(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 389 334**

(51) Int. CI.:
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **10002690 .5**
(96) Fecha de presentación: **15.03.2010**
(97) Número de publicación de la solicitud: **2230617**
(97) Fecha de publicación de la solicitud: **22.09.2010**

(54) Título: **Bloqueo de un soporte de datos portátil**

(30) Prioridad:
18.03.2009 DE 102009013852

(45) Fecha de publicación de la mención BOPI:
25.10.2012

(45) Fecha de la publicación del folleto de la patente:
25.10.2012

(73) Titular/es:
GIESECKE & DEVRIENT GMBH (100.0%)
PRINZREGENTENSTRASSE 159
81677 MÜNCHEN, DE

(72) Inventor/es:
SEEMÜLLER, KLEMENS

(74) Agente/Representante:
ARPE FERNÁNDEZ, Manuel

DESCRIPCIÓN

Bloqueo de un soporte de datos portátil

La presente invención se refiere a un procedimiento en un soporte de datos portátil para bloquear el soporte de datos, así como a un soporte de datos portátil de este tipo.

Los soportes de datos portátiles, en particular las tarjetas inteligentes (*Smart Cards*), las tarjetas de radiotelefonía móvil (U)SIM, las tarjetas multimedia seguras, las tarjetas con función de pago o similares, pueden comprometerse con un análisis del consumo de corriente del soporte de datos, por ejemplo con un ataque SPA o DPA ("Simple Power Analysis [análisis de potencia sencillo]" o "Differential Power Analysis [análisis de potencia diferencial]"), durante una determinada acción física sobre el soporte de datos, por ejemplo durante un ataque realizado con luz láser. La finalidad de tales ataques es interferir en el funcionamiento del soporte de datos portátil de tal manera que puedan reconocerse datos relevantes para la seguridad mediante un análisis del consumo de corriente o sea posible eludir una comprobación de seguridad del soporte de datos portátil.

En una medida usual para la defensa contra tales ataques, el soporte de datos en cuestión es bloqueado, al menos parcialmente, al detectarse un intento de ataque y se escribe una marca de bloqueo correspondiente en la memoria no volátil del soporte de datos. Sin embargo, un atacante puede interferir en este mecanismo de protección, ya que la escritura de la marca de bloqueo en la memoria no volátil provoca un consumo elevado de corriente y por ello puede detectarse mediante un análisis de la evolución del consumo de corriente del soporte de datos, es decir de la "firma de corriente" del proceso de escritura. Por lo tanto, un atacante puede detectar el bloqueo del soporte de datos e impedirlo por ejemplo mediante una desconexión de la alimentación de corriente del soporte de datos.

El documento DE 10322671 A1 da a conocer un dispositivo para generar un consumo de corriente adicional en un dispositivo de procesamiento de datos. El dispositivo de procesamiento de datos presenta un procesador y una memoria. El dispositivo para generar un consumo de corriente adicional está configurado para superponer un consumo de corriente adicional a un consumo de corriente útil del dispositivo de procesamiento de datos sin el dispositivo para generar un consumo de corriente adicional. El dispositivo para generar un consumo de corriente adicional presenta un dispositivo para detectar si tiene lugar o no un acceso del procesador a la memoria, así como un dispositivo para acceder a la memoria. Cuando el dispositivo para la detección detecta que no está teniendo lugar un acceso a la memoria por el procesador, el dispositivo para acceder a la memoria accede a la misma y genera con ello un consumo de corriente superpuesto al consumo de corriente útil.

El documento DE 10324419 A1 da a conocer un dispositivo para manipular información de caché contenida en una memoria caché. La información de caché está contenida en la memoria caché en varias líneas de caché. La memoria caché se halla en un dispositivo de procesamiento de datos que, además de la memoria caché, también presenta una memoria principal. El dispositivo para la manipulación consta de un dispositivo para la puesta a disposición de una señal de disparo de manipulación en instantes consecutivos, con una periodicidad fijada de manera aleatoria o determinista, así como de un dispositivo para la invalidación de una línea de caché o para la sobrescritura de una línea de caché con información procedente de la memoria principal, en respuesta a una recepción de la señal de disparo de manipulación.

Ravi S. et al "Tamper resistance mechanisms for secure embedded systems", VLSI Design, 2004, Proceedings. 17th International Conference on Mumbai, India, 5-9 de enero de 2004, Los Alamitos, CA, USA, IEEE Comput. Soc., US, Bd. 17th Conference, 1 de enero de 2004, páginas 605-611, ISBN: 978-0-7695-2072-8, ofrece una visión de conjunto de distintos ataques y explica cómo pueden utilizarse para introducirse a través de funciones de seguridad, o debilitarlas, en un sistema incorporado. El diseño a prueba de falsificación se refiere al proceso del diseño de una arquitectura de sistema, y su implementación, que esté protegida contra ataques. Se presentan planteamientos que se han propuesto para desarrollar un sistema incorporado a prueba de falsificación, en combinación con ejemplos de productos comerciales.

