(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 548 688**

(51) Int. CI.:

G06F 21/72 (2013.01)
G06F 11/07 (2006.01)
G07F 7/08 (2006.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.12.2011 E 11801979 (3)**

(97) Fecha y número de publicación de la concesión europea: **02.09.2015 EP 2652665**

(54) Título: **Soporte de datos portátil que comprende un contador de error de control**

(30) Prioridad:

14.12.2010 DE 102010054446

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.10.2015

(73) Titular/es:

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

(72) Inventor/es:

GIBIS, OLIVER

(74) Agente/Representante:

ARPE FERNÁNDEZ, Manuel

DESCRIPCIÓN

Soporte de datos portátil que comprende un contador de error de control

[0001] La presente invención se refiere a un soporte de datos portátil con un contador de operaciones erróneas y a un procedimiento para proteger una instrucción en el soporte de datos mediante un contador de operaciones erróneas.

[0002] En relación con los soportes de datos portátiles, por ejemplo tarjetas chip, los contadores de operaciones erróneas se emplean para limitar la ejecución no autorizada de instrucciones relevantes para la seguridad con el fin de obtener datos del soporte de datos relevantes para la seguridad. Por ejemplo se conoce ya el método de limitar el número de introducciones erróneas sucesivas. Si se sobrepasa este número, el soporte de datos se bloquea. Mediante un contador de operaciones erróneas pueden detectarse también ataques de otro tipo a cualesquiera instrucciones ejecutadas en el soporte de datos. Si, por ejemplo, un cálculo realizado mediante una instrucción es perturbado por una acción externa sobre el soporte de datos con el fin de, por medio del resultado perturbado, espiar datos secretos implicados en el cálculo, esta acción puede detectarse de forma interna en el soporte de datos repitiendo el cálculo antes de emitir un resultado. La emisión de un resultado del cálculo se realiza sólo si ambos cálculos proporcionan un resultado idéntico. En caso contrario, puede partirse de un ataque a uno de los cálculos y un contador de operaciones erróneas correspondiente anota este ataque.

[0003] Sin embargo, un atacante que realice un ataque como el anteriormente descrito a una instrucción de un soporte de datos, por ejemplo robado, puede reconocer, por medio de un análisis de determinados parámetros del soporte de datos, por ejemplo por medio del consumo de corriente, si la comparación de los dos resultados del cálculo presenta igualdad o no. Con ello, el atacante tiene la posibilidad de desactivar el soporte de datos cortando la alimentación de corriente antes de que el contador de operaciones erróneas pueda anotar el ataque. De este modo, el atacante puede en cierto modo invalidar el contador de operaciones erróneas y realizar el ataque tantas veces como quiera.

[0004] Por este motivo, se ha pasado a, partiendo de un valor inicial positivo predefinido, disminuir un contador de operaciones erróneas ya antes de ejecutar la instrucción relevante para la seguridad e incrementarlo solamente si la instrucción se ha ejecutado sin interrupciones. De este modo, el contador de operaciones erróneas puede detectar con seguridad un ataque como el anteriormente descrito, dado que, en caso de cortarse la alimentación de corriente aún durante la ejecución de la instrucción, ya no se incrementa el contador. En consecuencia, en la siguiente llamada de la instrucción el valor indicado por el contador de operaciones erróneas está reducido en uno. Si se prevé que la instrucción se ejecute en el soporte de datos solamente mientras el contador de operaciones erróneas presente un valor positivo, el número de ataques a la instrucción está limitado por el valor inicial del contador de operaciones erróneas. De este modo puede impedirse con seguridad un ataque extensivo a la instrucción.

[0005] Sin embargo, este tipo de contador de operaciones erróneas también tiene desventajas. Por una parte, la disminución del contador de operaciones erróneas antes de ejecutar cada instrucción relevante para la seguridad y el subsiguiente incremento suponen una pérdida de rendimiento en todos los casos en los que no se produce ningún ataque. Por otra parte, la necesidad de efectuar repetidos accesos de escritura para la disminución y el subsiguiente incremento del contador de operaciones erróneas puede mermar la durabilidad de las áreas de memoria correspondientes del soporte de datos, proporcionadas por ejemplo por células de memoria EEPROM.

[0006] El documento DE 101 41 926 A1 revela un procedimiento previsto para la gestión de una memoria de datos, que presenta páginas de memoria con, respectivas, varias palabras de memoria, siendo necesario acceder a toda la página de memoria para escribir una palabra de memoria. El procedimiento soporta transacciones con operaciones de escritura atómicas, almacenándose imágenes de la memoria en una memoria tampón de recuperación para, en caso de una interrupción de la transacción, permitir una recuperación del contenido de la memoria con respecto a las operaciones de escritura atómicas de la transacción. Además, el procedimiento soporta operaciones de escritura no atómicas durante transacciones en curso. Al menos cuando exista en la memoria tampón de recuperación una imagen de memoria de una página de memoria afectada por la operación de escritura no atómica, se crea, sobre la base de la imagen de memoria existente, una imagen de memoria modificada de acuerdo con la operación de escritura no atómica, de manera que, en caso de recuperarse el contenido de la memoria, se mantengan en el contenido de la memoria los efectos de operaciones de escritura no atómicas realizadas con éxito. Un microcontrolador y una tarjeta chip presentan características correspondientes. Mediante la invención se pone a disposición una gestión de memoria para una memoria de datos grabable sólo página a página, que, además de operaciones de escritura atómicas, también soporta operaciones de escritura no atómicas en transacciones.

[0007] El documento CA 2 247 475 A1 revela un procedimiento para garantizar la seguridad de un módulo de seguridad, estando el módulo configurado para conectarlo a un ordenador. El fin del procedimiento es impedir que una operación segura pueda comprometerse a través de una interrupción.

[0008] El documento WO 2008/084016 A1 se refiere a un procedimiento y un circuito para la protección de datos contra un acceso no autorizado por medio de interrupciones de funcionamiento, incrementándose o disminuyéndose un contador después de cada interrupción registrada y reiniciándose el contador automáticamente después de cierto tiempo.

