(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 390 638**

(51) Int. CI.:
G06K 19/073 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09169345 .7**
(96) Fecha de presentación: **03.09.2009**
(97) Número de publicación de la solicitud: **2164031**
(97) Fecha de publicación de la solicitud: **17.03.2010**

(54) Título: **Procedimiento y dispositivo de protección de un microcircuito contra ataques**

(30) Prioridad:
11.09.2008 FR 0856116

(45) Fecha de publicación de la mención BOPI:
14.11.2012

(45) Fecha de la publicación del folleto de la patente:
14.11.2012

(73) Titular/es:
OBERTHUR TECHNOLOGIES (100.0%)
50, QUAI MICHELET
92300 LEVALLOIS-PERRET, FR

(72) Inventor/es:
THIEBAULD DE LA CROUÉE, HUGUES y
CHAMLEY, OLIVIER

(74) Agente/Representante:
PÉREZ BARQUÍN, Eliana

DESCRIPCIÓN

Procedimiento y dispositivo de protección de un microcircuito contra ataques

La presente invención se refiere a un procedimiento y a un dispositivo de protección de un microcircuito contra ataques. Se aplica, en particular, a la protección de tarjetas con chips contra los ataques con análisis del consumo eléctrico ("side channel attacks with power analysis").

El documento FR 2878633 A describe un procedimiento y dispositivo de ese tipo.

Para proteger los datos y los programas que éstos conservan, las tarjetas con microprocesador pueden implementar un banderín de destrucción ("kill-card flag"). Cuando la tarjeta detecta un evento que considera que es un ataque, pone irreversiblemente este banderín en un valor dado y este banderín con este valor impide el funcionamiento posterior del microprocesador. Este banderín se conserva en la memoria no volátil y poner el banderín en el valor dado implica efectuar una escritura en la memoria no volátil (mediante la ejecución de una función denominada "Killcard").

Unos ataques sofisticados se basan en el análisis de la ejecución con el fin de detectar la ejecución de una función de protección, o contramedida, lanzada por un microcircuito, con el fin de perturbar la ejecución de esta función de protección mediante una acción física sobre el microcircuito (mediante perturbación de la frecuencia de reloj suministrada al microcircuito, mediante láser sobre una zona del circuito, etc.) o de impedir la ejecución de esta función de protección (mediante el corte de la alimentación al microcircuito, por ejemplo). De ese modo, la detección de la ejecución de la función de protección es una condición previa a su perturbación o a su inhibición. Esto permite al atacante llevar adelante así su ataque convirtiendo en inoperativa a la función de protección o debilitándola.

Ciertos de estos ataques sofisticados utilizan unas técnicas de análisis de consumo para determinar el funcionamiento del microprocesador. En particular, las operaciones de escritura en memoria no volátil implican un consumo eléctrico muy superior a las operaciones aritméticas en memoria activa. El análisis del consumo utiliza de ese modo el hecho de que las diferentes operaciones consumen diferentes cantidades de electricidad. Estas diferentes operaciones presentan de ese modo diferentes firmas en términos del consumo eléctrico. El hecho de que una operación de escritura en memoria no volátil sea muy distinta, porque es muy consumidora de electricidad, permite en el ataque evitar que el banderín tome efectivamente el valor dado que prohíbe la utilización posterior del microprocesador. Desde que la firma de esta escritura se detecta por el ataque, la alimentación del microprocesador se corta y la operación de escritura no se finaliza.

La presente invención viene a remediar estos inconvenientes.

Con este fin, de acuerdo con un primer aspecto, la presente invención presenta un procedimiento de protección del microcircuito contra un ataque, caracterizado porque comprende:

- una etapa de determinación de si se detecta un ataque,

- si se detecta un ataque, una etapa de realización de una función de protección, y

- si no se detecta ningún ataque, una etapa de realización de una función de señuelo que simula la función de protección para que sea perceptible, desde el exterior de dicho microcircuito, de una forma sensiblemente idéntica a la función de protección.

De ese modo, un atacante no puede determinar si su ataque ha sido detectado percibiendo la realización de la función de protección puesto que incluso si el ataque no ha sido detectado, la función de señuelo simula la realización de la función de protección.

Se observa que la simulación de la función de protección por la función de señuelo se ejecuta preferiblemente hasta un instante en el que ya no es posible para un atacante beneficiarse de la detección de la ejecución de la función de protección para llevar adelante su ataque. De ese modo, preferiblemente, la función de señuelo tiene una duración superior o igual a la de la función de protección o a la tomada por la función de protección para impedir el funcionamiento normal del microcircuito, pudiendo ser perceptible la función de señuelo a continuación de esta duración sin que esto impida la protección del microcircuito.

Se observa que la magnitud física perceptible en el exterior del microcircuito y modulada por la función de protección y por la función de señuelo puede ser una radiación o un campo electromagnético, una resistencia, una capacidad, una inductancia, un voltaje, un amperaje o un consumo eléctrico, por ejemplo.

De acuerdo con las características particulares, a continuación de la etapa de determinación de si se ha detectado un ataque, la función de protección no se ejecuta si la función de señuelo se ha ejecutado.

De acuerdo con las características particulares, la función de señuelo representa un consumo eléctrico sensiblemente idéntico al de la función de protección.

De ese modo, en el caso de que el consumo eléctrico provocado por la realización de la función de protección sea perceptible desde el exterior del microcircuito, se prevé, en el curso del funcionamiento normal del microcircuito, realizar una función de señuelo que presente la misma firma, en términos de consumo eléctrico. El atacante no puede por lo tanto distinguir ya, en base al consumo eléctrico del microcircuito, la ejecución de la función de protección y el funcionamiento normal del microcircuito.

