(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 473 326**

(51) Int. CI.:

G06F 21/60 (2013.01)
G06F 21/55 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.08.2005 E 05798504 (6)**

(97) Fecha y número de publicación de la concesión europea: **19.03.2014 EP 1779284**

(54) Título: **Procedimiento y dispositivo de tratamiento de datos**

(30) Prioridad:

17.08.2004 FR 0408928

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.07.2014

(73) Titular/es:

OBERTHUR TECHNOLOGIES (100.0%)
420, rue d'Estienne d'Orves
92700 Colombes , FR

(72) Inventor/es:

CHAMBEROT, FRANCIS

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

DESCRIPCIÓN

Procedimiento y dispositivo de tratamiento de datos

La presente invención se refiere a un procedimiento de tratamiento de datos, aplicado por ejemplo en una tarjeta de microcircuito.

En ciertos contextos, se busca que el funcionamiento de los aparatos de tratamiento de datos sea seguro. Este es especialmente el caso en el ámbito del dinero electrónico, en el que una entidad electrónica (por ejemplo una tarjeta de microcircuito) es portadora de información que representa un valor pecuniario y que solo puede por lo tanto modificarse según un protocolo determinado. Asimismo puede tratarse de una entidad electrónica que permite la identificación de su portador, en cuyo caso el funcionamiento debe ser seguro para evitar cualquier falsificación o uso abusivo.

Tal entidad electrónica es por ejemplo una tarjeta bancaria, una tarjeta SIM para telefonía (procediendo el acrónimo de SIM del inglés *Subscriber Identity Module*), un pasaporte electrónico, un módulo seguro de tipo HSM (del inglés *Hardware Security Module*) tal como una tarjeta PCMCIA de tipo IBM4758, sin que estos ejemplos sean limitativos.

Para mejorar la seguridad del funcionamiento, se pretende la protección contra los diversos tipos de ataques considerables. Una categoría importante de ataques que hay que reprimir está constituida por los ataques denominados por generación de fallos, durante los cuales personas malintencionadas pretenden hacer salir el aparato de tratamiento de datos de su funcionamiento normal, y por lo tanto seguro.

Para detener este tipo de ataques, los procedimientos de tratamiento de datos habitualmente usados prevén etapas de verificación del desarrollo normal del procedimiento, con el objetivo de detectar anomalías, cuyo posible origen sea un ataque por generación de fallos. Cuando se detecta una anomalía (es decir que el desarrollo normal no está verificado), se procede inmediatamente al tratamiento de la anomalía, generalmente denominada tratamiento de seguridad. Este tipo de tratamiento consiste efectivamente en una contramedida destinada a reprimir el ataque, por ejemplo impidiendo cualquier funcionamiento posterior del aparato de tratamiento de datos.

Como se ha indicado, se concibe habitualmente el tratamiento de la anomalía como inmediato después de la detección, ya que el hecho de seguir con el tratamiento en presencia de una anomalía implica a primera vista el riesgo de seguir degradando el funcionamiento del aparato de tratamiento de datos, y por lo tanto de su seguridad.

Sin embargo, el inventor indica que esta concepción habitual da al atacante una información sobre el momento en el que se lleva a cabo la detección de la anomalía. En efecto, el instante de detección de la anomalía es en sí mismo difícilmente accesible desde el exterior. Sin embargo, se piensa que el atacante puede tener acceso, por una observación y un análisis del consumo eléctrico (o de la radiación electromagnética) del aparato, en el instante de implementación del tratamiento de la anomalía, por ejemplo en el caso en el que este tratamiento consiste en una acción sobre un dispositivo externo. Puesto que este tratamiento va inmediatamente después de la detección de la anomalía en la concepción habitual, el atacante deduciría de ello de manera relativamente fácil el instante de detección de la anomalía.

De este modo, debido a la proximidad de la detección de la anomalía y del tratamiento de la misma en los sistemas usuales, el atacante tiene acceso a una información adicional acerca del funcionamiento del aparato de tratamiento de datos, lo cual es evidentemente perjudicial para la seguridad del procedimiento.

El documento US 2003/0028794 A1 divulga un procedimiento de protección de un dispositivo informático en el que se comparan datos de huellas digitales, en función del resultado de esta comparación, se actualiza una variable de control para compararla con un umbral.

La invención propone un procedimiento según la reivindicación 1.

Un atacante que pretende comprender el funcionamiento del procedimiento tendrá de este modo dificultades para discernir el funcionamiento normal (caso de verificación positiva) del funcionamiento en caso de anomalía (es decir, de verificación negativa).

La segunda acción es por ejemplo diferente de la primera acción. De este modo la segunda acción puede comprender menos riesgos, incluso ningún riesgo, para la seguridad del sistema.

Cuando se lleva a cabo una tercera acción en caso de verificación positiva, la etapa de tratamiento puede comprender la realización de al menos una cuarta acción que tiene al menos una segunda característica común con la tercera acción.

Un atacante no podrá por lo tanto distinguir los modos de funcionamiento. De este modo, no podrá evitar el tratamiento de la anomalía.

Cuando el procedimiento se aplica en un aparato electrónico, la primera y segunda acciones pueden tener una primera o una segunda característica común que es, por ejemplo, el consumo eléctrico o la radiación electromagnética del aparato generado/a por la primera, respectivamente la tercera, acción y por la segunda, respectivamente la cuarta, acción. De este modo, un atacante no podrá distinguir el modo de funcionamiento normal del modo de funcionamiento anormal por la observación del comportamiento eléctrico y/o electromagnético del aparato electrónico.

La primera o segunda característica común puede ser asimismo el número de instrucciones aplicado en la primera, respectivamente la tercera, acción y en la segunda, respectivamente la cuarta, acción, lo cual hace imposible la distinción de los modos de funcionamiento por la duración de dichas acciones.

La primera o segunda característica común puede ser además el tipo de instrucción aplicado por la primera, respectivamente la tercera, acción y por la segunda, respectivamente la cuarta, acción, lo cual garantiza una gran similitud en la firma eléctrica y/o electromagnética de dichas acciones.