[0009 El objetivo de la presente invención es proponer un procedimiento para proteger un soporte de datos mediante un contador de operaciones erróneas, que pueda implementarse ahorrando recursos y cuidando los recursos.

[0010] Este objetivo se logra mediante un procedimiento y un soporte de datos con las características de las reivindicaciones independientes. En las reivindicaciones dependientes se indican configuraciones ventajosas y perfeccionamientos.

[0011] En un procedimiento según la invención en un soporte de datos portátil para proteger el soporte de datos contra ataques externos al soporte de datos se utiliza al menos un contador en el soporte de datos. Una instrucción predefinida se protege aquí de tal manera que sólo es ejecutada por el soporte de datos si el al menos un contador se halla dentro de un rango de valores admisible predefinido, en particular cuando el valor indicado por el al menos un contador no es inferior a un valor mínimo predefinido. Según la invención, el al menos un contador se acciona, por regla general se disminuye, cuando, por medio de una memoria tampón de recuperación del soporte de datos, se detecta que se ha perturbado una ejecución anterior de una instrucción.

[0012] El accionamiento del contador corresponde, como ya se ha mencionado, por ejemplo a una disminución del contador. En caso de un error reiterado se abandona entonces el rango de valores admisible hacia abajo, es decir que el valor se hace inferior a un valor mínimo predefinido. Se sobrentiende que, análogamente a la primera variante arriba mencionada, según una segunda variante el contador también puede estar configurado de tal manera que la instrucción predefinida se ejecute sólo cuando el, al menos, un contador no abandone hacia arriba el rango de valores predefinido, o sea que no sobrepase un valor máximo predefinido. Aquí, al detectarse una perturbación el, al menos, un contador se acciona incrementándolo. Con vistas a una mayor sencillez e inteligibilidad, en lo que sigue nos referiremos en la mayoría de los casos solamente a la primera de las dos variantes mencionadas, que es completamente equivalente a la segunda variante en cuanto a la funcionalidad.

[0013] Por consiguiente, un soporte de datos portátil según la invención comprende, al menos, una memoria y un procesador, que está configurado para ejecutar una instrucción almacenada en la memoria, y al menos un contador para proteger la instrucción. El soporte de datos está aquí configurado para ejecutar la instrucción predefinida sólo si el, al menos un, contador se encuentra dentro de un rango de valores predefinido. El soporte de datos está configurado para, por medio de una memoria tampón de recuperación de dicho soporte de datos, detectar si se ha perturbado una ejecución anterior de una instrucción. Además, el soporte de datos está configurado para accionar el contador cuando se haya detectado tal perturbación.

[0014] De este modo puede lograrse una protección del soporte de datos o de instrucciones individuales contra ataques mediante errores, que ahorre recursos y que cuide los recursos. Sólo en un caso de error concreto, cuando realmente haya tenido lugar un ataque, se acciona el al menos un contador, que sirve de contador de operaciones erróneas. En cambio, no se realizan accesos de escritura ya antes de cada ejecución de una instrucción a proteger; y adicionalmente después de la instrucción, si no ha tenido lugar un ataque. De este modo pueden evitarse un gran número de accesos de escritura, lo que hace posible aumentar en suma considerablemente el rendimiento del soporte de datos. Además, los recursos del soporte de datos, en particular las áreas de memoria correspondientes de una memoria no volátil, por ejemplo de una memoria EEPROM, se cuidan en el sentido de que se reduce ostensiblemente el número de accesos de escritura a estas áreas de memoria, que contienen el al menos un contador. De este modo se aumenta la vida útil de las áreas de memoria correspondientes y por lo tanto también la vida útil del soporte de datos.

[0015] Por medio de la memoria tampón de recuperación es posible, como se describe detalladamente más adelante, detectar si se ha perturbado una ejecución anterior de una instrucción. Es posible que el, al menos un, contador del soporte de datos esté configurado para contar distintas perturbaciones del soporte de datos, es decir independientemente de la instrucción específica que haya sido perturbada. Además es posible que el, al menos un, contador se accione solamente cuando, por medio de una memoria tampón de recuperación del soporte de datos, se detecte que se ha perturbado una ejecución anterior de la instrucción predefinida concreta. Es decir que, según esta forma de realización, el contador está configurado para contar solamente perturbaciones de la instrucción predefinida, con el fin de proteger la instrucción predefinida. Como se describe más adelante, en el soporte de datos pueden estar previstos simultáneamente distintos contadores. Puede haber contadores que, por medio de la memoria tampón de recuperación, detecten perturbaciones que afecten a instrucciones individuales concretas, y contadores que cuenten perturbaciones que afecten al soporte de datos como tal o al menos a una pluralidad de instrucciones.

[0016] Una perturbación de una ejecución anterior de una instrucción se detecta preferentemente por el hecho de que, antes de la ejecución actual de la instrucción predefinida, exista una entrada válida en la memoria tampón de recuperación. El significado de una entrada válida se describe más adelante con mayor detalle.

[0017] La memoria tampón de recuperación se utiliza en general para proteger un área de memoria del soporte de datos contra la incoherencia producida por un acceso de escritura perturbado al área de memoria. La memoria tampón de recuperación puede comprender entradas relativas a una pluralidad de áreas de memoria diferentes. Así pues, la memoria tampón de recuperación sirve más que nada para garantizar, de forma ya conocida, la integridad de la información almacenada en el soporte de datos.