Como se ha mencionado más arriba, en el caso en que el atacante detenga la alimentación del microcircuito cada vez que se desencadena la función de señuelo, no puede analizar el funcionamiento del microcircuito. El ataque se convierte por lo tanto en ineficaz y el microcircuito se protege contra este tipo de ataque. Se observa que, en este tipo de ataque, si el atacante no corta la alimentación eléctrica cuando detecta el consumo eléctrico de la función de señuelo, con el fin de proseguir la observación del funcionamiento del microcircuito después de la realización de una función de señuelo, dejará necesariamente que se ejecute la función de protección cuando su ataque haya sido detectado.

De acuerdo con unas características particulares, la función de protección es una función de colocación en fuera de servicio del microcircuito, preferiblemente mediante la escritura de un dato en la memoria no volátil. Por ejemplo, la función de protección es una función “Killcard” expuesta anteriormente.

De acuerdo con unas características particulares, la función de protección efectúa una etapa de escritura de un dato predeterminado en una primera dirección de una memoria no volátil.

De ese modo, previendo, en el funcionamiento normal del microcircuito, incluso en ausencia de detección de un ataque, la realización de la función de señuelo que presenta la misma firma en términos de consumo eléctrico que la función “Killcard”, se convierte el ataque en ineficaz.

De acuerdo con unas características particulares, la función de señuelo efectúa una etapa de escritura en memoria no volátil en una segunda dirección diferente de la primera dirección.

De acuerdo con unas características particulares, en el curso de la etapa de escritura en la segunda dirección por la función de señuelo, se escribe un mismo número de informaciones binarias que en el curso de la escritura en la primera dirección por la función de protección, y se pone en práctica el mismo algoritmo de escritura que durante la escritura en la primera dirección por la función de protección.

De acuerdo con unas características particulares, en el curso de la etapa de escritura en la segunda dirección por la función de señuelo, se escribe dicho dato predeterminado en dicha segunda dirección.

De acuerdo con unas características particulares, en el curso de la etapa de realización de la función de señuelo, se efectúa una escritura en la memoria no volátil, en la primera dirección, de un dato diferente a dicho dato predeterminado.

Cada una de estas características particulares refuerza la similitud de las firmas de la función de protección y de la función de señuelo, en términos de consumo eléctrico.

De acuerdo con unas características particulares, dichas etapas de escritura en memoria no volátil implementan un algoritmo diferente al de otras etapas de escritura en memoria no volátil efectuadas durante el funcionamiento normal del microcircuito.

Se observa que el algoritmo puede ser diferente de manera lógica o material, aplicándose este último caso cuando las células de la memoria son de naturaleza diferente.

De acuerdo con unas características particulares, en el curso de al menos una parte de dichas etapas de escritura en la memoria no volátil, no se pone en práctica el dato de verificación. Principalmente, no se implementa la suma de verificación (en inglés “checksum”).

De acuerdo con unas características particulares, en el curso de al menos una parte de dichas etapas de escritura en memoria no volátil, no se pone en práctica la relectura del dato escrito.

De acuerdo con unas características particulares, en el curso de al menos una parte de dichas etapas de escritura en memoria no volátil, no se pone en práctica el borrado de la zona de escritura (“erase”).

Gracias a cada una de estas disposiciones, se aceleran las etapas de escritura y se reduce por lo tanto el riesgo de que el ataque tenga tiempo de cortar la alimentación antes del fin de la función “killcard”, sin que, por lo tanto, las firmas de las diferentes funciones sean diferentes. Además, se acelera el funcionamiento del microcircuito puesto

que la duración de la realización de ciertas funciones de escritura se reduce. Finalmente, se reduce el uso de las células de memoria afectadas por la función de señuelo reduciendo el número de ciclos de escritura/lectura.

De acuerdo con unas características particulares, si la rescritura de datos, en la memoria no volátil es perceptible, desde el exterior de dicho microcircuito, de manera idéntica a la escritura inicial de dichos datos, la función de señuelo no incluye el borrado de la zona de escritura. En efecto, en este caso, la función de protección, que impone una escritura, y la función de señuelo que, excepto en su primera iteración, puede incluir unas rescrituras idénticas, puede tener la misma firma sin la fase preliminar denominada “erase”.

De acuerdo con unas características particulares, dicho borrado de la zona de escritura se sustituye, en cada etapa de escritura en la que está ausente, por un borrado parcial de la zona de escritura.

Por ejemplo, se realiza un borrado parcial de ese tipo efectuando una descarga (o carga según las arquitecturas de la memoria) de las cargas de cada célula de memoria afectada por la escritura durante una duración inferior a la que permite una descarga (o carga) completa de la célula de memoria.

De acuerdo con unas características particulares, la función de protección pone en práctica dicha etapa de borrado de la zona de escritura. Gracias a estas disposiciones, se acelera el funcionamiento del microcircuito, puesto que la función de señuelo no realiza siempre el borrado de la zona de escritura mientras se garantiza la buena escritura por la función de protección, durante la detección de un ataque.

De acuerdo con unas características particulares, una parte de las ejecuciones de la función de señuelo comprenden dicha etapa de borrado de la zona de escritura. Estas características se aplican, particularmente, en el caso en que las firmas de la escritura y de la rescritura no sean idénticas y en donde la función de protección incluye la fase preliminar de borrado de las células en las que se va a efectuar la escritura.

De acuerdo con unas características particulares, la función de protección efectúa una etapa de cifrado de al menos un dato sensible.