La primera o segunda característica común puede también ser el tipo de datos procesados por la primera, respectivamente la tercera, acción y por la segunda, respectivamente la cuarta, acción, lo que garantiza asimismo tal similitud.

Cuando la primera, respectivamente la tercera, acción comprende un acceso a una primera zona de una memoria, la segunda, respectivamente la cuarta, acción puede comprender un acceso a una segunda zona de dicha memoria diferente de la primera zona. El tratamiento de los datos parece por lo tanto similar en ambos modos de funcionamiento mencionado anteriormente, pero de hecho se efectúa en contextos diferentes.

Según otra posibilidad, la primera o segunda característica común es la comunicación con un dispositivo externo, que puede ser por ejemplo un criptoprocesador, una memoria (por ejemplo, una memoria regrabable de semiconductor), o un terminal de usuario. La comunicación con tales dispositivos exteriores es en efecto observada por los atacantes y esta característica común es por lo tanto particularmente susceptible de inducirles a error.

La primera acción puede incluir una etapa segura, por ejemplo un algoritmo criptográfico, que está de este modo protegida contra los ataques por generación de fallo.

Por ejemplo, los datos de bloqueo se graban en una memoria física.

Según una posibilidad particularmente interesante, la grabación de datos de bloqueo puede llevarse a cabo según una cronología idéntica a una grabación de datos en la memoria física en caso de desarrollo normal del procedimiento.

Según una realización, estos datos representan un valor pecuniario. De este modo, un atacante no podrá discernir a *priori* un bloqueo del aparato de una operación sobre el valor que representa.

El criterio es negativo por ejemplo si se proporciona una firma errónea o si se detecta una anomalía.

El criterio puede también ser negativo si se detecta un ataque. Como ya se ha visto, la invención es especialmente interesante en este contexto.

El criterio puede asimismo ser negativo si se detecta un error funcional. Tal tratamiento en caso de error funcional no es habitual pero se revela interesante para mejorar la seguridad del sistema, especialmente porque tales errores funcionales son muy raros fuera de las situaciones de ataque y traducen de este modo la probable presencia de un ataque.

Según una posible característica, la etapa de tratamiento y la etapa de verificación están separadas por una etapa intermedia que comprende al menos una instrucción determinada durante la ejecución del procedimiento, por ejemplo de manera aleatoria. La comprensión del funcionamiento del sistema por el atacante sigue siendo todavía complicada.

Según una posible realización, una tarjeta de microcircuito comprende un microprocesador y el procedimiento es aplicado por el microprocesador.

La invención propone asimismo un dispositivo según la reivindicación 25.

Este dispositivo es por ejemplo una tarjeta de microcircuito.

Otras características y ventajas de la presente invención se pondrán de manifiesto en la siguiente descripción, realizada con referencia a los dibujos adjuntos, en los que:

- la figura 1 representa de manera esquemática los elementos principales de una forma de realización posible para una tarjeta de microcircuito;

- la figura 2 representa el aspecto físico general de la tarjeta de microcircuito de la figura 1;

- la figura 3 representa un procedimiento realizado conforme a una primera realización de la invención;

- la figura 4 representa un procedimiento realizado conforme a una segunda realización de la invención;

- la figura 5 representa un procedimiento realizado conforme a una tercera realización de la invención.

La tarjeta de microcircuito 10, cuyos elementos principales están representados en la figura 1, incluye un microprocesador 2 conectado por una parte a una memoria viva (o RAM del inglés *Random Access Memory*) 4 y por otra parte a una memoria de semiconductor regrabable 6, por ejemplo una memoria muerta borrable y programable eléctricamente (o EEPROM del inglés *Electrically Erasable Programable Read Only Memory).* En una variante, la memoria regrabable de semiconductor 6 podría ser una memoria ultrarrápida.

Las memorias 4, 6 están conectadas al microprocesador 2 por un bus cada una en la figura 1; en una variante, podría tratarse de un bus común.

La tarjeta de microcircuito 10 incluye asimismo una interfaz 8 de comunicación con un terminal de usuario realizada aquí en forma de contacto, de los cuales uno asegura una conexión bidireccional con el microprocesador 2. La interfaz 8 permite de este modo el establecimiento de una comunicación bidireccional entre el microprocesador 2 y el terminal de usuario en el que la tarjeta de microcircuito 10 se insertará.

De este modo, durante la inserción de la tarjeta de microcircuito 10 en un terminal de usuario, el microprocesador 2 aplicará un procedimiento de funcionamiento de la tarjeta de microcircuito 10, según un juego de instrucciones, almacenadas por ejemplo en una memoria muerta (o ROM del inglés *Read-Only Memory*) - no representada - o en la memoria regrabable 6, que define un programa de ordenador. Este procedimiento incluye generalmente el intercambio de datos con el terminal de usuario a través de la interfaz 8 y el tratamiento de datos en el seno de la tarjeta de microcircuito 10, y precisamente en el seno del microprocesador 2 con un uso eventual de datos almacenados en la memoria regrabable 6 y de datos almacenados temporalmente en la memoria viva 4.

Ejemplos de tales procedimientos que aplican la invención se dan a continuación con referencia las figuras 3 a 5.

La figura 2 representa el aspecto físico general de la tarjeta de microcircuito 10 realizada con la forma general de un paralelepípedo rectángulo de muy bajo espesor.

La interfaz de comunicación 8 provista de los contactos ya mencionados aparece claramente en la cara de la tarjeta de microcircuito 10 visible en la figura 2, en forma de rectángulo inscrito en la cara superior de la tarjeta de microcircuito 10.

La figura 3 representa un procedimiento de lectura en la memoria regrabable 6 tal que puede ser aplicado por la tarjeta de microcircuito 10 presentada en la figura 1, por ejemplo gracias a la ejecución de un programa de ordenador en el seno del microprocesador 2. Este procedimiento es proporcionado como un primer ejemplo de aplicación de la invención.