[0018] Si se perturba un acceso de escritura a un área de memoria de una memoria del soporte de datos antes de que el acceso de escritura haya concluido con éxito, pueden producirse pérdidas de datos o incoherencias en relación con los datos a escribir o los datos previamente almacenados en el área de memoria. Para evitar esto, la memoria tampón de recuperación comprende, al menos por el tiempo que dure el acceso de escritura, el contenido original del área de memoria antes de comenzar el acceso de escritura. Por regla general, la entrada comprende información adicional, por ejemplo el tamaño de los datos almacenados temporalmente, la dirección del área de memoria en la que los datos están almacenados en la memoria, y similares. En este caso, la entrada correspondiente de la memoria tampón de recuperación se marca como "válida". La marca "válida" significa que, en caso de error, los datos actualmente almacenados de forma temporal en la entrada deben escribirse de nuevo en el área de memoria correspondientemente designada. Si el acceso de escritura a la memoria, o la instrucción que comprende este acceso de escritura, ha concluido con éxito, la entrada existente en la memoria tampón de recuperación que protege el acceso de escritura se marca como "no válida". Una entrada "no válida" ya no debe

escribirse de nuevo en la memoria, en caso de realizarse una comprobación de la memoria tampón de recuperación en este sentido, por ejemplo al activar el soporte de datos, porque el proceso de escritura correspondiente ya ha concluido con éxito antes.

[0019] Si ahora se produce un error durante el acceso de escritura, por ejemplo un corte de la alimentación de corriente del soporte de datos, al activarse de nuevo el soporte de datos puede detectarse que en la memoria tampón de recuperación existe una entrada válida. Para restablecer la integridad de la información almacenada en el soporte de datos, la entrada almacenada en la entrada de la memoria tampón de recuperación se escribe ahora en primer lugar de nuevo en el área de memoria correspondiente del soporte de datos designada en la entrada. A continuación, la entrada de la memoria tampón de recuperación se marca como no válida – es decir en particular que puede volver a utilizarse para fines de almacenamiento intermedio –, análogamente al caso de una conclusión del proceso de escritura con éxito.

[0020] Por otra parte, ahora es posible, como ya se ha descrito, detectar por medio de la memoria tampón de recuperación en general un ataque mediante errores al soporte de datos, por ejemplo en forma de un corte de la alimentación de corriente, por el hecho de que exista una entrada válida en la memoria tampón de recuperación antes de ejecutar una instrucción. Con este fin, después de activar el soporte de datos, antes de ejecutar instrucciones, se comprueba el estado de la memoria tampón de recuperación. Es decir que el soporte de datos comprueba si en la memoria tampón de recuperación hay entradas válidas. Esto significa que se ha perturbado una instrucción anterior – o más exactamente un acceso de escritura de una instrucción anterior – antes de que haya sido posible concluir por completo y con éxito la instrucción, o el acceso de escritura. Por consiguiente, esta entrada válida de la memoria tampón de recuperación indica en particular un ataque al soporte de datos. Este ataque puede entonces anotarse mediante el accionamiento del al menos un contador. En este caso, la ejecución de la instrucción se hace depender, como ya se ha descrito, de si el contador aún se halla dentro del rango de valores válido.

[0021] Como ya se ha mencionado, la memoria tampón de recuperación puede comprender entradas relativas a diferentes áreas de memoria. Estas diferentes áreas de memoria pueden a su vez asignarse a diferentes instrucciones, por ejemplo de tal manera que un acceso de escritura a un área de memoria determinada se realice a partir de una instrucción asignada a esta área de memoria. La memoria tampón de recuperación puede ahora comprobarse en el sentido de si una entrada predefinida está marcada como válida. Una validez de esta entrada predefinida corresponde entonces al caso en el que ha tenido lugar el acceso de escritura perturbado durante una ejecución de la instrucción predefinida, que se asigna a la entrada en la forma descrita. Por lo tanto, en este caso el al menos un contador se acciona solamente cuando se haya perturbado la instrucción predefinida correspondiente.

[0022] Por otra parte, como se indicó anteriormente, un contador del soporte de datos puede estar configurado de manera que cuente perturbaciones en general del soporte de datos. Un contador de este tipo se acciona cuando, tras la conexión del soporte de datos, se detecta como válida alguna entrada de la memoria tampón de recuperación, independientemente de si esta entrada está asignada a una instrucción determinada y, en caso afirmativo, de qué instrucción se trate. También son posibles las formas mixtas, es decir contadores que cuenten la perturbación de una instrucción entre una cantidad predeterminada de instrucciones y para ello dependan de una cantidad correspondiente de entradas de la memoria tampón de recuperación.

[0023] Como se ha descrito, por medio de la memoria tampón de recuperación pueden detectarse solamente perturbaciones de la ejecución de instrucciones que accedan con fines de escritura a una memoria del soporte de datos. Si, por el contrario, no se realiza ningún acceso de escritura durante la ejecución de una instrucción, entonces no se producen cambios en la memoria tampón de recuperación. Tales instrucciones pueden protegerse adicionalmente de forma ya conocida, disminuyendo el al menos un contador antes de una ejecución de la instrucción e incrementándolo solamente si la instrucción se ha ejecutado sin interrupciones. De este modo está garantizada también una protección eficaz de estas instrucciones sin acceso de escritura. Dado que la mayoría de las instrucciones relevantes para la seguridad prevén al menos un acceso de escritura a la memoria del soporte de datos – y por consiguiente pueden protegerse según la invención –, esta protección ya conocida para las instrucciones que no comprenden accesos de escritura no entra apenas en consideración en el total y si perjudica los recursos del soporte de datos es a lo sumo ligeramente.

[0024] Según una forma de realización preferida, el, al menos un, contador se ajusta también tras la entrega del soporte de datos a un usuario. Es decir que, además del primer ajuste del contador durante la fabricación del soporte de datos, existe la posibilidad de ajustar el contador de nuevo cuando el soporte de datos ya se ha puesto en servicio. En el marco de la presente invención se denomina ajuste del contador tanto a un ajuste de un valor del contador como a un ajuste de un rango de valores admisible del contador, así como de un patrón de evolución admisible del contador.