De acuerdo con unas características particulares, la función de señuelo no tiene otra función más que la de simular la función de protección.

La función de señuelo no es de ese modo funcional y no influye en el funcionamiento del microcircuito aparte de su fase de ejecución. Por ejemplo, la función de señuelo efectúa la escritura de datos que no son leídos jamás o el cifrado de al menos un dato inútil en el funcionamiento del microcircuito. Gracias a estas disposiciones, se puede prever una función de señuelo más rápida, por ejemplo una escritura más rápida, por ejemplo, sin etapa de borrado y/o sin etapa de verificación del dato escrito, que si la función de señuelo fuera útil en el funcionamiento del microcircuito.

De acuerdo con un segundo aspecto, la presente invención prevé un dispositivo de protección de un microcircuito contra un ataque, caracterizado porque comprende:

• un medio de determinación de si se ha detectado un ataque y

• un medio de control adaptado:

- si se detecta un ataque, para realizar una función de protección y

- si no se detecta ningún ataque, una etapa de realización de una función de señuelo que simula la función de protección que sea perceptible, desde el exterior de dicho microcircuito, de manera sensiblemente idéntica a la función de protección.

De acuerdo con un tercer aspecto, la presente invención prevé una entidad electrónica de chips o portátil que incluye el dispositivo objeto de la presente invención, tal como se ha expuesto sucintamente anteriormente.

Por ejemplo, esta entidad electrónica es tal como un PDA (acrónimo de “personal digital assistant” por asistente personal digital), una llave USB (acrónimo de “universal serial bus” por bus serie universal), una tarjeta de memoria, un teléfono móvil, un pasaporte electrónico o una tarjeta de chips (es decir de acuerdo con la norma ISO 7816 y asegurada, por ejemplo certificada de conformidad con los criterios comunes).

Siendo las ventajas, objetivos y características particulares de este dispositivo y de esta entidad, similares a los del procedimiento objeto de la presente invención, tal como se ha expuesto sucintamente con anterioridad, no se recuerdan aquí.

Otras ventajas, objetivos y características de la presente invención surgirán con la descripción que seguirá a continuación, en un sentido explicativo y de ningún modo limitativo, en relación con los dibujos adjuntos, en los que:

- la figura 1 representa, esquemáticamente, un modo de realización particular del dispositivo objeto de la presente invención,

- la figura 2 representa, en la forma de un diagrama lógico, unas etapas implementadas en un primer modo de realización particular del procedimiento objeto de la presente invención,

- la figura 3 representa, en la forma de un diagrama lógico, unas etapas implementadas en una etapa de escritura normal de una memoria no volátil,

- la figura 4 representa, en la forma de un diagrama lógico, unas etapas implementadas en una variante preferente del modo de realización del procedimiento objeto de la presente invención, y

- la figura 5 representa, en la forma de un diagrama lógico, unas etapas implementadas en un segundo modo de realización particular del procedimiento objeto de la presente invención.

En la descripción que sigue a continuación, se ha considerado, a modo de ejemplo, que la magnitud física perceptible desde el exterior del microcircuito es el consumo eléctrico, debido al hecho de que los ataques actualmente conocidos la conciernen. No obstante la presente invención no se limita a este tipo de magnitud física modulada durante la detección de un ataque sino que se extiende, por el contrario, a todas las magnitudes físicas moduladas perceptibles en el exterior del microcircuito, o en contacto con el microcircuito o con unos enlaces ligados a él o a distancia.

De ese modo, una magnitud física modulada afectada por la presente invención puede ser una radiación o un campo electromagnético, una resistencia, una capacidad, una inducción, un voltaje, un amperaje o un consumo eléctrico, por ejemplo.

Si se detecta un ataque, se realiza una función de protección del microcircuito modulando, en consecuencia, al menos una magnitud física predeterminada perceptible en el exterior de dicho microcircuito. De acuerdo con la presente invención, en el curso del funcionamiento normal del microcircuito, se realiza una función de señuelo que simula la función de protección modulando cada dicha magnitud física predeterminada perceptible desde el exterior de dicho microcircuito de manera sensiblemente idéntica a la función de protección. Esta simulación de la función de protección por la función de señuelo se ejecuta preferiblemente hasta un instante en el que ya no es posible para un atacante beneficiarse de la detección de la ejecución de la función de protección para llevar adelante su ataque. De ese modo, preferiblemente, la función de señuelo tiene una duración superior o igual a la tomada por la función de protección para impedir el funcionamiento normal del microcircuito, pudiendo ser perceptible la función de señuelo a continuación de esta duración sin que esto impida la protección del microcircuito.

Se observa, en la figura 1, una tarjeta de un microcircuito 105 que incluye, ligados entre sí por un bus 155, un microprocesador 110, unas entradas/salidas 115, una memoria no volátil 120 que conserva un sistema operativo ("operating system") 125, una memoria no volátil 130 que incluye una matriz de memoria 135 y directamente controlada por el microprocesador 110.

Un programa 150 de escritura rápida tal como el expuesto en relación con la figura 4 se conserva o bien en la memoria no activa 120, como se ilustra en la figura 1, o bien en la memoria no volátil 130, o bien está cableado en el microprocesador 110. Como variante, el programa 150 se implementa directamente por el sistema operativo 125 conservado en la memoria no activa 120.

La memoria no activa 120 o la memoria no volátil 130 conservan unas instrucciones de un programa de funcionamiento de la tarjeta 105. Este programa pone en práctica, particularmente, las etapas del modo de realización particular del procedimiento ilustrado en la figura 2.