Tal procedimiento se utiliza por ejemplo cuando datos grabados en la memoria regrabable (o EEPROM) 6 deben ser utilizados por el microprocesador 2 durante una operación de tratamiento de datos; los datos grabados en memoria regrabable 6 son previamente leídos para ser transferidos a la memoria viva 4 donde podrán ser manipulados con facilidad.

Como se ha representado en la etapa E302 de la figura 3, el procedimiento recibe en la entrada la dirección ADR en la que debe efectuar la lectura en la memoria regrabable (o EEPROM) 6.

En la etapa E304, el procedimiento inicializa con el valor 0 un indicador de error S.

Al inicializarse correctamente las variables, se pasa entonces a etapas de verificación dedicadas a asegurar un funcionamiento seguro del sistema como es necesario generalmente en los contextos seguros de uso de las tarjetas de microcircuito.

De este modo, se procede en la etapa E306 a la verificación de una suma de control. Naturalmente, otras verificaciones son posibles, pero no han sido representadas en la figura 3 por claridad de exposición de la invención.

La etapa E306 de verificación de una suma de control consiste en verificar que los datos grabados en memoria regrabable 6 son efectivamente coherentes con la suma de control (a veces denominada según la terminología anglosajona "*checksum*") asociada a estos datos.

En una alternativa a la etapa E308: si la suma de control no es errónea, es decir que la verificación de la suma de control es positiva, se sigue con el funcionamiento normal en la etapa E314 descrita más adelante; si por el contrario se

detecta un error en la suma de control, es decir que la etapa de verificación de la suma de control da un resultado negativo, se procede a la etapa E310.

Se puede observar que la presencia de una suma de control errónea, si indica en cualquier caso un desarrollo anormal del funcionamiento de la tarjeta de microcircuito, puede tener diversos orígenes: puede tratarse de un error funcional (por ejemplo un error en el contenido de la memoria regrabable 6), pero puede tratarse asimismo de la huella de un ataque por generación de fallo.

En la etapa E310, se actualiza el indicador de error S con el valor 1 para indicar que se ha detectado una anomalía.

Se procede entonces a la etapa E312, en la que se sustituye la dirección de lectura ADR recibida en la entrada del procedimiento (véase la etapa E302 descrita anteriormente) por la dirección de una "zona de señuelo" situada en la memoria regrabable 6. La zona de señuelo es una zona de memoria a *priori* diferente de la dirección recibida en la etapa E302; se trata por ejemplo de una dirección en la que ninguna lectura debe efectuarse normalmente en funcionamiento normal (es decir durante el desarrollo normal y sin anomalía del procedimiento de funcionamiento de la tarjeta de microcircuito).

A modo de ejemplo, estas zonas de señuelo pueden incluir datos determinados de manera aleatoria y/o datos de igual estructura que los datos que inicialmente estaban previstos leer en la dirección ADR recibida en la etapa E302.

Se observa que la etapa E312 que se acaba de describir no constituye una etapa de tratamiento de la anomalía detectada en la etapa E308: por ejemplo, no se trata ni de la transmisión de un código relativo a la anomalía detectada, ni de la visualización de un mensaje relativo a esta anomalía, ni de una contramedida para el caso en el que se considera que la anomalía procede de un ataque por generación de fallo.

Después de la etapa E312 (realizada como la etapa E310 solo en caso de desarrollo anormal del funcionamiento de la tarjeta de microcircuito, es decir en caso de verificación negativa del funcionamiento normal en la etapa), se procede a la etapa E314 que, como se indica más arriba, forma parte del desarrollo normal del funcionamiento de la tarjeta de microcircuito (en caso de verificación positiva de la suma de control como se indica en relación con la etapa E308).

La etapa E314 consiste en transferir los datos de la memoria regrabable 6 a la memoria viva 4 y constituye por lo tanto a este respecto el núcleo del procedimiento de la figura 3, después de las etapas de inicialización y de verificación.

En concreto, la etapa E314 efectúa una lectura en la memoria regrabable 6 en la dirección especificada por la variable ADR mencionada anteriormente y una grabación de los datos leídos en memoria viva 4 en una zona habitualmente designada memoria intermedia que sirve generalmente para la manipulación de los datos.

Se puede observar que, en el caso en el que la suma de control ha sido verificada positivamente en las etapas anteriores, la variable ADR apunta efectivamente a la dirección en memoria regrabable 6 recibida en la entrada, es decir a los datos que deben efectivamente ser leídos. Por el contrario, cuando se ha detectado una suma de control errónea (es decir que la verificación ha sido negativa en las etapas anteriores), la variable ADR apunta a la zona de señuelo definida en la etapa E312, de manera que la etapa E314 realizará de hecho la transferencia de los datos de la zona de señuelo en la zona de memoria intermedia en la memoria viva 4, y no la lectura requerida por la dirección recibida en la etapa E302.

De este modo, en el caso en el que se detecta una anomalía de funcionamiento por la verificación negativa de la etapa E306, no se efectúa un acceso en memoria regrabable 6 en la dirección prevista en funcionamiento normal, donde están generalmente almacenados datos relativamente sensibles desde el punto de vista de la seguridad. De este modo hay una protección contra el acceso a estos datos sensibles por un atacante, en el caso en el que el origen de la anomalía detectada es un ataque por generación de fallo.

Además, al ser realizada la etapa E314 en funcionamiento normal como después de la detección de una anomalía de funcionamiento (aunque con datos diferentes), es casi imposible para un atacante detectar, por ejemplo por medidas de corriente, una salida del funcionamiento normal.

Después de la etapa E314, el procedimiento sigue en la etapa E316 donde se prueba el indicador de error S.

Si el indicador de error S vale 1, lo que corresponde al caso en el que se ha procedido en la etapa E310 (es decir en el caso de una detección de anomalía por verificación negativa de la suma de control en la etapa E306), se procede a la etapa E320 donde se trata la anomalía anteriormente detectada, por ejemplo por la grabación de datos de bloqueo (o cerrojo) en la memoria regrabable 6.