Francois Koeune et al, "A tutorial on physical security and side-channel attacks", 1 de enero de 2005, Foundations of security analysis and design III; lecture notes in computer science; LNCS, Springer, Berlin, DE, páginas 78 a 108, ISBN 978-3-540-28955-5, revela que una rama de la criptografía se centra en las limitaciones físicas a las que se enfrenta un equipo criptográfico real e intenta evaluar estos límites, como por ejemplo tiempos de ejecución, consumo de energía, etc., para descubrir los secretos de los equipos. Esto condujo a ataques específicos de implementación, lo que con frecuencia llevó a que éstos fuesen mucho más eficaces que los mejores ataques criptoanalíticos conocidos en relación con un sencillo ejemplo básico como objeto idealizado. Este documento ofrece una visión de conjunto de los principales tipos de ataque y muestra los principios en los que éstos se basan.

El objetivo de la presente invención es por lo tanto asegurar un bloqueo fiable del soporte de datos en caso de un intento de ataque.

Este objetivo se logra mediante un procedimiento y un soporte de datos con las características de las reivindicaciones independientes. En las reivindicaciones dependientes de éstas se indican configuraciones ventajosas y perfeccionamientos de la invención.

Según la invención se realizan de manera continua en un soporte de datos portátil accesos de escritura a una memoria del soporte de datos en instantes de escritura arbitrariamente consecutivos, bloqueándose, al menos parcialmente, el soporte de datos mediante uno de los accesos de escritura ejecutados de manera continua en caso de detectarse un intento de ataque al soporte de datos.

Correspondientemente, un soporte de datos portátil según la invención comprende al menos un procesador, una memoria y un dispositivo de detección para detectar intentos de ataque al soporte de datos, así como un dispositivo de control preparado para ejecutar accesos de escritura a la memoria de manera continua en instantes de escritura arbitrariamente consecutivos y, en el caso de que el dispositivo de detección detecte un intento de ataque, bloquear el soporte de datos, al menos parcialmente, mediante uno de los accesos de escritura ejecutados de manera continua.

Mediante esta invención se impide que un atacante detecte el bloqueo del soporte de datos analizando la evolución del consumo de corriente del soporte de datos, ya que el soporte de datos se bloquea mediante un acceso de escritura cuyo consumo de corriente no es detectable en la evolución del consumo de corriente causada por los accesos de escritura ejecutados de todos modos de manera continua. Es decir que el acceso de escritura necesario para bloquear el soporte de datos provoca un consumo de corriente de un nivel similar al de los accesos de escritura a la memoria realizados de manera continua, por lo que un atacante no puede determinar cuál de los accesos de escritura ejecutados de manera continua se utiliza para bloquear el soporte de datos.

En relación con la presente invención debe entenderse por una ejecución continua de accesos de escritura un patrón temporal de accesos de escritura que no puede resolverse en cuanto al tiempo de tal manera que un acceso de escritura para el bloqueo del soporte de datos pueda diferenciarse de otros accesos de escritura, por ejemplo como acceso de escritura aislado dentro de un intervalo prolongado sin más accesos de escritura. La ejecución continua de accesos de escritura produce por lo tanto un enmascaramiento o encubrimiento de un acceso de escritura de este tipo destinado a un bloqueo, al menos parcial, del soporte de datos.

Un patrón temporal irresoluble de accesos de escritura tal se consigue en particular si, por una parte, entre en cada dos de los respectivos accesos de escritura ejecutados de manera continua no existen intervalos de tiempo de una duración tal que, para lograr una defensa contra el intento de ataque detectado, el soporte de datos ya no pueda bloquearse a tiempo con el siguiente acceso de escritura de todos modos previsto y, por otra parte, un acceso de escritura ejecutado expresamente para el bloqueo del soporte de datos inmediatamente después de detectarse un intento de ataque no puede detectarse como irregularidad o similar dentro del patrón temporal de los accesos de escritura ejecutados de manera continua. En particular está previsto que los intervalos de tiempo entre en cada dos de los respectivos accesos de escritura ejecutados de manera continua sean más cortos que el lapso de tiempo que un atacante necesita al menos para un intento de ataque (por ejemplo el lapso de tiempo necesario para interferir en el soporte de datos y acceder de forma no autorizada a sus datos), con el fin de que un atacante no pueda eludir el bloqueo automático del soporte de datos desconectando la alimentación de corriente del soporte de datos en cada uno de los accesos de escritura continuos.

En los accesos de escritura ejecutados de manera continua se escriben preferentemente datos en una memoria no volátil del soporte de datos. Con la utilización de una memoria no volátil puede impedirse que, mediante un corte de la alimentación de corriente de una memoria volátil, sea posible borrar de nuevo una marca de bloqueo escrita en la memoria para un bloqueo del soporte de datos. La memoria no volátil es especialmente una memoria EEPROM o una memoria Flash.