Como se ilustra en relación con las figuras 2 y 5, el procedimiento objeto de la presente invención se pone en práctica cada vez que el funcionamiento de la tarjeta de microcircuito 105 comprende una etapa 205 de determinación de si tiene lugar un ataque, de acuerdo con unas técnicas conocidas.

Si se detecta un ataque, se efectúa una función de protección destinada a proteger la tarjeta y/o su contenido.

En conformidad con la presente invención, incluso si no se detecta ningún ataque, se efectúa una función de señuelo que simula la función de protección siendo perceptible, desde el exterior de dicho microcircuito, de manera sensiblemente idéntica a la función de protección.

En unos modos de realización simples, la función de señuelo es idéntica a la función de protección en un valor de parámetro o de variable cercanos y estos valores presentan el mismo número de datos binarios ("bits") y, eventualmente, el mismo número de datos binarios iguales a "0".

Como se ilustra en la figura 2, en unos modos de realización, la función de protección consiste, en el curso de una etapa 210, en escribir un dato predeterminado en una primera dirección de una memoria no volátil. Se trata, por ejemplo, de poner en un valor predeterminado un banderín de destrucción “kill flag”, escribiendo un dato predeterminado, en una primera dirección de la memoria no volátil que corresponde a este banderín.

En unos modos de realización, en conformidad con la presente invención, incluso si no se detecta ningún ataque, se efectúa una etapa 215 de realización de una función que presente la misma firma, en términos de consumo eléctrico, que la etapa de escritura de un dato predeterminado en la primera dirección de la memoria no volátil.

En unos modos de realización simples, en el curso de la etapa de realización de la función de señuelo, se efectúa una escritura en la memoria no volátil en una segunda dirección diferente de la primera dirección.

Para que las firmas sean lo más parecidas posible, en el curso de la etapa de escritura en la segunda dirección, se escribe un mismo número de informaciones binarias que el dato predeterminado y se implementa el mismo protocolo de escritura que durante la escritura del dato predeterminado. Preferiblemente, en el curso de la etapa de escritura en la segunda dirección, se escribe el dato predeterminado en la segunda dirección.

Por ejemplo, si la función “Killcard(dirección1)” se utiliza durante la detección de un ataque, la función “Killcard(dirección2)” se implementa cuando no hay detección de un ataque.

Un código, o serie de instrucciones, correspondiente es el siguiente:

```
If attack detected {
Complete processing of the current APDU;
Killcard(adresse1);
}
Else {
   Complete processing of the current APDU
Killcard(adresse2);
}
```

Como variante, la función de protección, denominada “killcard1(dirección1)” es diferente de la función de señuelo, denominada, por ejemplo, “killcard2(dirección2)”, efectuándose la segunda, por ejemplo, sin relectura ni verificación de los datos de verificación, como se expone a continuación.

Como se ilustra en la figura 5, en unos modos de realización, la función de protección consiste, en el curso de una etapa 510, en cifrar al menos un objeto sensible conservado en la memoria no volátil, con una clave secreta, en escribirla en la memoria no volátil y en hacerla inaccesible, por ejemplo, borrando la versión en claro del objeto sensible. De ese modo, una vez cifrados los datos, el circuito no puede ya funcionar normalmente.

En estos modos de realización, de conformidad con la presente invención, incluso si no se detecta ningún ataque, en el curso del funcionamiento del microcircuito, se efectúa una etapa 515 de realización de una función que presenta la misma firma, en términos de consumo eléctrico, que la etapa de cifrado de cada objeto sensible y de escritura en la memoria no volátil. Por ejemplo, en el curso de la etapa 515, se efectúa un cifrado de datos inútiles en el funcionamiento del microcircuito.

Debido al hecho de la reversibilidad del cifrado, con una clave simétrica o asimétrica, el emisor (“issuer”) de la tarjeta puede descifrar cada dato sensible cifrado de ese modo en el curso de la etapa 510, rescribirlo en la memoria no volátil y convertir de ese modo la tarjeta, de nuevo, en operativa.

Como variante, sólo se realiza un cifrado parcial de los datos por la función de señuelo. La función de señuelo no tiene entonces una duración tan larga como la función de protección. En efecto, incluso si el atacante puede detectar entonces la función de protección, de una duración más larga, y cortar inmediatamente la alimentación del microcircuito, el microcircuito está protegido porque unos datos necesarios para su funcionamiento, al menos normales, están borrados, incluso si todos los datos que deben ser borrados por la función de protección no lo han sido.

Como se describe más adelante en relación con la figura 4, una variante de este algoritmo consiste en utilizar una función Killcard modificada para, durante una escritura en una de la primera y segunda direcciones, no realizar el borrado de la zona de escritura, de relectura y/o de verificación del dato de verificación, particularmente de la suma de verificación (“checksum”). Con este fin, antes de realizar la operación de escritura, el microprocesador de la

tarjeta determina si esta escritura se refiere a una de las direcciones dirección1 o dirección2. Si es así, se utiliza la operación de escritura simplificada (véase la figura 4). Si no, se realiza la operación de escritura completa (véase la figura 3). Se observa que la diferencia de tratamiento puede también ser el resultado de la arquitectura de la memoria en sí.

En unas variantes, en el curso de la etapa de realización de la función de señuelo, se efectúa una escritura en la memoria no volátil, en la primera dirección, de un dato diferente a dicho dato predeterminado que se escribe, en la misma dirección, por la función de protección.