La grabación de un cerrojo en la memoria regrabable 6 consiste en grabar algunos datos en esta memoria 6 que impedirán cualquier uso posterior de la tarjeta de microcircuito 10. Por ejemplo, si la tarjeta de microcircuito 10 se inserta posteriormente en otro terminal de usuario, el microprocesador 2 de la tarjeta de microcircuito 10 detectará la presencia de los datos de bloqueo en la memoria regrabable 6 y no procederá a ningún tratamiento ni intercambio de

informaciones con el terminal de usuario.

La grabación de un cerrojo en la memoria regrabable 6 constituye una contramedida particularmente eficaz contra un ataque por generación de fallo. Este tipo de tratamiento de la anomalía detectada es por lo tanto particularmente interesante en los casos en los que esta anomalía procede de un ataque por generación de fallo, o en los casos en los que la seguridad debe ser de un nivel tal que cualquier anomalía de funcionamiento debe implicar el bloqueo de la tarjeta de microcircuito.

La contramedida puede asimismo consistir en borrar datos confidenciales, por ejemplo claves secretas, de la memoria regrabable 6.

En una variante, la etapa de tratamiento de la anomalía podría consistir en actualizar un indicador (memorizado en memoria viva 4 o en memoria regrabable 6) representativo de la anomalía detectada durante el procedimiento de la figura 3. Esta solución permite no llevar inmediatamente al bloqueo de la tarjeta de microcircuito, guardando la huella de la presencia de una anomalía de funcionamiento para analizar el problema encontrado y eventualmente proceder entonces al bloqueo de la tarjeta (por ejemplo si otros elementos corroboran la hipótesis de un ataque por generación de fallo).

Si la etapa E316 anteriormente descrita indica que el indicador de error S no vale 1 (es decir que la verificación de la etapa E306 ha sido positiva), el procedimiento sigue con su funcionamiento normal en la etapa E318, en la que la dirección de la zona de memoria intermedia en memoria viva 4 mencionada anteriormente es emitida en la salida para permitir el uso de los datos leídos en la memoria regrabable 6 durante el funcionamiento posterior de la tarjeta de microcircuito.

Por ejemplo, si el procedimiento es una rutina *Read Record,* tal como se define en la norma ISO 7816, se emite en las etapas posteriores el contenido de la zona de memoria intermedia.

La figura 4 representa un procedimiento de lectura en memoria regrabable 6 realizado conforme a una segunda realización de la invención.

Este procedimiento se aplica por ejemplo por la ejecución de las instrucciones de un programa de ordenador por el microprocesador 2.

Como para el procedimiento de la figura 3, el procedimiento aquí descrito recibe en la entrada, en la etapa E402, la dirección ADR en la que debe leer datos en la memoria regrabable 6.

Se procede entonces en la etapa E404 a una verificación del tipo de fichero leído. La etapa E404 puede por ejemplo consistir en leer en la memoria regrabable 6 el encabezamiento del fichero designado por la dirección ADR y verificar que los datos de este encabezamiento corresponden efectivamente a datos indicativos del tipo que debe ser leído por aplicación del procedimiento aquí descrito.

Si el tipo de fichero designado por el encabezamiento no corresponde al tipo de fichero que debe ser leído, se sale del desarrollo normal del procedimiento en la etapa E406 para pasar a la etapa E430 descrita más adelante. Si por el contrario el tipo de fichero es correcto, la etapa E406 envía a la etapa E408 del funcionamiento normal actualmente descrita.

En la etapa E408, se verifica que la lectura en memoria regrabable 6 está autorizada por comparación de los derechos de acceso necesarios especificados en el encabezamiento del fichero con los presentados por el usuario, siendo estas informaciones accesibles en memoria viva 4.

Si la lectura en memoria regrabable 6 no es autorizada según los datos leídos en memoria viva, la verificación de la posibilidad de acceso a esta memoria 6 es negativa y se pasa entonces a la etapa E432 descrita más adelante.

Por el contrario, si se determina en la etapa E410 que el acceso a la memoria regrabable 6 es autorizado, se pasa a la etapa E412 para seguir con el desarrollo normal del funcionamiento de la tarjeta de microcircuito.

Las etapas E404 a E410 proceden de este modo a verificaciones del funcionamiento normal de la tarjeta de microcircuito. Se podrían realizar naturalmente otras verificaciones distintas de las proporcionadas aquí a modo de ejemplos.

La etapa E412 ya mencionada, en la que se procede si las diferentes verificaciones relativas al funcionamiento normal han sido positivas, consiste en leer los datos almacenados en la dirección ADR en la memoria regrabable 6 para almacenarlos en memoria viva 4 para usarlos posteriormente durante un tratamiento de datos efectuado por el microprocesador 2.

Esta etapa provoca por lo tanto accesos de lectura repetidos en la memoria regrabable 6 y accesos de grabación

repetidos en la memoria viva 4.

Una vez terminada la transferencia de los datos de la memoria regrabable 6 a la memoria viva 4 (bien por la lectura de un número fijo de bits en memoria regrabable 6, bien por la lectura del nombre preciso de bits que hay que leer recibidos por ejemplo en la entrada en la etapa E402), se procede a una etapa E414 de verificación de la exactitud de los datos leídos. Para ello, se efectúa por ejemplo una nueva lectura de los datos en la memoria regrabable 6 y una comparación de estos datos con los datos correspondientes almacenados anteriormente en la memoria viva 4 en la etapa E412.

Si se detecta un error durante la comparación, la etapa E416 envía a la etapa E434 descrita más adelante.

Si por el contrario todos los datos han sido leídos correctamente (es decir que la segunda lectura en la memoria regrabable 6 genera datos idénticos a los leídos durante la etapa E412), la etapa E416 lleva a seguir con el funcionamiento normal por la etapa E418 actualmente descrita.