[0025] De este modo es posible permitir en todo momento a una entidad autorizada un ajuste del contador. Esto es aplicable especialmente también cuando el soporte de datos se halle ya en uso. De este modo se hace posible por una parte entregar el contador al usuario con un valor inicial muy bajo en el momento de la entrega. Así se garantiza una gran seguridad del soporte de datos y de las instrucciones ejecutables en el mismo. Esto es aplicable especialmente para el caso de que el usuario pierda el soporte de datos, por ejemplo por robo. Por otra parte se hace posible, mediante un ajuste adecuado, aumentar después de cierto tiempo de nuevo el contador, por ejemplo al valor inicial original, cuando, partiendo del valor original, ya haya disminuido debido a una operación errónea efectuada por descuido por un usuario autorizado o debido a averías técnicas. De este modo puede impedirse un bloqueo no intencionado del soporte de datos. Esto resulta oportuno si las operaciones erróneas por equivocación autorizadas y los fallos técnicos que han llevado a una disminución del contador se han ido sumando en el curso de la utilización del soporte de datos hasta alcanzar un número igual al valor inicial. Así pues, mediante el ajuste

múltiple según la invención del contador puede impedirse el bloqueo del soporte de datos. De este modo se mejoran la manejabilidad y la fiabilidad de la utilización del soporte de datos, sin limitar la seguridad.

[0026] El contador puede, en todo momento del ciclo de vida del soporte de datos, mantenerse tan bajo que un ataque de una entidad no autorizada a una instrucción predefinida sea posible sólo en un alcance sumamente limitado. Al mismo tiempo puede evitarse que el soporte de datos se bloquee por una operación errónea eventual, realizada por equivocación o por causas técnicas. Un contador disminuido por tales motivos puede ajustarse de nuevo y adecuadamente incluso después de la fabricación del soporte de datos, es decir incluso cuando el soporte de datos ya se ha entregado al usuario y en caso dado lleva cierto tiempo en servicio.

[0027] Como entidades autorizadas para realizar un ajuste del contador entran varias instancias en consideración. Tal ajuste puede por ejemplo permitirse al usuario del soporte de datos. También puede efectuar un ajuste del contador una entidad emisora del soporte de datos. Por último, este ajuste puede ser efectuado también por el soporte de datos mismo. Además pueden variar las condiciones que deben cumplirse para que la instancia en cuestión pueda efectuar un ajuste. Por regla general, un ajuste del, al menos un, contador es posible sólo después de una autenticación realizada con éxito ante el soporte de datos. Por último, por una parte puede predefinirse libremente el valor al que se ajusta el contador en el ajuste, o el rango de valores admisible, o la evolución admisible del contador. Por otra parte, los nuevos valores ajustados del contador pueden depender de especificaciones externas o de una evolución previa del valor indicado por el contador.

[0028] Según otro aspecto, que no está limitado a la forma de realización del procedimiento con contador ajustable, está prevista en el soporte de datos, como ya se ha mencionado, una pluralidad de contadores. Un primer contador se utiliza para proteger una primera instrucción y un segundo contador, distinto del primer contador, se utiliza para proteger una segunda instrucción, por regla general distinta de la primera instrucción. El número de contadores puede variar. Además es posible proteger mediante un contador una pluralidad de instrucciones. Cada uno de los contadores puede – si es ajustable – ajustarse por separado, como se describió anteriormente. De este modo es posible proteger adecuadamente diferentes instrucciones de distintas maneras.

[0029] En el caso de que el, al menos un, contador abandone el rango de valores predefinido, se desactiva el soporte de datos o al menos una instrucción protegida por el, al menos un, contador. En este caso ya no podrán realizarse más ataques al soporte de datos o a la instrucción. Los datos sensibles no pueden llegar a manos de personas no autorizadas. Dado que una desactivación por equivocación del soporte de datos o de la instrucción queda casi excluida por el hecho de que el contador se ajusta de nuevo y adecuadamente según sea necesario para compensar eventuales operaciones erróneas o dificultades técnicas, en caso de una desactivación del soporte de datos puede partirse, con una probabilidad muy grande, de un ataque al soporte de datos.

[0030] A continuación se explica la presente invención a modo de ejemplo con referencia a los dibujos adjuntos, que muestran:

- Figura 1una forma de realización preferida de un soporte de datos según la invención y
- Figura 2 etapas de una forma de realización preferida del procedimiento según la invención.

[0031] Un soporte de datos portátil 10, que aquí está representado como una tarjeta chip, comprende dos interfaces de comunicación de datos diferentes 20, 22. La primera interfaz de comunicación de datos 20, está configurada como un campo de contactos. Éste permite establecer contacto con el soporte de datos 10 mediante un lector que funcione con contacto, por ejemplo un terminal para tarjetas chip usual. La segunda interfaz de comunicación de datos 22 sirve para la comunicación de datos sin contacto y está configurada como una antena en forma de bobina. La alimentación de energía al soporte de datos 10 se realiza en el modo de funcionamiento respectivo, con contacto o sin contacto, respectivamente de manera ya conocida por medio de la interfaz de comunicación de datos 20, 22 respectiva. Existe la posibilidad de que el soporte de datos 10 comprenda adicionalmente una alimentación de energía propia, por ejemplo en forma de una batería (no mostrada). Como alternativa, el soporte de datos 10 puede estar configurado también sólo para un modo de funcionamiento, con contacto o sin contacto.

[0032] Además, el soporte de datos 10 comprende un procesador (CPU 30) y una serie de memorias 50, 60, 70.

[0033] Una memoria ROM no volátil regrabable 50 comprende un sistema operativo (OS) 52, que controla el soporte de datos 10, y aplicaciones 54, 56, que están configuradas para soportar la ejecución de instrucciones relevantes para la seguridad en el soporte de datos 10, por ejemplo en el caso de una autenticación, en el caso de un cálculo de una función criptográfica o similares. Como alternativa, el sistema operativo 52, o al menos partes del mismo, y las aplicaciones 54, 56 pueden estar almacenados también en la memoria EEPROM no volátil regrabable 60. En ésta pueden estar almacenadas aplicaciones adicionales, por ejemplo distintas aplicaciones de usuario, y contadores 62, 64 para proteger las instrucciones relevantes para la seguridad 54, 56. En la memoria 60 está prevista además una memoria tampón de recuperación 66.

[0034] La función de los contadores 62, 64 y de la memoria tampón de recuperación 66 se describe con mayor detalle más adelante y con referencia a la figura 2.