Como se observa, en la figura 3, un protocolo actual de escritura de un dato en la memoria no volátil comprende:

- una etapa 305 de borrado de la zona de escritura, al menos en la dirección en la que se debe escribir un dato; esta etapa se denomina, en inglés, “erase”;

- una etapa 310 de determinación de al menos una suma de verificación (en inglés “checksum”) a partir del dato que debe ser escrito;

- una etapa 315 de escritura del dato y de cada suma de verificación determinada durante la etapa 310;

- una etapa 320 de la relectura del dato escrito y de cada suma de verificación; y

- una etapa 325 de determinación de la validez de las sumas de verificación rehaciendo, en los datos leídos, una determinación de cada suma de verificación correspondiente y comparándola con la suma de verificación leída.

Se observa que la etapa 305 de borrado de la zona de escritura puede consistir en una puesta a un mismo nivel de las cargas de la zona de escritura.

Como se comprende, este protocolo de escritura impone una etapa de escritura muy larga que usa la memoria y ralentiza la ejecución.

Se observa aquí que la detección de un error de suma de verificación para la dirección dirección2 no tiene ninguna consecuencia, puesto que los datos escritos no son vueltos a leer jamás, en unos modos de realización, no se desencadena ninguna acción en el caso de una detección de ese tipo.

En otros modos de realización, esta detección se considera como un índice de un ataque. Si se detecta otro índice, ligado por ejemplo, al sobrepaso de un valor límite por el número utilizaciones de una clave de cifrado o de autenticaciones de la tarjeta, se determina que se produce un ataque y se realiza la función de protección del microcircuito.

Como se observa en la figura 4, en unos modos de realización preferidos del procedimiento objeto de la presente invención, el protocolo de escritura en la segunda dirección y, eventualmente, también en la primera dirección no incluye:

- la etapa de borrado de la zona de escritura; esta etapa se mantiene, eventualmente, para ciertas escrituras elegidas aleatoriamente o cíclicamente, en el curso de la etapa 405;

- la etapa de determinación de al menos una suma de verificación (en inglés “checksum”); esta etapa se mantiene, eventualmente, para ciertas escrituras elegidas aleatoriamente o cíclicamente, en el curso de una etapa 410;

- la etapa de escritura de la suma o sumas de verificación; esta etapa se mantiene, eventualmente, en el curso de una etapa 416 para cada suma de verificación determinada en el curso de una etapa 410;

- la etapa de relectura del dato escrito; esta etapa se mantiene, eventualmente, en el curso de una etapa 420, para los datos que hayan dado lugar a la determinación de al menos una suma de verificación;

- la etapa de determinación de la validez de las sumas de verificación rehaciendo, sobre los datos leídos, una determinación de cada suma de verificación correspondiente; esta etapa se mantiene, eventualmente, en el curso de la etapa 425, para los datos que hayan dado lugar a la determinación de al menos una suma de verificación.

De ese modo, en un modo de realización preferido, el protocolo de escritura en la memoria no volátil, en una de entre la primera y segunda direcciones, no incluye más que:

- la etapa 415 de escritura del dato, y

- únicamente para ciertas escrituras de datos elegidos aleatoriamente o cíclicamente, la etapa 405 de borrado de la zona de escritura y/o las etapas 410, 416, 420 y 425.

Se observa aquí que la escritura efectuada por la función de señuelo no puede jamás incluir el borrado de la zona de escritura ("erase") en el caso de que la escritura, por un lado, y el mantenimiento del estado de escritura, por otro lado, presenten la misma firma. En efecto, si estas firmas son diferentes, cuando la función de señuelo se reitera sin borrado de la zona de escritura ("erase"), mantiene las mismas células de memoria no volátil en el estado de escritura, lo que implicaría una firma diferente de la función de protección que, por definición, corresponde a un cambio de estado de las células de la memoria no volátil. De ese modo, si estas firmas son diferentes, al menos una parte de las funciones de señuelo (por ejemplo seleccionadas cíclicamente o aleatoriamente) comprenden el borrado de la zona de escritura.

Como variante, en lugar de eliminar totalmente el borrado de la zona de escritura, se prevé un borrado parcial. Un borrado parcial de ese modo puede consistir en realizar una descarga (o carga según las arquitecturas) de las cargas de cada célula de memoria afectada por la escritura durante una duración inferior a la que permite una descarga (o carga) completa de la célula de memoria.

En unos modos de realización, la escritura en la memoria no volátil efectuada por la función de protección incluye la generación, la escritura, la relectura y la verificación de la suma o sumas de verificación mientras que la escritura en memoria no volátil efectuada por la función de señuelo no las incluye. Como variante, como se expone más abajo, sólo ciertas escrituras (seleccionadas cíclicamente o aleatoriamente) efectuadas por la función de señuelo comprenden la generación, la escritura, la relectura y la verificación de la suma o sumas de verificación. En estos dos últimos casos, la utilización de la memoria se reduce, la velocidad de funcionamiento normal del microcircuito se incrementa, mientras se impide a un atacante reconocer la realización de la función de protección.

En consecuencia, el retardo de finalización de la escritura es muy limitado cuando no hay borrado de la zona de escritura y/o no hay implementación de la suma o sumas de verificación, con relación al estado de la técnica. Se evita de ese modo ralentizar demasiado el funcionamiento del microcircuito por la realización repetida de la función de señuelo. Además, se reduce la utilización de la memoria por las escrituras realizadas por la función de señuelo. En efecto, las células de memoria utilizadas por la función de señuelo podrían envejecer demasiado rápidamente puesto que las memorias tienen una duración de vida limitada en términos del número de ciclos de escritura. Retirando la etapa de relectura de los datos escritos así como la etapa de borrado de la zona de escritura ("erase"), no solamente se reduce la duración de la escritura sino que se alarga la duración de vida útil de las células de memoria utilizadas por la función de señuelo.