La etapa E418 consiste en devolver a la salida la dirección de almacenamiento en memoria viva de los datos leídos en la memoria regrabable 6, para que los mismos estén disponibles en el funcionamiento normal posterior de manera esquemática representado por la etapa E420 en la figura 4. Cuando se trata de un comando *Read Record* definido por la norma ISO 7816, esta etapa E420 consiste por ejemplo en emitir los datos leídos.

En el caso en el que se ha detectado un tipo de fichero erróneo en la etapa E406, se procede como se indica anteriormente en la etapa E430 de actualización de estado de error E para que el mismo indique un error procedente del tipo de fichero.

La etapa E430 va seguida de la etapa E450, en la que se procede a la lectura de una zona de señuelo en memoria viva 4. La zona de señuelo es por ejemplo una zona dedicada, sin otro uso, que contiene datos dedicados a este uso y que aquí son diferentes por ejemplo de los derechos de acceso relativos a la autorización de lectura en memoria regrabable 6 mencionada en la etapa E408.

Se procede a continuación a la etapa E452 en la que se compara el dato leído en la etapa E450 (es decir el dato leído en la zona de señuelo que se puede por lo tanto denominar "datos de señuelo ") con el valor 0.

Se puede observar que las etapas E450 y E452 no tienen ningún papel funcional en el procedimiento de funcionamiento de la tarjeta, es decir que los datos que son tratados o el resultado de la comparación efectuada no tienen ninguna incidencia sobre las otras partes del procedimiento.

Sin embargo, la realización de estas dos etapas no se distingue, para un observador exterior tal como un atacante que mide los consumos de corriente de la tarjeta de microcircuito, de las operaciones realizadas durante la etapa E408 de funcionamiento normal descritas anteriormente. En efecto, las operaciones de las etapas E408 y E410 que consistían en la lectura de datos en memoria viva y en su comparación tienen una firma similar a las operaciones similares de lectura en memoria viva y de comparación con el valor 0 realizadas en las etapas E450 y E452.

De este modo, en este punto del procedimiento, es imposible para un atacante, determinar por observaciones llevadas desde el exterior que se ha detectado una anomalía en la etapa E406.

La etapa E452 va seguida de la etapa E454 que se describirá más adelante.

En el mismo orden de ideas de lo que se acaba de presentar a propósito de la detección de un tipo de fichero erróneo, se procede como se ha visto en caso de prohibición de acceso en memoria regrabable (etapas E408 y E410) a una etapa E432, en la que se actualiza el estado de error E para indicar que el error procede de una prohibición de lectura de la memoria regrabable 6.

La etapa E432 va asimismo seguida de la etapa E454 ya mencionada y que se va a describir actualmente.

En la etapa E454, el procedimiento realiza acciones de lectura en una zona de señuelo de la memoria regrabable 6 y acciones de grabación en una zona de señuelo de la memoria viva 4.

Como se ha indicado anteriormente, las zonas de señuelo en las memorias 4, 6 son zonas de estas memorias en las que se graban datos que no tienen ninguna función particular durante el funcionamiento normal. Los accesos de lectura o de grabación a estas zonas de señuelo permiten sin embargo simular, para un observador exterior del desarrollo del procedimiento, las etapas realizadas durante el funcionamiento normal por ejemplo en la etapa E412, sin consecuencias sobre los datos usados, por otra parte, por el procedimiento o sobre la seguridad del mismo.

La etapa E454 va seguida de una etapa E456 de lectura de zonas de señuelo tanto en la memoria viva 4 como en la memoria regrabable 6. Como se ha indicado anteriormente, estos acceso de lectura no tienen ningún carácter funcional en el funcionamiento normal del programa (es decir que los datos leídos en las zonas de señuelo no se utilizan en otras partes del procedimiento). Sin embargo, para un atacante que intenta conocer el funcionamiento interno del

procedimiento mediante observaciones (por ejemplo del consumo eléctrico del microprocesador o de las memorias 4, 6), las etapas E454 y E456 generan firmas que son similares respectivamente a las firmas generadas por las etapas E412 y E414 durante el funcionamiento normal.

De este modo, en este punto del procedimiento, es imposible para un atacante, determinar por observación externa del funcionamiento de la tarjeta de microcircuito, si el procedimiento realiza las etapas E412 y E414 del funcionamiento normal, o las etapas E454 y E456 posteriores a la detección de una anomalía de funcionamiento (ya sea una anomalía debida a un tipo de fichero erróneo o una salida del funcionamiento normal por prohibición de acceso a la memoria regrabable 6).

Al igual que las etapas E450 y E452, las etapas E454 y E456 no son etapas de tratamiento de la anomalía detectada, ya que estas etapas trabajan con datos de señuelo, sin pretender solucionar un error funcional, ni llevar a cabo una contramedida para el caso en el que la anomalía procede de un ataque por generación de fallo.

La etapa E456 va seguida de la etapa E458 descrita más adelante.

En la hipótesis formulada más arriba donde la verificación de la exactitud de los datos leídos en la etapa E412 por la etapa E414 es negativa, la etapa E416 va seguida de la etapa E434 de actualización del estado de error E para que el mismo indique que el error detectado procede de un error durante la lectura en la memoria regrabable 6.

La etapa E434 va seguida entonces de la etapa E458 ya mencionada y actualmente descrita.

La etapa E458 consiste en emitir el estado de error tal como ha sido determinado durante una etapa anterior (es decir durante una de las etapas E430, E432 y E434). Esta emisión del código de error puede ser realizada con destino a otro procedimiento (u otra parte de procedimiento) aplicado en la tarjeta de microcircuito. Por ejemplo, si el procedimiento representado en la figura 4 representa un subprograma ejecutado cuando el programa principal de gestión del funcionamiento de la tarjeta de microcircuito requiere una lectura en la memoria regrabable 6, la etapa E458 puede consistir en devolver el valor del estado de error al programa principal.

En una variante, la emisión del estado de error en la etapa E458 puede dirigirse al terminal de usuario a través de la interfaz 8.

El procedimiento representado en la figura 4 incluye de este modo dos ramas principales:

- una primera rama que corresponde al desarrollo normal del procedimiento (etapas E402 a E420);

- una segunda rama compuesta por etapas en las que una parte al menos se realiza después de que se haya detectado una anomalía (etapas E450 a E458).