Los distintos accesos de escritura continuos se realizan preferentemente de manera que se cause una evolución del consumo de corriente lo más similar posible a la evolución del consumo de corriente en el tiempo causada por un acceso de escritura destinado al bloqueo, al menos parcial, del soporte de datos, lo que puede lograrse mediante una elección adecuada de los datos a escribir. De este modo se asegura que un atacante no pueda, mediante un análisis temporal preciso de la evolución del consumo de corriente del soporte de datos, diferenciar un acceso de escritura destinado al bloqueo, al menos parcial, del soporte de datos de los demás accesos de escritura ejecutados de manera continua.

Aparte de un acceso de escritura destinado al bloqueo, al menos parcial, del soporte de datos, en los accesos de escritura ejecutados de manera continua se realizan preferentemente sólo accesos de escritura a la memoria en blanco, que no escriban ningún dato adecuado o designado para utilización, sino únicamente para enmascarar o encubrir un acceso de escritura destinado al bloqueo del soporte de datos. Sin embargo, también pueden ser accesos de escritura utilizados por una aplicación existente para la funcionalidad normal. Al mismo tiempo, una elección adecuada de los datos no adecuados o no designados para utilización permite asegurar que los accesos de escritura continuos causen una evolución del consumo de corriente lo más similar posible a la evolución del consumo de corriente causada por un acceso de escritura destinado al bloqueo, al menos parcial, del soporte de datos. En un acceso de escritura en blanco puede escribirse por ejemplo una marca de bloqueo inactiva en un área cualquiera de la memoria, con el fin de hacer irreconocible la escritura de una marca de bloqueo activa en la memoria. En un caso extremo puede también tratarse sólo de un acceso de escritura en blanco, pero que deba ser pasado por la aplicación para la funcionalidad correcta.

En el bloqueo al menos parcial del soporte de datos, preferentemente se bloquean de forma temporal o permanente aplicaciones potencialmente ejecutables o se suspenden o se bloquean o se terminan de forma temporal o permanente aplicaciones que se estén ejecutando en ese instante (es decir sus procesos de aplicación). Especialmente se bloquean aplicaciones críticas para la seguridad, es decir aplicaciones que afecten a la seguridad o la integridad del soporte de datos y sus datos o del poseedor autorizado del soporte de datos. Preferentemente se bloquean los procesos de aplicación ejecutados durante el intento de ataque detectado, ya que éstos podrían ser el objetivo del intento de ataque. Si los requisitos de seguridad son elevados, puede resultar ventajoso bloquear todas las aplicaciones o todos los procesos de aplicación ejecutados. Dependiendo de los requisitos de seguridad, el bloqueo puede ser temporal, es decir limitado en el tiempo hasta un instante concreto o hasta un suceso determinado (por ejemplo el desbloqueo mediante la introducción de un código), o permanente, es decir irrevocable.

En el bloqueo, al menos parcial, del soporte de datos pueden bloquearse también de forma temporal o permanente determinados accesos a la memoria predefinidos o todos ellos, es decir accesos de escritura o lectura no específicos o accesos en el marco de la ejecución de un proceso de aplicación o accesos de este tipo a áreas de memoria, registros o datos específicos. En particular pueden bloquearse accesos a la memoria críticos para la seguridad, que afecten especialmente a la integridad de datos confidenciales o secretos del soporte de datos o del poseedor autorizado. Si los requisitos de seguridad son elevados, se bloquean preferentemente todos los accesos a la memoria.

El soporte de datos está equipado preferentemente con un dispositivo de detección que detecte el mayor número posible de tipos distintos de ataques físicos al soporte de datos, por ejemplo ataques con luz, ataques mediante la acción de temperaturas extremas, radiación o similares. El dispositivo de detección mismo está realizado preferentemente como hardware o como software o como una combinación de hardware y software. Si se detecta un intento de ataque, el dispositivo de control recibe una señal correspondiente del dispositivo de detección y bloquea entonces el soporte de datos con el siguiente de los accesos a memoria realizados de forma continua. El soporte de datos se bloquea con especial preferencia si se detecta un intento de ataque en forma de un ataque con luz, ya que los ataques con luz son relativamente fáciles de realizar y constituyen un importante riesgo para la seguridad que se da con frecuencia. El soporte de datos se bloquea con especial preferencia mediante el acceso de escritura provocado por el dispositivo de control inmediatamente siguiente a la detección del intento de ataque, con el fin de proteger el soporte de datos lo antes posible contra el intento de ataque.

Los accesos de escritura ejecutados de manera continua puede realizarlos en particular el dispositivo de control en instantes de escritura fijamente predefinidos o determinados aleatoriamente. Por ejemplo puede predefinirse fijamente un patrón de accesos de escritura regular o que aparezca lo más irregularmente posible o puede determinarse mediante un proceso aleatorio la duración del intervalo de tiempo hasta la realización del siguiente acceso de escritura. Si los instantes de escritura se fijan mediante un proceso aleatorio, no es necesario que el instante de escritura en el que se bloquea el soporte de datos mediante uno de los accesos de escritura continuos tras la detección de un intento de ataque se determine mediante el proceso aleatorio, sino que puede situarse por ejemplo lo antes posible tras el instante en que se ha detectado el intento de ataque.