[0035] La memoria tampón de recuperación 66 sirve, de forma ya conocida, para proteger la integridad de la información almacenada en el soporte de datos 10. Para proteger un acceso de escritura a una dirección en la memoria 60, los datos que están almacenados antes del acceso de escritura en el área de memoria a escribir se almacenan de manera intermedia en una entrada 68 de la memoria tampón de recuperación 66. A continuación se realiza el acceso de escritura al área de memoria de la memoria 60. Si éste tiene éxito, es decir en particular si ha concluido sin perturbaciones ni interrupciones, puede prescindirse de nuevo de la entrada 68 en la memoria tampón de recuperación 66. Sin embargo, si se ha perturbado el acceso de escritura, por ejemplo mediante un corte de la alimentación de corriente del soporte de datos 10, la información almacenada en el soporte de datos 10 podría volverse incoherente debido a que, por ejemplo, se hubieran escrito ya en el área de memoria partes de los datos a escribir, mientras que aún quedasen en las áreas parciales todavía sin escribir partes de los datos antes

almacenados en la misma. Para subsanar tal incoherencia, se escribe de vuelta en el área de memoria la entrada 68 de la memoria tampón de recuperación 66 que contiene el juego de datos que estaba almacenado en el área de memoria antes del acceso de escritura perturbado. Esto puede realizarse por ejemplo inmediatamente después de un nuevo arranque del soporte de datos 10.

[0036] Por regla general, la memoria tampón de recuperación 66, como ya se ha mencionado, está establecida en la memoria no volátil 60 y comprende distintas entradas 68. Cada una de las entradas 68 comprende aquí por ejemplo un octeto de estado, un campo de dirección, un campo de tamaño, un campo de datos y un campo de control. El campo de estado indica si la entrada es actualmente "válida" o "no válida". Una entrada "válida" comprende datos a proteger que son objeto de un acceso de escritura a la memoria 60 del soporte de datos 10, no habiendo concluido aún completamente con éxito el acceso de escritura. Por medio de una entrada "válida" puede saberse, tras la activación del soporte de datos, que previamente se ha perturbado un acceso de escritura y aún debe escribirse de nuevo en la memoria el juego de datos correspondiente de la entrada. En cambio, una entrada "no válida" no comprende datos relevantes y por lo tanto puede utilizarse como memoria tampón. El campo de dirección sirve para registrar una dirección con referencia a la memoria 60 en la que está almacenado el juego de datos, que puede almacenarse en el campo de datos de la entrada 68 con fines de protección. El tamaño del campo de datos lo indica el campo de tamaño de la entrada 68. Por último, el campo de control puede comprender una suma de comprobación, mediante la cual se protege de nuevo el contenido de los campos arriba descritos. La memoria tampón de recuperación 66 misma puede comprender, además de las entradas 68, un campo de estado que indique, por ejemplo, si hay entradas válidas o si la memoria ya no tiene actualmente capacidad para el almacenamiento intermedio.

[0037] A continuación se describen, con referencia a la figura 2, las etapas de una forma de realización preferida de un procedimiento para proteger una instrucción contra ataques mediante errores.

[0038] Después de que el soporte de datos 10 haya sido activado y puesto en servicio de forma ya conocida, por ejemplo mediante la secuencia de instrucciones "ICC_ON/RESET [encender/reponer] -> startup [arrancar]() -> main [principal]() -> Send[enviar]ATR", el soporte de datos 10 comprueba en una etapa S1 la memoria tampón de recuperación 66.

[0039] Dentro de esta etapa se comprueba en primer lugar, en la etapa parcial TS11, si en la memoria tampón de recuperación 66 existen entradas válidas 68. Esta comprobación puede afectar por una parte al campo de estado de la memoria tampón de recuperación 66 y por otra parte a los campos de estado de las distintas entradas 68. Si en la etapa parcial TS11 se detecta una entrada válida 68, en la etapa parcial TS12 se restablece el contenido del área de memoria correspondiente de la memoria 60 en la forma antes descrita, por ejemplo mediante una función "v_RestoreRollbackBuffer[restablecer memoria tampón de recuperación]()". En otra etapa parcial TS13 se disminuye, al menos; uno de los contadores 62, 64.

[0040] La existencia de una entrada válida 68 en la memoria tampón de recuperación 66 significa que se ha perturbado o interrumpido una ejecución anterior de una instrucción del soporte de datos 10. Más exactamente, esto significa que se ha perturbado o interrumpido un acceso de escritura a la memoria 60 del soporte de datos 10 que debía llevarse a cabo dentro de una instrucción.

[0041] Como causa de tal perturbación entra en consideración un ataque al soporte de datos 10 o a una instrucción determinada del soporte de datos 10, por ejemplo un corte calculado de la alimentación de corriente del soporte de datos 10. Los contadores 62, 64 están configurados para contar tales ataques. Una instrucción del soporte de datos 10 se ejecuta solamente cuando el contador 62, 64 asignado a la instrucción se halla dentro de un rango de valores predefinido, o sea por ejemplo cuando no es negativo. De este modo se impide a un atacante atacar demasiadas veces una instrucción. Cada vez que se detecta un ataque a la instrucción se disminuye correspondientemente el contador 62, 64 asignado a la instrucción, como ya se ha descrito.

[0042] La validez de una entrada 68 de la memoria tampón de recuperación 66 puede significar por ejemplo que se ha perturbado un acceso de escritura de una instrucción determinada asignada a esta entrada. Esta asignación puede efectuarse haciendo que la instrucción correspondiente comprenda un acceso de escritura que siempre se realice a una dirección predefinida en la memoria 60. Esta dirección está almacenada entonces en el campo de dirección de la entrada 68. En este caso se disminuirá correspondientemente en la etapa parcial TS13 estrictamente el contador 62, 64 asignado a esta instrucción.

[0043] Por otra parte, el soporte de datos 10 puede comprender por ejemplo un contador 62, 64 destinado a registrar todos los ataques al soporte de datos 10. Un contador de este tipo siempre se disminuye en la etapa parcial TS13, independientemente de cuál de las entradas 68 del soporte de datos 10 esté marcada como "válida". La existencia de un ataque al soporte de datos 10 puede detectarse también ya por una entrada de estado "válida" de la memoria tampón de recuperación 66.