Como se ha visto, una gran parte de las etapas de la primera rama es simulada, en caso de detección de anomalía, por una etapa correspondiente de la segunda rama. Para ello, la etapa correspondiente en la segunda rama usa una instrucción del mismo tipo que la etapa correspondiente en la primera rama, en su caso aplica una comunicación con un dispositivo idéntico al usado en la etapa correspondiente de la primera rama, para generar para un atacante la misma firma, en términos de consumo eléctrico o de radiación electromagnética por ejemplo.

La figura 5 representa un procedimiento aplicado en una tarjeta de microcircuito del tipo monedero electrónico (a veces denominado por el nombre inglés *purse*) según las enseñanzas de una tercera realización de la invención.

Este procedimiento se aplica por ejemplo mediante la ejecución de un programa constituido por instrucciones en el seno del microprocesador 2 de la tarjeta de microcircuito.

La figura 5 representa las etapas principales del procedimiento aplicado para pagar con el monedero electrónico, es decir modificar el dato almacenado en la tarjeta de microcircuito que represente el valor del monedero electrónico en el sentido de un aumento de este valor.

Este procedimiento empieza por lo tanto en la etapa E502, en la que el microprocesador 2 de la tarjeta de microcircuito 10 recibe del usuario (a través de la interfaz 8) un código de control de crédito C, el importe a abonar M y una firma S, como se representa en la etapa E502.

Como se verá a continuación, la firma S permite garantizar que el usuario dispone efectivamente de una autorización para efectuar este crédito; efectivamente, sin esta precaución, cualquiera podría solicitar el aumento del valor del monedero electrónico, lo cual no es evidentemente aceptable.

Ahora se describirán las etapas aplicadas durante el funcionamiento normal del procedimiento de crédito del monedero electrónico.

En la etapa E504, que sigue a la etapa E502 durante el funcionamiento normal, el microprocesador controla la lectura en la memoria regrabable 6 de una clave K especificando la dirección de almacenamiento de esta clave en la memoria regrabable 6. La clave K almacenada en la memoria regrabable 6 es secreta y no es por lo tanto accesible desde el exterior.

El microprocesador 2 procede entonces a la etapa E506 de envío de la clave secreta K leída en la memoria regrabable 6 y del código de control C a un criptoprocesador (non representado en la figura 1). El criptoprocesador efectúa un cálculo criptográfico a partir de los datos recibidos (clave secreta K, código de control C) según algoritmos clásicos en criptografía, por ejemplo el algoritmo DES. Más en concreto, se aplica aquí un algoritmo al código de control C usando la clave secreta K, para obtener una firma calculada S1.

El criptoprocesador devuelve entonces al microprocesador 2 la firma calculada S1 (etapa E508).

Si el usuario que controla la ejecución del procedimiento es efectivamente autorizado a realizar el crédito, tiene asimismo conocimiento de la clave secreta K y ha podido por consiguiente determinar la firma S de manera idéntica al cálculo que se acaba de realizar para calcular la firma S1.

Por este motivo en la etapa E se compara la firma recibida del usuario S con la firma calculada S1 basándose en la clave secreta K almacenada en la tarjeta de microcircuito, lo cual permite determinar si la grabación del crédito es autorizada.

De este modo, si la comparación entre S y S1 es positiva en la etapa E510, se procede a la etapa E512 en la que se graba el importe a abonar M, o en una variante el valor del monedero electrónico resultante de este crédito, en la memoria regrabable 6.

Sin embargo, si se determina en la etapa E510 que la firma S recibida del usuario no se corresponde con la firma calculada S1, no se puede autorizar el crédito del monedero electrónico y se procede entonces a la etapa E514, por la cual el microprocesador 2 emite hacia el terminal de usuario un estado de error.

Se acaban de describir las principales etapas de un procedimiento de crédito de un monedero electrónico. Naturalmente, para asegurar un funcionamiento seguro de este procedimiento, estas etapas principales están separadas por etapas de verificación del desarrollo normal del procedimiento, que permiten por diferentes pruebas detectar por una parte errores funcionales y por otra parte ataques, por ejemplo por generación de fallo.

En caso de detección de un ataque, el microprocesador 2 procede a etapas diferentes de las del funcionamiento normal, como se describe ahora. Según una variante eventualmente compatible con lo que se describe a continuación, el procedimiento puede asimismo aplicar estas etapas diferentes (u otras etapas diferentes del funcionamiento normal) si se detecta un error funcional (en lugar de un ataque).

Como se ha representado en línea de puntos en la figura 5, si se detecta un ataque entre la etapa E502 de recepción de los datos y la etapa E504 de lectura de la clave secreta K en la memoria regrabable 6, se procede a la etapa E520, en la que se lee en la memoria regrabable 6 datos en una dirección K' que constituye una zona de señuelo que corresponde a la zona que contiene la clave secreta K leída en la etapa E504 durante el funcionamiento normal.

De este modo, si un atacante genera un ataque por fallo que es detectado por el microprocesador 2, se procede a la etapa E520 cuya firma eléctrica o electromagnética (tal como se observa por el atacante) es similar a la de la etapa E504 realizada en funcionamiento normal. El atacante piensa de este modo que su ataque no ha sido detectado y que el microprocesador 2 lee efectivamente en la memoria regrabable 6 la clave secreta K.

Después de la etapa E520, se procede a la etapa E522. Se procede asimismo a esta etapa E522 si un ataque es detectado por etapas de verificación del desarrollo normal del procedimiento situadas entre las etapas E504 y E506 descritas anteriormente.

La etapa E522 consiste en enviar al criptoprocesador (mencionado anteriormente en lo que se refiere a las etapas E506 y E508) datos C' y K' que constituyen datos de señuelo. De este modo, la etapa E522 no tiene ningún carácter funcional particular, pero simula la realización de la etapa E506 para un atacante que observa el funcionamiento de la tarjeta de microcircuito 10 por el simple estudio de los consumos eléctricos o de la radiación electromagnética generados por esta tarjeta.