También es posible realizar los accesos de escritura en instantes de escritura dependientes de la realización de uno o varios procesos de aplicación cualesquiera o concretos en el soporte de datos. En particular, los accesos de escritura pueden realizarse cada vez que un comando determinado, un comando cualquiera o todos los comandos sean ejecutados por un proceso de aplicación. Para fijar los instantes de escritura no se requiere ningún gasto técnico adicional, en particular ningún hardware adicional.

El soporte de datos portátil es preferentemente una tarjeta inteligente, una tarjeta de radiotelefonía móvil (U)SIM, una tarjeta multimedia segura, una tarjeta con función de pago u otro soporte de datos portátil de este tipo. El dispositivo de control está realizado preferentemente como componente de software, en particular como parte de un sistema operativo del soporte de datos, por ejemplo como aplicación de sistema operativo, biblioteca de sistema operativo o similar. En este caso, el procedimiento según la invención puede implementarse muy fácilmente sin que sea necesario un hardware adicional.

De la descripción siguiente de ejemplos de realización según la invención y de otras alternativas de realización, en conexión con los dibujos, se desprenden otras características y ventajas de la invención. Los dibujos muestran:

- figura 1, esquemáticamente, la evolución del consumo de corriente de un soporte de datos portátil (a) sin un intento de ataque y (b) con un intento de ataque tratado según la invención;

- figura 2, esquemáticamente, un soporte de datos portátil según la invención.

La figura 2 muestra esquemáticamente un soporte de datos portátil 1 según la invención, por ejemplo una tarjeta inteligente, una tarjeta de radiotelefonía móvil (U)SIM, una tarjeta multimedia segura, una tarjeta con función de pago u otro soporte de datos portátil 1 de este tipo. El soporte de datos 1 comprende una unidad de memoria 2, un procesador 3, un dispositivo de detección 4 para la detección de intentos de ataque y una interfaz de comunicación 5, comprendiendo la unidad de memoria 2 una memoria permanente ROM 21 con el sistema operativo 21a del soporte de datos 1, una memoria no volátil EEPROM o Flash 22 y una memoria volátil RAM 23. El soporte de datos

portátil 1 comprende además buses de datos 6, 7, 8 mediante los cuales el procesador 3 puede comunicarse de forma bidireccional con la unidad de memoria 2, el dispositivo de detección 4 y la interfaz de comunicación 5.

En el presente ejemplo de realización, el dispositivo de detección 4 para la detección de intentos de ataque está configurado como dispositivo separado. Como alternativa, el dispositivo de detección 4 puede estar realizado también mediante una aplicación o función de sistema operativo almacenada en la unidad de memoria 2. El dispositivo de detección 4 está preparado para detectar cualesquiera ataques físicos al soporte de datos 1, en particular ataques basados en la acción de una radiación, por ejemplo ataques con luz.

El soporte de datos 1 comprende también un dispositivo de control 21b que, como se muestra en la figura 1a, realiza de manera continua, en instantes de escritura arbitrariamente consecutivos t_{n-2}, t_{n-1}, t_n, t_{n+1}, accesos de escritura a la memoria no volátil 22. Si, como se ilustra en la figura 1b en el instante t_a con un rayo, tiene lugar un intento de ataque y éste es detectado por el dispositivo de detección 4, el soporte de datos 1 no es bloqueado inmediatamente por el dispositivo de control 21b mediante un correspondiente acceso de escritura a la memoria no volátil 22, ya que un bloqueo inmediato así podría ser detectado por el atacante como un acceso de escritura extraordinario o irregular mediante un análisis de la evolución del consumo de corriente del soporte de datos 1. El dispositivo de control 21b bloquea más bien el soporte de datos 1 en el instante t_n mediante el siguiente acceso de escritura normal de los realizados de manera continua. Si no es posible efectuar un bloqueo mediante el siguiente acceso de escritura a realizar en el instante t_n, por ejemplo porque el intervalo de tiempo entre el intento de ataque detectado y el siguiente acceso de escritura normal sea demasiado pequeño para iniciar el acceso de escritura de bloqueo, el bloqueo también puede realizarse con el acceso de escritura que sigue al siguiente, en el instante t_{n+1}. Independientemente de la forma de realización concreta, el proceso de escritura que bloquea el soporte de datos 1 se realiza lo antes posible tras la detección de un intento de ataque.