Se observa también que, si el envejecimiento de la célula provoca unos errores detectables por la implementación de una suma de verificación, esto permite detectar este deterioro. En este caso, el programa de funcionamiento puede conmutar automáticamente la escritura por la función de señuelo sobre otra célula inutilizada.

Se observa que la presente invención se puede poner en práctica en la forma de un programa que se ejecute en el microcircuito o en la forma de un circuito integrado especializado, por ejemplo un ASIC (de Application-Specific Integrated Circuit), un circuito de lógica programable o un circuito integrado digital que se pueda reprogramar después de su fabricación.

Cuando una tarjeta con microcircuitos implementa el modo de realización preferido del procedimiento objeto de la presente invención, el atacante que analice el consumo eléctrico no puede determinar en qué caso la carta actúa tras la detección de un ataque.

En unos modos de realización, una entidad electrónica de chips o portátil incluye un dispositivo de protección de un microcircuito que implementa el procedimiento de protección objeto de la presente invención.

Por ejemplo, esta entidad electrónica es un PDA (acrónimo de "personal digital assistant" por asistente personal digital), una llave USB (acrónimo de "universal serial bus" por bus serie universal), una tarjeta de memoria, un teléfono móvil, un pasaporte electrónico o una tarjeta de chips (es decir de acuerdo con la norma ISO 7816 y asegurada, por ejemplo certificada de conformidad con los criterios comunes).

Se observa que, preferiblemente, la función de señuelo no tiene otro efecto/resultado/función que el hecho de ser un señuelo para la función de protección, que sea perceptible, desde el exterior del microcircuito, de manera sensiblemente idéntica a la función de protección.

La función de señuelo no es de ese modo funcional y no influencia el funcionamiento del microcircuito aparte de la fase de ejecución de esta función de señuelo. Por ejemplo, la función de señuelo efectúa la escritura de datos que no son jamás leídos o utilizados o el cifrado de al menos un dato inútil en el funcionamiento del microcircuito. Gracias a esta característica preferible, se puede prever una función de señuelo más rápida, por ejemplo una escritura más rápida, por ejemplo, sin etapa de borrado y/o sin etapa de verificación del dato escrito, que si la función de señuelo fuera útil en el funcionamiento del microcircuito.

REIVINDICACIONES

1. Procedimiento de protección de un microcircuito contra un ataque, que comprende:

- una etapa (205) de determinación de si se detecta un ataque,

- si se detecta un ataque, una etapa (210, 510) de realización de una función de protección;

caracterizado porque el procedimiento comprende además:

- si no se detecta ningún ataque, una etapa (215, 515) de realización de una función de señuelo que simula la función de protección para que sea perceptible, desde el exterior de dicho microcircuito, de manera sensiblemente idéntica a la función de protección.

2. Procedimiento de acuerdo con la reivindicación 1, caracterizado porque la función de señuelo presenta un consumo eléctrico sensiblemente idéntico al de la función de protección.

3. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 ó 2, caracterizado porque la función de protección efectúa una etapa de escritura de un dato predeterminado en una primera dirección de una memoria no volátil.

4. Procedimiento de acuerdo con la reivindicación 3, caracterizado porque la función de señuelo efectúa una etapa de escritura en memoria no volátil en una segunda dirección diferente de la primera dirección.

5. Procedimiento de acuerdo con la reivindicación 4, caracterizado porque, en el curso de la etapa de escritura en la segunda dirección por la función de señuelo, se escribe un mismo número de informaciones binarias que en el curso de la escritura en la primera dirección por la función de protección y se implementa el mismo algoritmo de escritura que durante la escritura en la primera dirección por la función de protección.

6. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 3 a 5, caracterizado porque dichas etapas de escritura en memoria no volátil implementan un algoritmo diferente al de las otras etapas de escritura en memoria no volátil efectuadas durante el funcionamiento normal del microcircuito.

7. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 3 a 6, caracterizado porque, en el curso de al menos una parte de dichas etapas de escritura en memoria no volátil, no se implementa el dato de verificación.

8. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 3 a 7, caracterizado porque, en el curso de al menos una parte de dichas etapas de escritura en memoria no volátil, no se implementa la relectura del dato escrito.

9. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 3 a 8, caracterizado porque, en el curso de al menos una parte de dichas etapas de escritura en memoria no volátil, no se implementa el borrado de la zona de escritura (“erase”).

10. Procedimiento de acuerdo con la reivindicación 9, caracterizado porque, si la rescritura de datos en la memoria no volátil es perceptible, desde el exterior de dicho microcircuito, de manera idéntica a la escritura inicial de dichos datos, la función de señuelo no incluye el borrado de la zona de escritura.

11. Procedimiento de acuerdo con la reivindicación 9, caracterizado porque la función de protección implementa dicha etapa de borrado de la zona de escritura.

12. Procedimiento de acuerdo con la reivindicación 11, caracterizado porque una parte de las ejecuciones de la función de señuelo comprende dicha etapa de borrado de la zona de escritura.

13. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 12, caracterizado porque la función de protección efectúa una etapa de cifrado de al menos un dato sensible.

14. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 13, caracterizado porque la función de señuelo no tiene otra función más que la de simular la función de protección.

15. Dispositivo de protección de un microcircuito contra un ataque, que comprende:

• un medio (110, 120, 130, 150) de determinación de si se ha detectado un ataque, y

• un medio de control (110, 120, 130, 150) adaptado:

- si se detecta un ataque, para realizar una función de protección;

estando dicho medio de control caracterizado porque está adaptado para:

- si no se detecta ningún ataque, realizar una función de señuelo que simula la función de protección que sea perceptible, desde el exterior de dicho microcircuito, de manera sensiblemente idéntica a la función de protección.