[0044] Una vez concluida la comprobación de la memoria tampón de recuperación 66 en la etapa S1, se transmite al intérprete de instrucciones una instrucción recibida, que se ejecuta en éste en la etapa S2.

[0045] Dentro de este etapa se comprueba en un primer etapa parcial TS21, como se describe más arriba, si el contador 62, 64 asignado a la instrucción se halla dentro de un rango de valores admisible, o sea en este caso por ejemplo que no sea negativo.

[0046] Si el contador 62, 64 es negativo, significa que ya se ha sobrepasado el número admisible de ataques o ejecuciones perturbadas de la instrucción. Por lo tanto, en la etapa TS22 se bloquea el soporte de datos 10 con el fin de proteger datos relevantes para la seguridad que se hallen en el mismo. De este modo ya no es posible realizar más ataques al soporte de datos 10 con el peligro de que puedan espiarse datos sensibles. Como alternativa, también es posible que, en lugar del soporte de datos 10, se bloquee solamente la instrucción correspondiente y por lo demás el soporte de datos 10 siga estando listo para el servicio.

[0047] Si, por el contrario, el contador 62, 64 se halla aún dentro del rango de valores predefinido, se ejecuta la instrucción en la etapa parcial TS23. Aquí pueden realizarse distintos accesos de escritura a la memoria 60 del soporte de datos 10, por ejemplo en la etapa parcial TS24 con respecto a los datos X o en la etapa parcial TS25 con respecto a los datos Y. Estos accesos de escritura se protegen, como se describe se describió anteriormente, mediante la memoria tampón de recuperación 66. Es decir que cada uno de estos accesos de escritura genera temporalmente una entrada válida 68 en la memoria tampón de recuperación 66.

[0048] Una vez concluida con éxito la instrucción, la memoria tampón de recuperación 66 se declara de nuevo no válida en la etapa S3, es decir que se marcan como "no válidas" los campos de estado correspondientes de las entradas 68 que de manera temporal se habían marcado como "válidas". Esto puede realizarse por ejemplo mediante una instrucción "Invalidate_RollbackBuffer [invalidar memoria tampón de recuperación]".

[0049] Tal declaración de "no válidas" relativa a las entradas 68 de la memoria tampón de recuperación 66 puede afectar a todas las entradas 68 actualmente válidas, o sea aplicarse de manera global a toda la memoria tampón de recuperación 66. Sin embargo, también puede ser conveniente marcar individualmente ciertas entradas "válidas" de nuevo como "no válidas" en cuanto haya concluido con éxito el acceso de escritura protegido correspondiente. Tal declaración de "no válidas" puede tener lugar también ya durante la ejecución de una instrucción TS23. Esto es aplicable particularmente con respecto a un acceso de escritura que afecte a un objeto de datos especial. Un objeto de datos de este tipo, por ejemplo un, así llamado, "Application Transaction Counter [contador de transacción de aplicación]", ATC, o un "PIN Try Counter [contador de intento de PIN", PTC, debe ponerse de forma obligatoria inmediatamente después de una escritura con éxito en el sistema de archivos del soporte de datos. Es decir que en el desarrollo posterior de la ejecución de la instrucción aún en curso se aplica ya el nuevo valor escrito del objeto de datos.

[0050] En cualquier caso se detecta un ataque a una instrucción que se realice mientras el acceso de escritura aún no ha concluido por completo. De este modo se garantiza la integridad de los datos y es posible mantener bajo el número de ataques mediante el contador 62, 64 correspondiente. Por consiguiente, los datos relevantes para la seguridad que se hallen en el soporte de datos 10 están protegidos eficazmente tanto contra un espionaje como contra una destrucción en el soporte de datos 10.

[0051]En ocasiones puede ocurrir que la ejecución de una instrucción no se haya interrumpido debido a un ataque, sino debido a un error técnico corriente, por ejemplo porque el soporte de datos 10 en funcionamiento sin contacto se haya alejado demasiado del lector. También son posibles otras perturbaciones.

[0052] Para impedir un bloqueo no intencionado del soporte de datos 10, que se deba a que tales perturbaciones del soporte de datos 10 se interpreten como ataques en la forma descrita – con una disminución correspondiente de los contadores afectados –, sería posible ajustar en la fabricación del soporte de datos 10 un valor inicial correspondientemente alto del contador 62, 64, a partir del cual se realiza la disminución en la etapa parcial TS13. Sin embargo, esto daría a un atacante la posibilidad de iniciar un número correspondientemente alto de ataques al soporte de datos 10, antes de que se desactive este último; y con cada ataque aumenta la probabilidad de extraer datos sensibles del soporte de datos 10. Si el valor inicial se ajusta muy bajo durante la fabricación del soporte de datos, éste se encuentra muy bien protegido contra ataques desde el exterior. Sin embargo, un número correspondientemente bajo de operaciones erróneas involuntarias o de fallos técnicos puede tener como consecuencia una desconexión no intencionada del soporte de datos 10.

[0053] Por este motivo, el soporte de datos 10 está configurado adicionalmente de tal manera que los contadores 62, 64 puedan ajustarse de nuevo repetidas veces, incluso después de la entrega del soporte de datos 10 a un usuario. Esto es aplicable tanto para el valor de los contadores 62, 64 mismos, como para los rangos de valores dentro de los cuales pueden moverse los contadores 62, 64 durante intervalos de tiempo predefinidos o definibles también durante el ajuste de los contadores 62, 64. La autorización para el ajuste de los contadores 62, 64 puede concederse tanto a un usuario como a una entidad emisora del soporte de datos 10. Para ello, por regla general es necesario, en cada caso una autenticación ante el soporte de datos 10. Por último, el ajuste puede ser realizado también por el soporte de datos 10 mismo, por ejemplo en función de una evolución de los contadores 62, 64 en el pasado. Además es posible que hayan de darse simultáneamente varias de las condiciones mencionadas para que pueda realizarse un ajuste de los contadores 62, 64.