Dado que, si no existiese un intento de ataque, el acceso de escritura según la forma de realización mostrada en la figura 1 se realizaría no obstante también en el instante t_n en forma de un acceso de escritura en blanco, un atacante no puede diferenciar la evolución del consumo de corriente en el tiempo (figura 1b) del soporte de datos 1 atacado, al detectarse el intento de ataque y bloquearse el soporte de datos 1 en el instante t_n, de la evolución del consumo de corriente (figura 1a) del soporte de datos 1 que tendría lugar sin el intento de ataque. Por lo tanto, el atacante no puede determinar por medio de la evolución del consumo de corriente como y cuándo el dispositivo de control 21b bloquea el soporte de datos mediante la escritura de una marca de bloqueo en la memoria 22. De este modo se enmascara o se encubre el bloqueo automático del soporte de datos 1 por parte de su dispositivo de control 21b.

En el presente ejemplo de realización, la evolución del consumo de corriente en el tiempo causada por el proceso de escritura de bloqueo tampoco puede en particular diferenciarse de la evolución del consumo de corriente en el tiempo que estaría causada por uno de los demás procesos de escritura ejecutados de manera continua. De este modo se asegura que un atacante no pueda, por medio de un análisis temporal de la evolución del consumo de corriente del soporte de datos 1 durante los accesos de escritura, diferenciar el acceso de escritura de bloqueo de los demás accesos de escritura continuos.

Para lograr la mejor coincidencia posible entre la evolución del consumo de corriente de un acceso de escritura de bloqueo y los demás procesos de escritura ejecutados de manera continua (que no provocan un bloqueo), se escribe respectivamente el mismo volumen de datos, es decir que en un acceso de escritura en blanco se escribe el mismo número de bits en la memoria 22 que en la escritura de una marca de bloqueo mediante un acceso de escritura de bloqueo.

En particular pueden escribirse los mismos datos en todos los procesos de escritura ejecutados de manera continua, es decir que los accesos de escritura que no provocan un bloqueo también escriben marcas de bloqueo en la memoria 22, que sin embargo no son activas porque, por ejemplo, no se escriben en el área de memoria prevista con este fin. De este modo se consigue, mediante todos los accesos de escritura ejecutados de manera continua, una evolución del consumo de corriente en el tiempo casi idéntica.

Sin embargo, dado que, dependiendo del tipo del intento de ataque, del proceso de aplicación que se esté ejecutando en ese instante o similar, puede elegirse cuáles de las aplicaciones o de los procesos de aplicación ejecutados o de los accesos a memoria se bloquean total o parcialmente, la marca de bloqueo puede diferir de un caso a otro. Por lo tanto, en los accesos de escritura en blanco que no provocan un bloqueo se escriben respectivamente datos que tienen únicamente una secuencia de bits similar, pero no idéntica, a la que escribe un proceso de escritura de bloqueo. Además, esta secuencia de bits a escribir por los accesos de escritura en blanco se varía de tal manera que un proceso de escritura ejecutado para bloquear el soporte de datos 1 no pueda, por medio de la evolución del consumo de corriente del soporte de datos 1 causada por la secuencia de bits escrita respectivamente, diferenciarse de los accesos de escritura en blanco que no provocan un bloqueo. Por consiguiente, con los accesos de escritura en blanco que no provocan un bloqueo del soporte de datos 1 no se escribe en particular ningún dato útil en la memoria 22, sino únicamente secuencias de bits especialmente adecuadas para el enmascaramiento y el encubrimiento de un acceso de escritura de bloqueo.

La figura 1 representa a modo de ejemplo una evolución del consumo de corriente del soporte de datos 1. En realidad, la evolución del consumo de corriente del soporte de datos 1 puede naturalmente ser más compleja que la

representada en la figura 1a, ya que ésta se ve influida también por otros componentes del soporte de datos 1 o por otros procesos ejecutados en el soporte de datos 1. Sin embargo, esto no afecta a la invención.

Al bloquear el dispositivo de control 21b el soporte de datos 1 en el instante t_n en la figura 1b, se bloquean de forma temporal o permanente las aplicaciones ejecutables, o los procesos de aplicación ejecutados, o determinados tipos de acceso a la memoria predefinidos, o el acceso a determinados datos o áreas de la memoria. En particular se bloquean las aplicaciones críticas para la seguridad o el acceso a datos contenidos en la memoria críticos para la seguridad. También se bloquean los procesos de aplicación que se estén ejecutando durante el intento de ataque en el instante t_a, ya que especialmente éstos podrían ser un objetivo del intento de ataque. Además pueden bloquearse también todas las aplicaciones, o todos los procesos de aplicación ejecutados, o todos los accesos a la memoria, si los requisitos de seguridad del soporte de datos 1 lo exigen. También dependiendo de eventuales requisitos de seguridad del soporte de datos 1, el bloqueo puede ser permanente y anulable sólo por un fabricante o una entidad emisora del soporte de datos 1 o ser temporal, es decir limitado en el tiempo hasta un instante concreto o hasta un suceso determinado, como por ejemplo el desbloqueo mediante la introducción un código o similar.