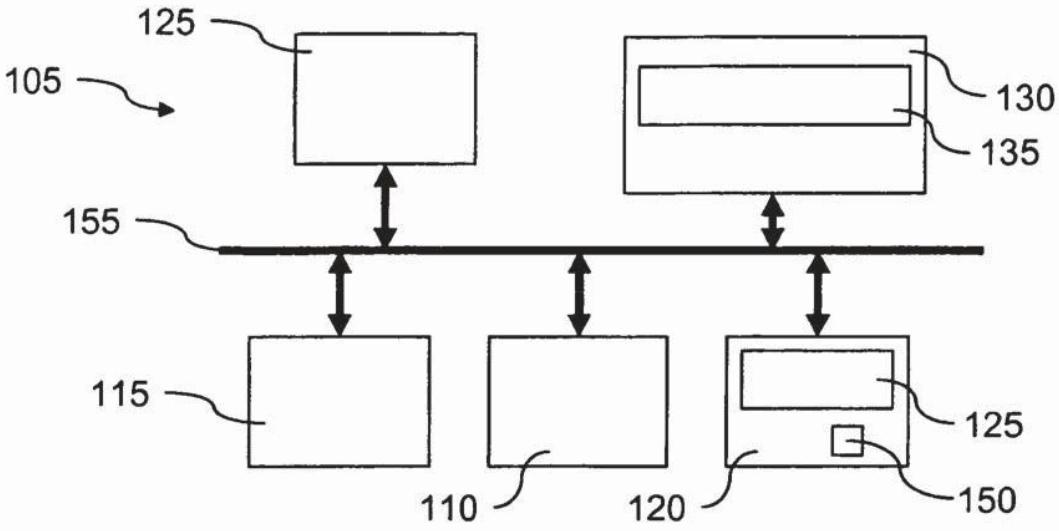

Figura 1

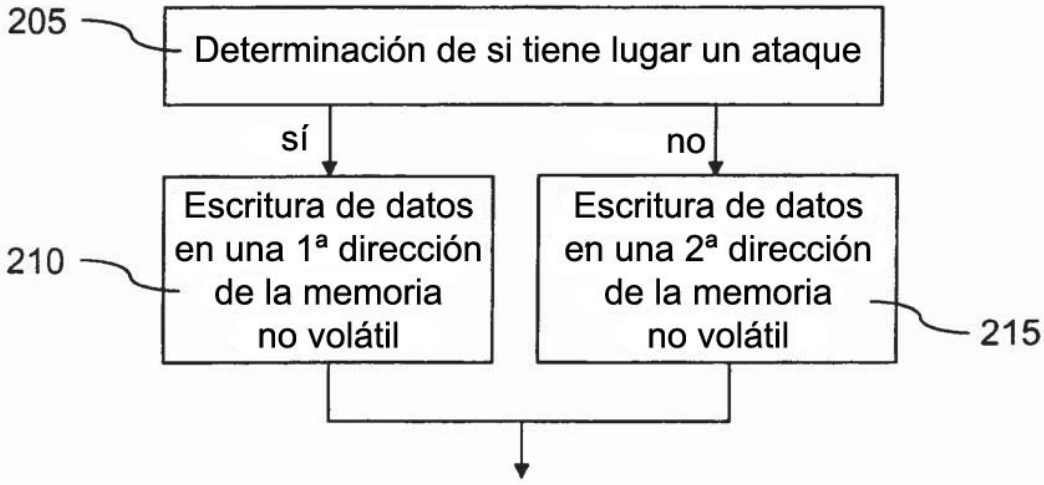

Figura 2

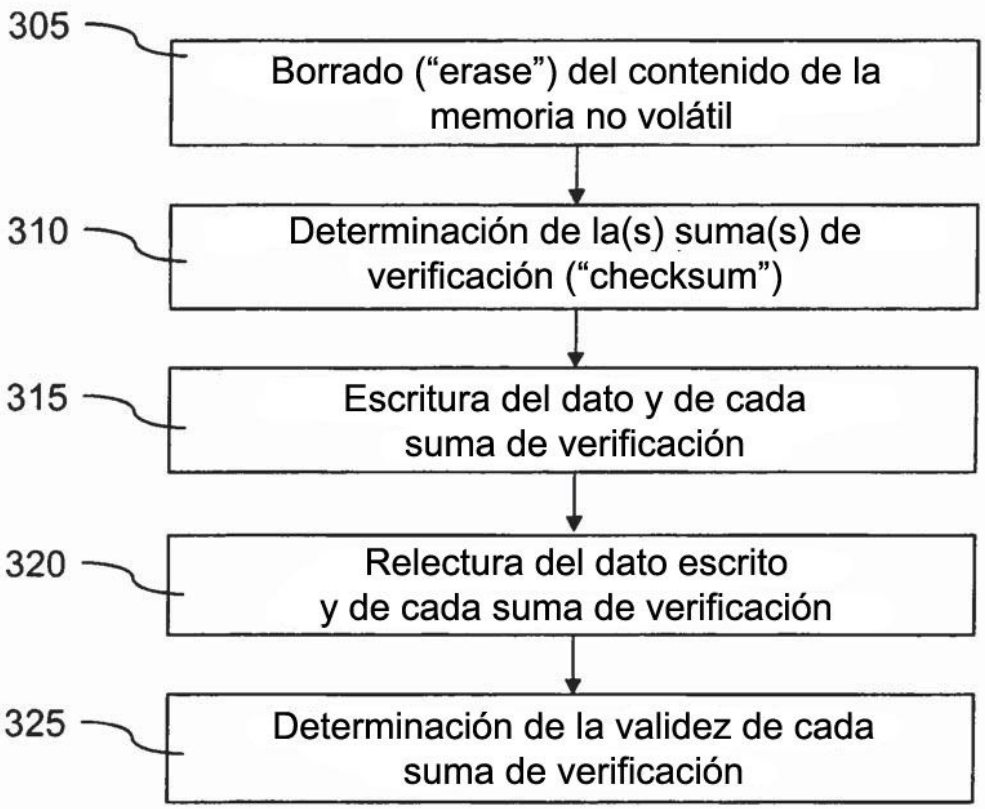
305
Borrado (“erase”) del contenido de la memoria no volátil
310
Determinación de la(s) suma(s) de verificación (“checksum”)
315
Escritura del dato y de cada suma de verificación
320
Relectura del dato escrito y de cada suma de verificación
325
Determinación de la validez de cada suma de verificación