[0054] Los distintos contadores 62, 64 pueden ajustarse respectivamente por separado. Un ajuste de uno de los contadores 62, 64 es independiente del ajuste del otro contador 62, 64. De este modo pueden protegerse de manera específica distintas instrucciones. Si, por ejemplo, el contador 62 protege una instrucción que se ejecuta en el modo de funcionamiento sin contacto, es conveniente ajustar este contador 62 más alto, en lo que se refiere al valor inicial, que el contador 64, que protege una instrucción correspondiente que se ejecuta en el modo de funcionamiento con contacto. En el contexto del modo de funcionamiento sin contacto pueden esperarse más cortes involuntarios de la alimentación de corriente que en el modo de funcionamiento con contacto.

[0055] Un usuario del soporte de datos 10 puede llevar a cabo un ajuste de los contadores 62, 64 si se autentica con éxito ante el soporte de datos 10. Esto puede realizarse, por ejemplo, mediante la introducción de un dato secreto, por ejemplo un PIN. Para la introducción de tal dato secreto, el soporte de datos 10 puede presentar un dispositivo de entrada (no mostrado), por ejemplo un teclado. También es posible, para la introducción de tales datos en el soporte de datos 10, conectar este último mediante una de las interfaces 20, 22 a un lector adecuado con dispositivo de entrada, por ejemplo un terminal para tarjetas chip. Existe la posibilidad de que el usuario pueda realizar entonces él mismo los ajustes en relación con el contador 62, 64. Como alternativa también es posible que, en cuanto se produzca una autenticación con éxito del usuario, el soporte de datos 10 reponga el ajuste de los contadores 62, 64 a valores internamente predefinidos.

[0056] El ajuste de los contadores 62, 64 puede ser llevado a cabo también por una entidad emisora del soporte de datos 10, por ejemplo un banco. Para ello debe conectarse el soporte de datos 10 a esta entidad. Esto puede realizarse por ejemplo mediante un lector adecuado, que a su vez esté conectado a la entidad emisora, por ejemplo por Internet. Para obtener una autorización para el ajuste de los contadores 62, 64, la entidad emisora puede autenticarse ante el soporte de datos 10 de forma ya conocida. Después es posible un ajuste de los contadores 62, 64 según las especificaciones de la entidad emisora. También en este caso, el ajuste del contador puede ser efectuado por el soporte de datos 10 mismo después de una autenticación con éxito de la entidad emisora. El soporte de datos 10 puede prever esto por ejemplo en cada caso después de transcurrir un intervalo de tiempo predefinido. El soporte de datos 10 puede saber que ha transcurrido el intervalo de tiempo por medio de un dispositivo cronométrico interno o por medio de un crono-fechador certificado obtenido de la entidad emisora.

REIVINDICACIONES

1. Procedimiento en un soporte de datos portátil (10), en el que el soporte de datos (10) ejecuta una instrucción predefinida (54; 56) sólo si, al menos un, contador (62; 64) del soporte de datos se halla dentro de un rango de valores predefinido (S2), **caracterizado porque** el, al menos un, contador (54; 56) se acciona (TS13) si, por medio de una memoria tampón de recuperación (66) del soporte de datos (10), se detecta (TS11) que se ha perturbado una ejecución anterior de una instrucción (54; 56).

2. Procedimiento según la reivindicación 1, **caracterizado porque** el, al menos un, contador (54; 56) se acciona si, por medio de la memoria tampón de recuperación (66) del soporte de datos (10), se detecta que se ha perturbado una ejecución anterior de la instrucción predefinida.

3. Procedimiento según la reivindicación 1 o 2, **caracterizado porque** una perturbación de una ejecución anterior de una instrucción (54; 56) se detecta por el hecho de que, antes de la ejecución actual de la instrucción predefinida (54; 56), exista una entrada válida (68) en la memoria tampón de recuperación (66).

4. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado porque** la memoria tampón de recuperación (66) se utiliza para proteger un área de memoria del soporte de datos (10) contra una incoherencia causada por un acceso de escritura perturbado a dicho área de memoria.

5. Procedimiento según la reivindicación 4, **caracterizado porque** el acceso de escritura tiene lugar durante una ejecución de la instrucción predefinida (54; 56).

6. Procedimiento según una de las reivindicaciones 1 a 5, **caracterizado porque** el, al menos un, contador (62; 64) se ajusta tras una entrega del soporte de datos (10) a un usuario.

7. Procedimiento según la reivindicación 6, **caracterizado porque** el, al menos un, contador (62; 64) se ajusta tras una autenticación con éxito ante el soporte de datos (10).

8. Procedimiento según una de las reivindicaciones 1 a 7, **caracterizado porque** está previsto más de un contador (62; 64), utilizándose un primer contador (62) para proteger una primera instrucción (54) y un segundo contador (64) para proteger una segunda instrucción (56).

9. Procedimiento según una de las reivindicaciones 1 a 8, **caracterizado porque** el, al menos un, contador (62; 64) se utiliza para proteger una pluralidad de instrucciones (54; 56).

10. Procedimiento según una de las reivindicaciones 1 a 9, **caracterizado porque** el soporte de datos (10), o al menos una instrucción (54; 56) protegida por el, al menos un, contador (62; 64), se desactiva (TS22) cuando el, al menos un, contador (62; 64) abandona el rango de valores predefinido.

11. Soporte de datos portátil (10), que comprende, al menos, una memoria (50; 60; 70) y un procesador (30), configurado para ejecutar una instrucción (54; 56) almacenada en dicha memoria (50; 60; 70), y al menos, un contador (62; 64) para proteger la instrucción (54; 56), estando el soporte de datos (10) configurado para ejecutar la instrucción (54; 56) sólo si el, al menos un contador (62; 64) se encuentra dentro de un rango de valores predefinido, **caracterizado porque** dicho soporte de datos (10) está configurado para, por medio de una memoria tampón de recuperación (66) de dicho soporte de datos (10), detectar si se ha perturbado una ejecución anterior de una instrucción (54; 56) y está configurado además para accionar el contador (62; 64) si se ha detectado tal perturbación.