En la forma de realización mostrada en la figura 1, los intervalos de tiempo entre los instantes de escritura tienen aproximadamente la misma duración. Éste puede ser especialmente el caso si los instantes de escritura respectivos se fijan según un patrón regular predefinido. También es posible hacer depender los instantes de escritura de la ejecución de un proceso de aplicación en el soporte de datos 1. En tal caso, los instantes de escritura pueden, por ejemplo, depender de un proceso de aplicación de tal manera que se realice un acceso de escritura cada vez que el proceso de aplicación ejecute un comando, o en puntos fijos del desarrollo del programa. Los intervalos de tiempo entre estos instantes de escritura pueden también configurarse de modo que sean variables, por ejemplo si los instantes de escritura se determinan mediante un proceso aleatorio o si los instantes de escritura se establecen según un esquema fijo, que parezca lo más variable y arbitrario posible.

Tanto en el caso en que los instantes de escritura se establecen según un esquema fijo, es decir que los accesos de escritura se realizan metódicamente, como en el caso de los instantes de escritura determinados aleatoriamente, el bloqueo del soporte de datos 1 no puede reconocerse por una evolución inesperada del consumo de corriente en el tiempo causada por un acceso de escritura de bloqueo inesperado. Dado que, además, los intervalos de tiempo entre los accesos de escritura son más cortos que el lapso de tiempo mínimo necesario para un intento de ataque, un atacante no puede tampoco impedir el bloqueo automático del soporte de datos, desconectando la alimentación de corriente del soporte de datos 1 en cada uno de los accesos de escritura continuos (que en caso dado reconoce por la evolución del consumo de corriente en el tiempo).

En el caso en que los instantes de los accesos de escritura ejecutados de manera continua se determinan mediante un proceso aleatorio, existe también, según una variante de realización especial de la invención, la posibilidad de elegir, de manera selectiva, el instante en el que se realiza el acceso de escritura de bloqueo de tal manera que, por una parte, el soporte de datos 1 se bloquee, al menos parcialmente, lo antes posible tras la detección del intento de ataque y, por otra parte, se mantenga el enmascaramiento de este acceso de escritura de bloqueo por los accesos de escritura que no provocan un bloqueo realizados en instantes de escritura determinados continua y aleatoriamente. Con este fin se elige en esta variante de realización un instante para el acceso de escritura de bloqueo que pueda ser con suficiente probabilidad un resultado del proceso aleatorio y/o no guarde una relación entendible con el instante de la detección del intento de ataque.

En otra variante de la invención pueden realizarse también, en lugar de los accesos de escritura que no provocan un bloqueo, otros procesos cualesquiera que causen una evolución del consumo de corriente en el tiempo suficientemente similar a la evolución del consumo de corriente causada por el proceso de escritura de bloqueo. Por ejemplo puede activarse correspondientemente una resistencia de carga u otro componente del soporte de datos 1. Esto puede ser especialmente conveniente si la activación continua del otro componente tiene asociada una utilidad o si debido a los procesos de escritura ejecutados de manera continua se utilizan demasiados recursos del soporte de datos (por ejemplo potencia de cálculo de un procesador).

REIVINDICACIONES

1. Procedimiento sobre un soporte de datos portátil (1), que comprende una ejecución de accesos de escritura a una memoria (2) del soporte de datos (1), caracterizado por las siguientes etapas:

- ejecución continua de accesos de escritura a la memoria (2) por un dispositivo de control del soporte de datos en instantes de escritura arbitrariamente consecutivos; y

- bloqueo, al menos parcial, del soporte de datos (1) mediante uno de los accesos de escritura ejecutados de manera continua, en caso de detectar un intento de ataque al soporte de datos (1),

- siendo los accesos de escritura ejecutados de manera continua, accesos de escritura ejecutados por una aplicación existente para la funcionalidad normal y no utilizándose aquí datos adecuados o designados para utilización y

- siendo los datos una secuencia de bits a escribir que se varía de manera tal que un proceso de escritura ejecutado para bloquear el soporte de datos (1) no puede, mediante la evolución del consumo de corriente del soporte de datos (1) causada por la secuencia de bits escrita respectivamente, diferenciarse de los accesos de escritura que no provocan un bloqueo.

2. Procedimiento según la reivindicación 1, caracterizado porque en la ejecución continua de accesos de escritura se escriben datos en una memoria no volátil (22) del soporte de datos (1).

3. Procedimiento según una de las reivindicaciones 1 a 2, caracterizado porque en los accesos de escritura ejecutados de manera continua que no bloquean parcialmente el soporte de datos (1) se realizan accesos de escritura a la memoria (2) en blanco.

4. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado porque en el bloqueo, al menos parcial, del soporte de datos (1) se bloquean de forma temporal o permanente aplicaciones ejecutables y/o procesos de aplicación ejecutados.

5. Procedimiento según una de las reivindicaciones 1 a 4, caracterizado porque en el bloqueo, al menos parcial, del soporte de datos (1) se bloquean de forma temporal o permanente accesos predefinidos o todos los accesos a la memoria (2).