Figura 3

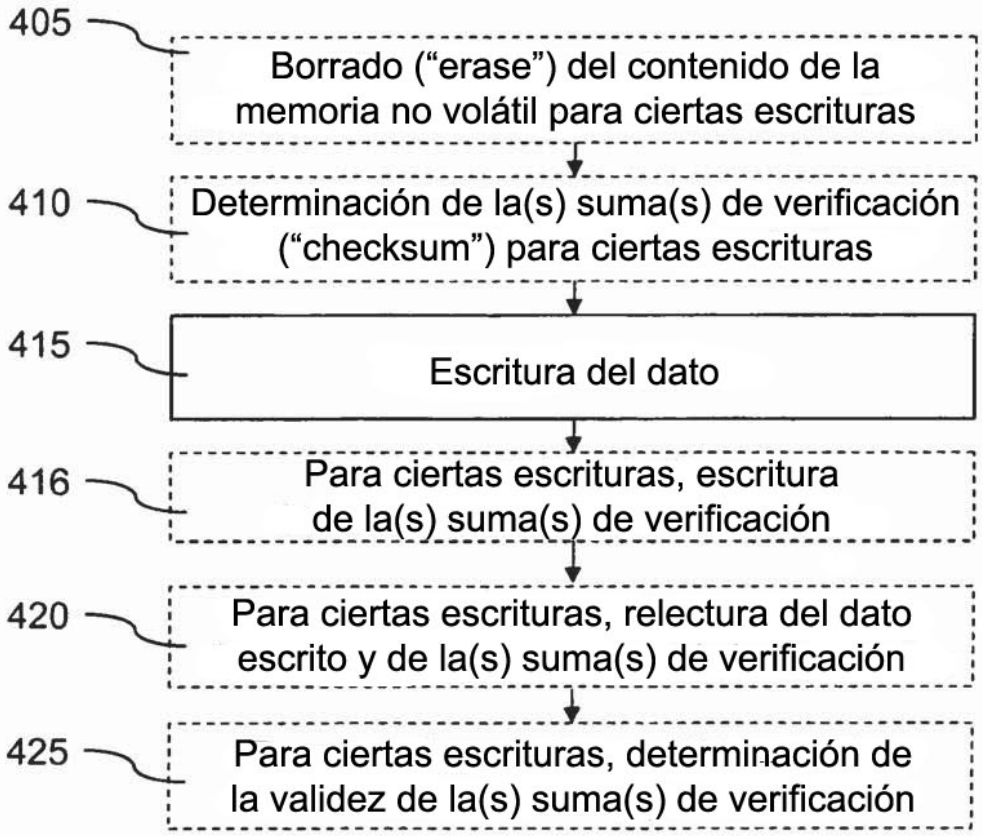

Figura 4

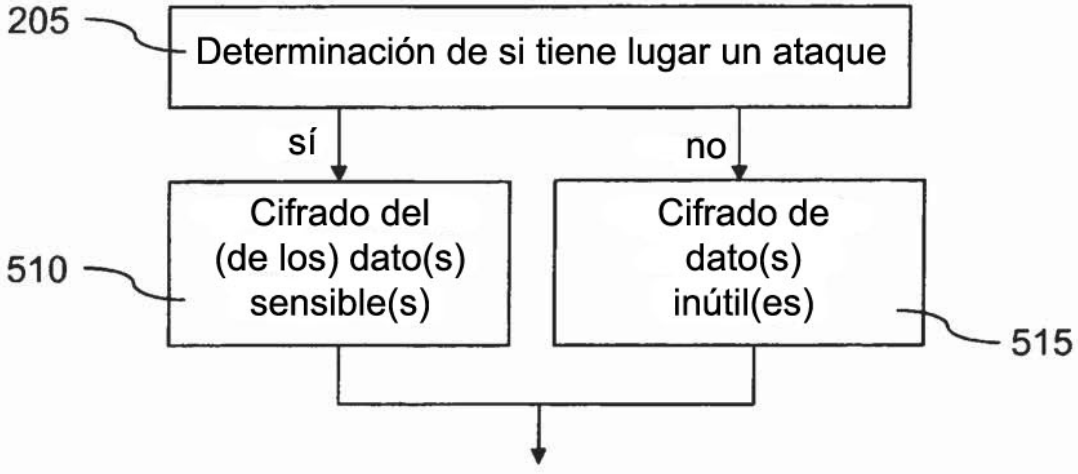

Figura 5