12. Soporte de datos según la reivindicación 11, **caracterizado porque** el al menos un contador (62; 64) está configurado para ser ajustable después de una entrega del soporte de datos (10) a un usuario.

13. Soporte de datos (10) según la reivindicación 11 o 12, **caracterizado porque** el soporte de datos (10) está configurado para llevar a cabo un procedimiento según una de las reivindicaciones 1 a 10.

FIG 1

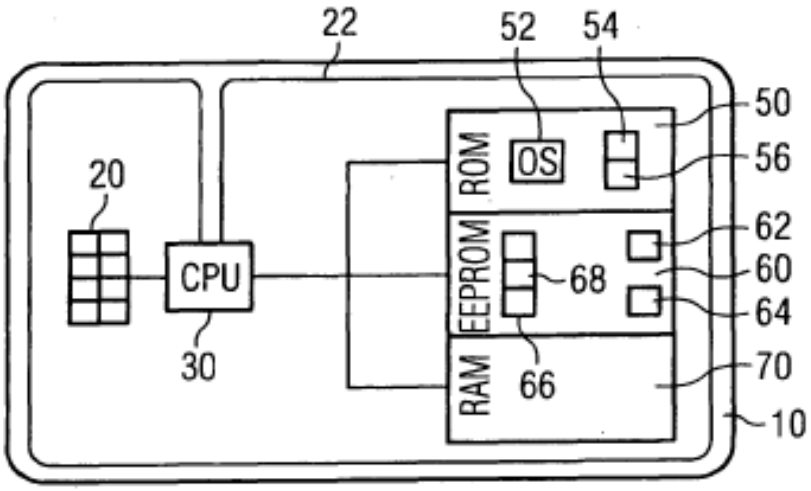
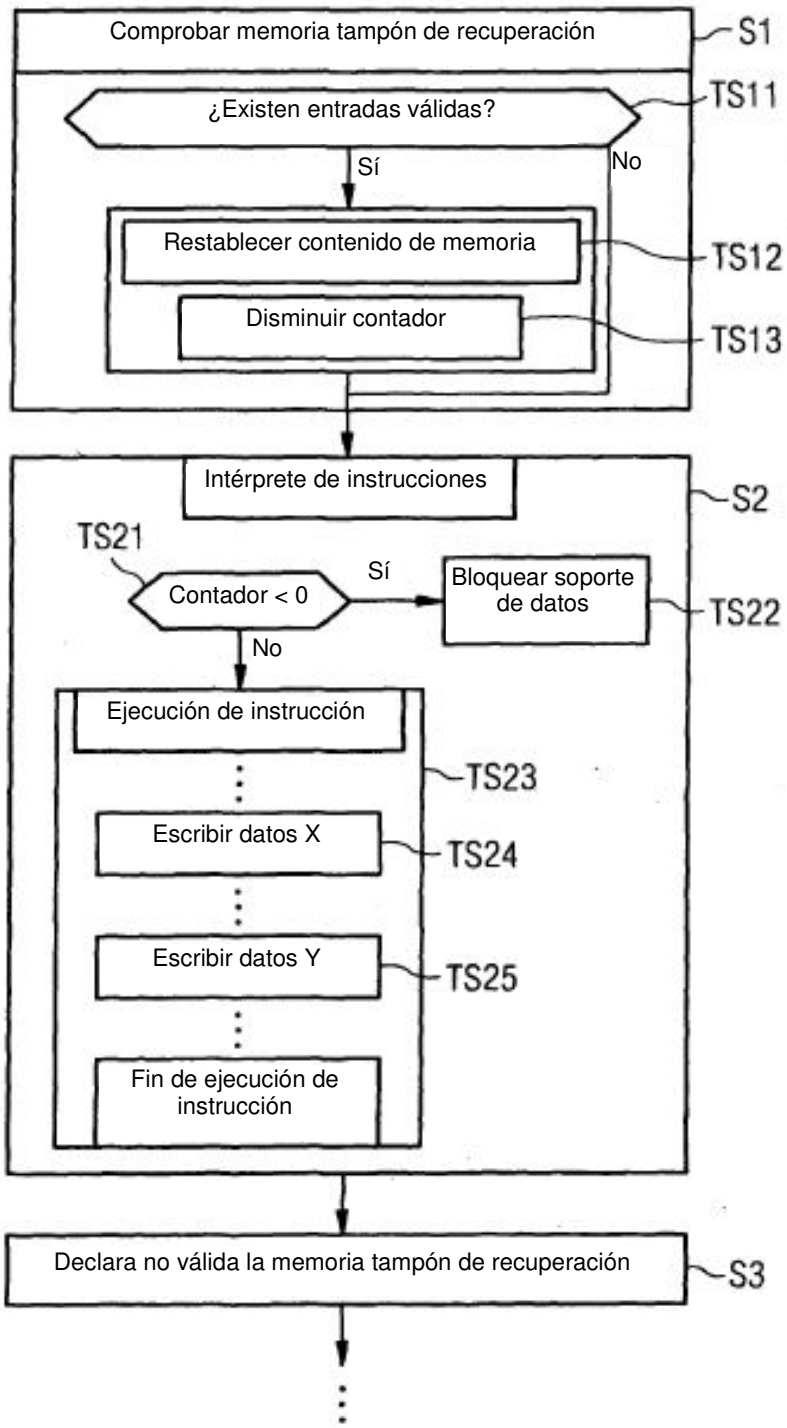


FIG 2


Comprobar memoria tampón de recuperación
S1
¿Existen entradas válidas?
TS11
Sí
No
Restablecer contenido de memoria
TS12
Disminuir contador
TS13
Intérprete de instrucciones
S2
TS21
Contador < 0
Sí
Bloquear soporte de datos
TS22
No
Ejecución de instrucción
TS23
Escribir datos X
TS24
Escribir datos Y
TS25
Fin de ejecución de instrucción
Declara no válida la memoria tampón de recuperación
S3

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 citados en la descripción

- DE 10141926 A1 **[0006]**
- CA 2247475 A1 **[0007]**
- WO 2008084016 A1 **[0008]**