6. Procedimiento según una de las reivindicaciones 1 a 5, caracterizado porque el soporte de datos (1) se bloquea, al menos parcialmente, en caso de detectar un intento de ataque en forma de un ataque con luz.

7. Procedimiento según una de las reivindicaciones 1 a 6, caracterizado porque el soporte de datos (1) se bloquea, al menos parcialmente, mediante el acceso de escritura siguiente a la detección del intento de ataque.

8. Procedimiento según una de las reivindicaciones 1 a 7, caracterizado porque los accesos de escritura se realizan de manera continua en instantes de escritura consecutivos fijamente predefinidos o determinados aleatoriamente.

9. Procedimiento según la reivindicación 8, caracterizado porque los accesos de escritura se realizan en instantes de escritura dependientes de una ejecución de un proceso de aplicación en el soporte de datos (1).

10. Procedimiento según la reivindicación 9, caracterizado porque los accesos de escritura se realizan cada vez que el proceso de aplicación ejecuta un comando.

11. Soporte de datos portátil (1), que comprende un procesador, una memoria (2) y un dispositivo de detección (4) para detectar intentos de ataque al soporte de datos (1), caracterizado por un dispositivo de control del soporte de datos (21b) que está preparado para ejecutar accesos de escritura a la memoria (2) de manera continua en instantes de escritura arbitrariamente consecutivos y, en caso que el dispositivo de detección (4) detecte un intento de ataque, bloquear el soporte de datos (1), al menos parcialmente, mediante uno de los accesos de escritura ejecutados de manera continua,

- siendo los accesos de escritura ejecutados de manera continua accesos de escritura ejecutados por una aplicación existente para la funcionalidad normal y no utilizándose aquí datos adecuados o designados para utilización y

- siendo los datos una secuencia de bits a escribir que se varía de tal manera que un proceso de escritura ejecutado para bloquear el soporte de datos (1) no puede, mediante la evolución del consumo de corriente del soporte de datos (1) causada por la secuencia de bits escrita respectivamente, diferenciarse de los accesos de escritura que no provocan un bloqueo.

12. Soporte de datos (1) según la reivindicación 11, caracterizado porque el soporte de datos (1) comprende un sistema operativo (21a) que a su vez comprende el dispositivo de control (21b).

13. Soporte de datos (1) según la reivindicación 11 ó 12, caracterizado porque el dispositivo de control (21b) está configurado para llevar a cabo un procedimiento según una de las reivindicaciones 2 a 10.

14. Soporte de datos (1) según una de las reivindicaciones 11 a 13, caracterizado porque el soporte de datos portátil (1) es una tarjeta inteligente, una tarjeta de radiotelefonía móvil (U)SIM, una tarjeta multimedia segura o una tarjeta con función de pago.