En el caso en el que la etapa E522 ha sido precedida por la etapa E520, el dato de señuelo K' puede ser el dato leído durante la etapa E520. En una variante, puede tratarse de un dato predeterminado y preferiblemente de un dato sin relación con el funcionamiento seguro de la tarjeta de microcircuito 10.

Como anteriormente, al ser la firma de la etapa E522 similar a la de la etapa E506 realizada en funcionamiento normal, un atacante ignora cuando se ejecuta la etapa E522 que su ataque ha sido de hecho detectado.

La etapa E522 va seguida por la etapa E524 descrita más adelante.

Como anteriormente, las etapas E506 y E508 pueden estar separadas por etapas de verificación del funcionamiento normal del procedimiento susceptibles de detectar un ataque, como se representa en línea de puntos en la figura 5. En caso de detección de ataque, el procedimiento sigue asimismo en la etapa E524.

La etapa E524 consiste en recibir una firma calculada por el criptoprocesador. Como anteriormente para las etapas E520 y E522, la etapa E524 permite simular una etapa del funcionamiento normal (aquí la etapa E508) para hacer indetectable para un atacante el hecho de que su ataque anterior ha sido detectado.

En el caso en el que se ha procedido anteriormente a la etapa E522, la firma S1' es por ejemplo la firma calculada por el criptoprocesador sobre la base de los datos C' y K' transmitidos durante la etapa E522. En este caso, la firma calculada S1' no tiene ningún carácter funcional ya que está basada sobre datos de señuelo.

Cuando el procedimiento llega a la etapa E524 después de la detección de un ataque entre las etapas E506 y E508, la etapa E524 puede por ejemplo consistir en la recepción efectiva de solo una parte de la firma calculada por el criptoprocesador sobre la base de los datos C y K emitidos en la etapa E506. El resto de la firma S1' es por ejemplo forzado a un valor predeterminado, de manera que el resultado obtenido (firma S1') no corresponde a la firma S1 para preservar la seguridad del funcionamiento de la tarjeta de microcircuito.

La etapa E524 va seguida de la etapa E526 en la que se efectúa por ejemplo una comparación del valor S1' que se acaba de determinar con la misma. Como anteriormente, esta etapa no tiene ningún carácter funcional (ya que el resultado de la comparación de un número con él mismo es evidentemente conocido por adelantado), pero permite simular la realización de la etapa E510 para un atacante que observa el comportamiento eléctrico y/o electromagnético de la tarjeta de microcircuito 10. En efecto, las etapas E526 y E510 que aplican la misma instrucción, tienen firmas eléctricas (y electromagnéticas) muy similares.

De este modo, si se ha detectado un ataque entre las etapas E502 y E508 del funcionamiento normal, el funcionamiento normal se ha interrumpido (por el paso a las etapas de señuelo E520 a E526) sin que sin embargo este cambio sea detectable por un atacante.

La etapa E526 va seguida de la etapa E528 en la que se graban datos de bloqueo (o cerrojo) en la memoria regrabable 6.

Como ya se ha mencionado a propósito de la primera realización descrita con referencia a la figura 3, la grabación de datos de bloqueo en la memoria regrabable 6 impide cualquier uso posterior de la tarjeta de microcircuito 10. Se trata, por lo tanto de una contramedida particularmente severa y eficaz en respuesta a la detección de un ataque.

Se observa, además, que la etapa E528 se realiza en un momento en que el funcionamiento normal habría realizado la etapa E512 de grabación del importe en memoria regrabable 6. De este modo, en un primer momento, la etapa E528 es confundida por el atacante con la etapa E512 del funcionamiento normal que posee la misma firma eléctrica y/o electromagnética, especialmente porque las etapas E512 y E528 corresponden a instrucciones del mismo tipo que realizan ambas una comunicación del microprocesador 2 con la memoria regrabable 6.

Como es bien visible en la figura 5, la etapa E512 y las etapas anteriores del funcionamiento normal tienen cada una una etapa de firma similar aplicada en caso detección de un ataque. Especialmente, la etapa E512 de grabación del importe en la memoria regrabable 6, que constituye una etapa importante en la aplicación del procedimiento, está asociada a la etapa E528 de grabación de los datos de bloqueo, que constituye en concreto la contramedida en caso de detección de un ataque contra este procedimiento.

De este modo, no solo un atacante no puede determinar la detección de su ataque a causa de las etapas E520 a E526 que simulan un funcionamiento normal, sino que la contramedida (aquí la grabación de los datos de bloqueo) se realiza, además, con una cronología tal que es confundida con una etapa del funcionamiento normal que tiene una firma eléctrica y/o electromagnética similar.

Los ejemplos que se acaban de describir solo son posibles realizaciones de la invención.

REIVINDICACIONES

1.- Procedimiento de seguridad en un dispositivo que aplica un procedimiento de tratamiento de datos que comprende:

- una etapa de verificación de un criterio indicativo del desarrollo normal del procedimiento de tratamiento de datos, y

- una etapa de tratamiento (E528) efectuada en caso de verificación negativa;

en el que se realiza una primera acción (E512) de grabación de datos en una memoria física (6) en caso de verificación positiva, en el que la etapa de tratamiento (E320; E528) incluye una segunda acción de grabación de datos en la memoria física (6) y en el que la grabación (E528) de datos de la segunda acción se lleva a cabo en el momento en el que se realizaría la grabación (E512) de datos de la primera acción en caso de desarrollo normal del procedimiento, caracterizado porque dicha segunda acción de grabación de datos incluye al menos una de entre:

- una grabación de datos de bloqueo que impide un uso posterior de dicho dispositivo,

- una grabación de datos representativos de una anomalía detectada en caso de verificación negativa, permitiendo dichos datos representativos de una anomalía detectada un análisis de un problema encontrado por dicho dispositivo.

