacenamiento de datos portátil (1), según cualquiera de las reivindicaciones 1 a 8, con al menos una celda de memoria no volátil (20), que comprende los pasos:
supervisión permanente de un flujo de corriente (I_3) entre una conexión fuente (S) y una conexión sumidero (D) de la celda de memoria (20) mediante un dispositivo de supervisión (30) del soporte de almacenamiento de datos (1) con el fin de detectar una modificación del flujo de corriente (I_3),
caracterizado por
la conmutación del soporte de almacenamiento de datos (1) a un estado seguro mediante un dispositivo de control (40) en función de la modificación detectada del flujo de corriente (I_3),
tal que la celda de memoria (20) es una celda de memoria EPROM (20) o una celda de memoria EEPROM (20),
tal que el soporte de almacenamiento de datos (1) incluye un dispositivo de carga que, aplica una carga en una puerta de la celda de memoria (20) antes de cada uso del soporte de almacenamiento de datos (1) con el fin de detectar un ataque mediante radiación ionizante a través de una descarga de la puerta, considerándose un aumento del flujo de corriente como consecuencia de la descarga de la puerta como indicio de un ataque de este tipo.

10. Sistema que comprende al menos un soporte de almacenamiento de datos portátil (1), según cualquiera de las reivindicaciones 1 a 8, así como un dispositivo de lectura para la comunicación con el soporte de almacenamiento de datos portátil (1).

FIG 1



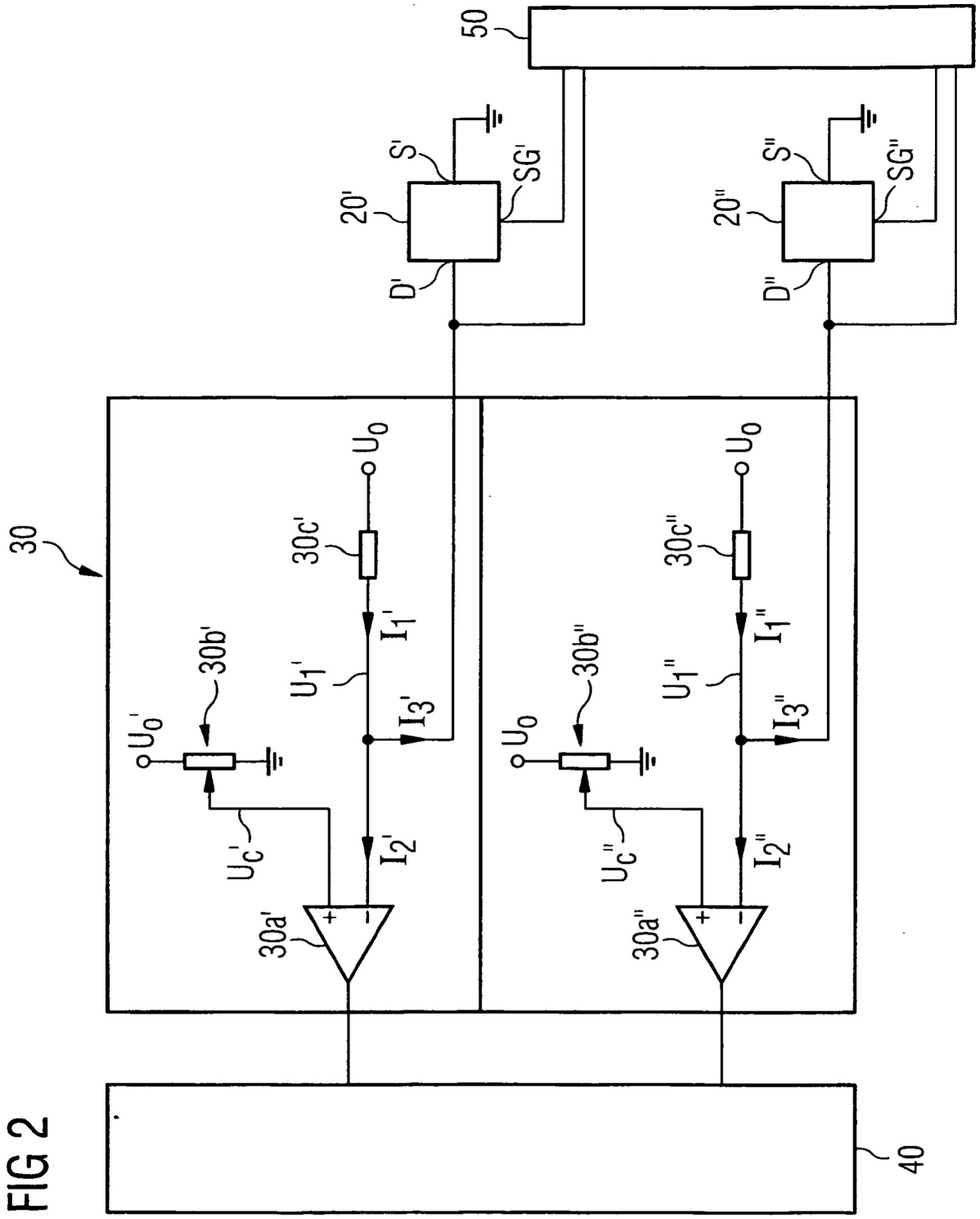

50
S'
SG'
20'
D'
S"
SG"
20"
D"
30
U_0
30c'
I_1'
U_1'
I_3'
30b'
U_0'
U_c'
I_2'
30a'
U_0
30c"
$I_1"$
$U_1"$
$I_3"$
30b"
U_0
$U_c"$
$I_2"$
30a"
40

FIG 2