FIG 1A

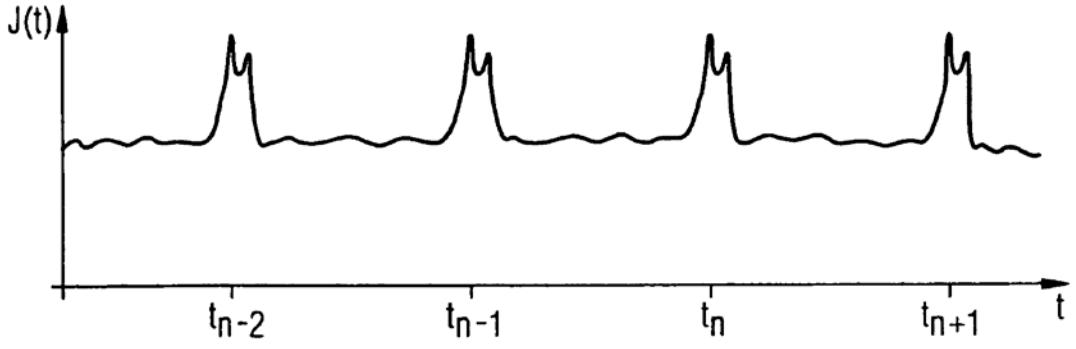


FIG 1B

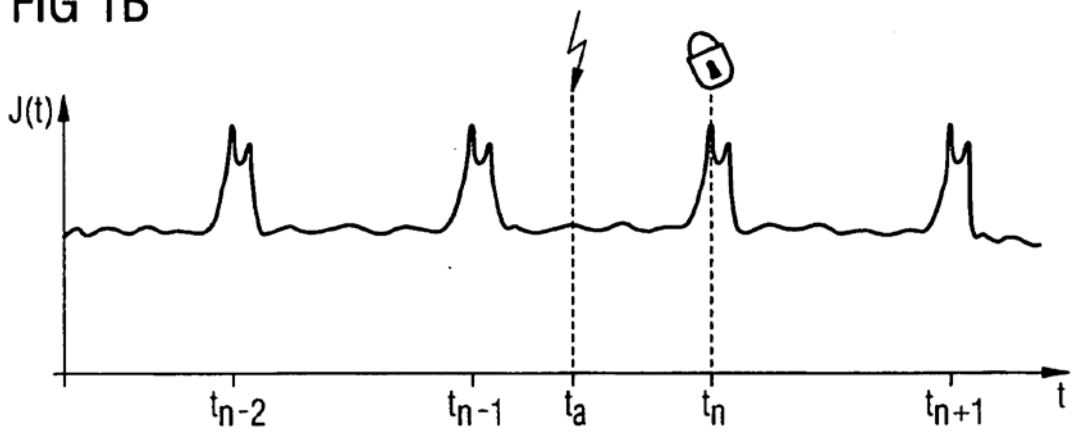
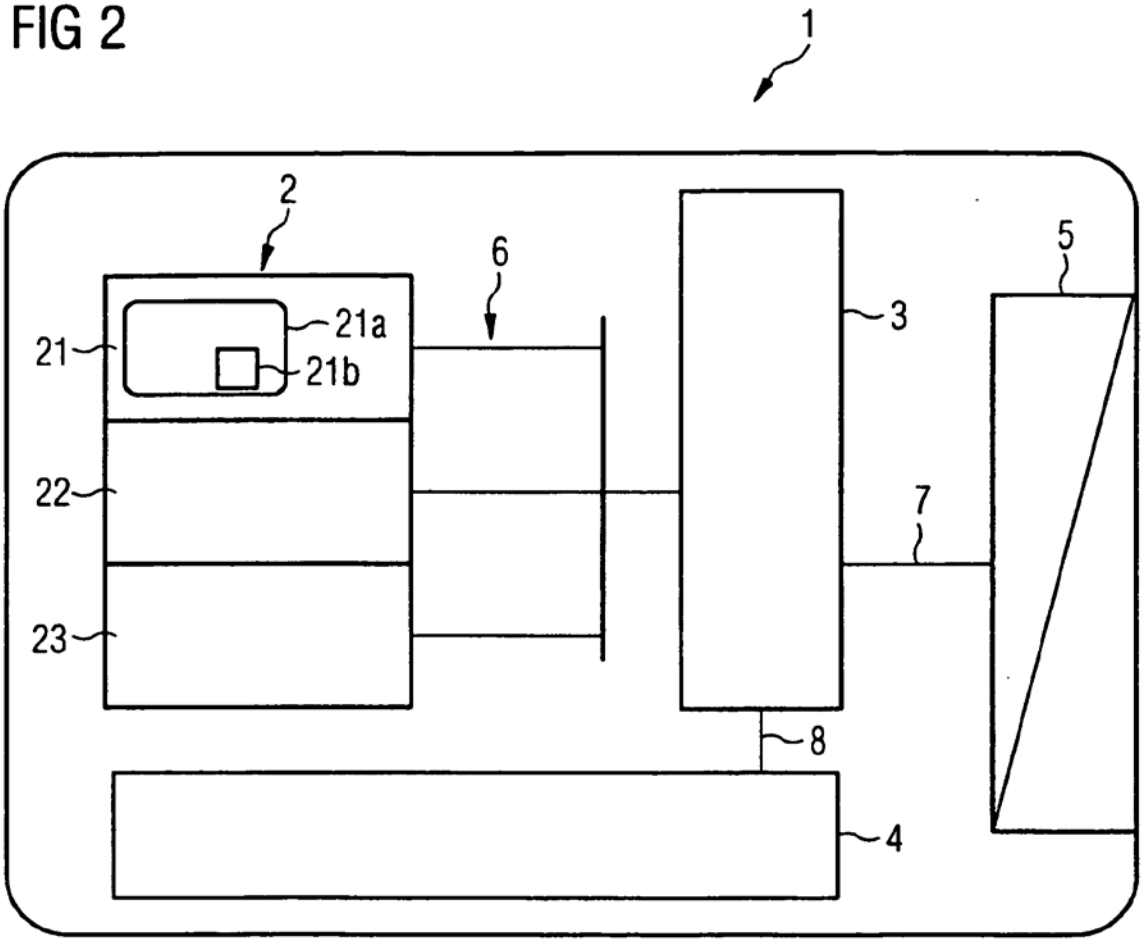


FIG 2



REFERENCIAS CITADAS EN LA DESCRIPCIÓN

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 citado en la descripción

- DE 10322671 A1 **[0004]**
- DE 10324419 A1 **[0005]**

Bibliografía de patentes citada en la descripción

- **Ravi S. et al.** Tamper resistance mechanisms for secure embedded systems. VLSI Design, 2004, 09. Januar 2004, vol. 17, 605-611 **[0006]**
- A tutorial on physical security and side-channel attacks. **Francois Koeune et al.** Foundations of security analysis and design III; lecture notes in computer science. LNCS, Springer, 01. Januar 2005, 78-108 **[0007]**