2.- Procedimiento según la reivindicación 1, que incluye, además, una etapa de bloqueo de dicho dispositivo que impide un uso posterior, tras dicho análisis.

3.- Procedimiento según una de las reivindicaciones anteriores, en el que dicha grabación de datos representativas de una anomalía detectada incluye la actualización de un indicador.

4.- Procedimiento según una de las reivindicaciones anteriores, en el que dicha seguridad pretende la protección de dicho dispositivo contra ataques.

5.- Procedimiento según una de las reivindicaciones anteriores, en el que dicha primera acción de grabación se refiere a primeros datos propios del desarrollo normal de dicho procedimiento y dicha segunda acción de grabación se refiere a segundos datos propios del desarrollo anormal del procedimiento.

6.- Procedimiento según la reivindicación 5, en el que dicha primera acción de grabación incluye la actualización de un primer dato propio del desarrollo normal de dicho procedimiento y dicha segunda acción de grabación se refiere a la actualización de un segundo dato propio del desarrollo anormal del procedimiento.

7.- Procedimiento según una de las reivindicaciones 1 a 6, en el que la segunda acción es diferente de la primera acción.

8.- Procedimiento según una de las reivindicaciones 1 a 7, en el que, al estar realizada una tercera acción (E418; E512) en caso de verificación positiva, la etapa de tratamiento comprende la realización de al menos una cuarta acción (E458; E528).

9.- Procedimiento según la reivindicación 8, en el que la tercera acción aplica una instrucción del mismo tipo que la cuarta acción.

10.- Procedimiento según la reivindicación 8, en el que la tercera acción comprende un acceso a una primera zona de una memoria, la cuarta acción comprende un acceso a una segunda zona de dicha memoria diferente de la primera zona.

11.- Procedimiento según la reivindicación 10, en el que dicha primera zona contiene una clave secreta.

12.- Procedimiento según la reivindicación 8, en el que la cuarta acción aplica una comunicación con un dispositivo externo idéntico al utilizado en la tercera acción.

13.- Procedimiento según la reivindicación 12, en el que el dispositivo externo es un criptoprocesador.

14.- Procedimiento según la reivindicación 12, en el que el dispositivo externo es una memoria (2, 6).

15.- Procedimiento según la reivindicación 12, en el que el dispositivo externo es una memoria regrabable de semiconductor (6).

16.- Procedimiento según la reivindicación 12, en el que el dispositivo externo es un terminal de usuario.

17.- Procedimiento según una de las reivindicaciones 1 a 16, en el que la primera acción incluye una etapa segura.

18.- Procedimiento según la reivindicación 17, en el que la etapa segura incluye un algoritmo criptográfico.

19.- Procedimiento según una de las reivindicaciones 1 a 18, en el que los datos representan un valor pecuniario.

20.- Procedimiento según una de las reivindicaciones 1 a 19, en el que el criterio es negativo si se proporciona una firma errónea.

21.- Procedimiento según una de las reivindicaciones 1 a 20, en el que el criterio es negativo si se detecta una anomalía.

22.- Procedimiento según una de las reivindicaciones 1 a 21, en el que el criterio es negativo si se detecta un ataque.

23.- Procedimiento según una de las reivindicaciones 1 a 22, en el que el criterio es negativo si se detecta un error funcional.

24.- Procedimiento según una de las reivindicaciones 1 a 23, aplicado por un microprocesador (2) de una tarjeta de microcircuito (10).

25.- Dispositivo de tratamiento de datos que comprende:

- medios de verificación de un criterio indicativo del funcionamiento normal del dispositivo; y

- medios de tratamiento aplicados en caso de verificación negativa, en el que primeros medios de acción de grabación de datos en una memoria física se aplican en caso de verificación positiva, y en el que los medios de tratamiento son capaces de grabar datos en la memoria física en el momento en que sería realizada la grabación de datos en la memoria física por los primeros medios de acción en caso de desarrollo normal del procedimiento, caracterizado porque los medios de tratamiento son capaces de grabar datos entre:

- datos de bloqueo que impiden un uso posterior de dicho dispositivo, y

- datos representativos de una anomalía detectada en caso de verificación negativa, permitiendo dichos datos representativos de una anomalía detectada un análisis de un problema encontrado por dicho dispositivo.

26. Dispositivo según la reivindicación 25, siendo el dispositivo una tarjeta de microcircuito.

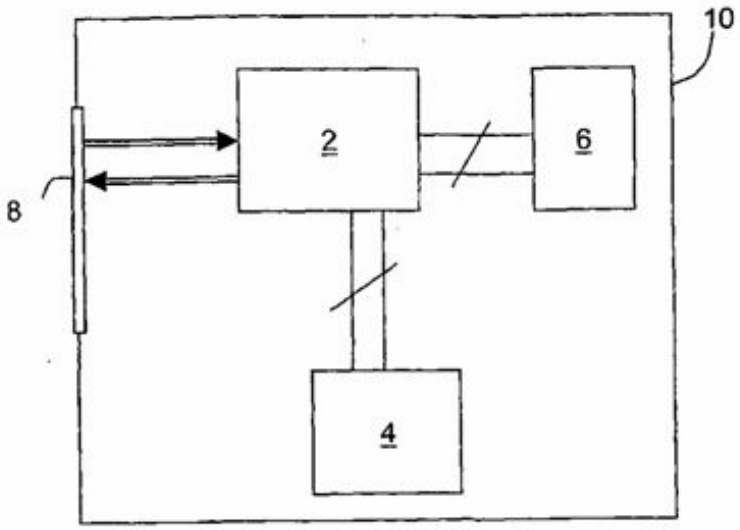

Figura 1

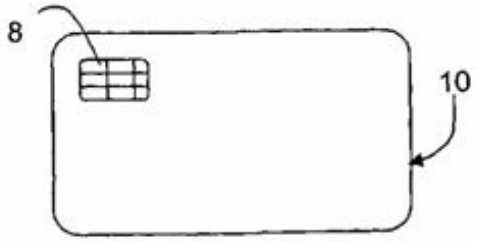

Figura 2

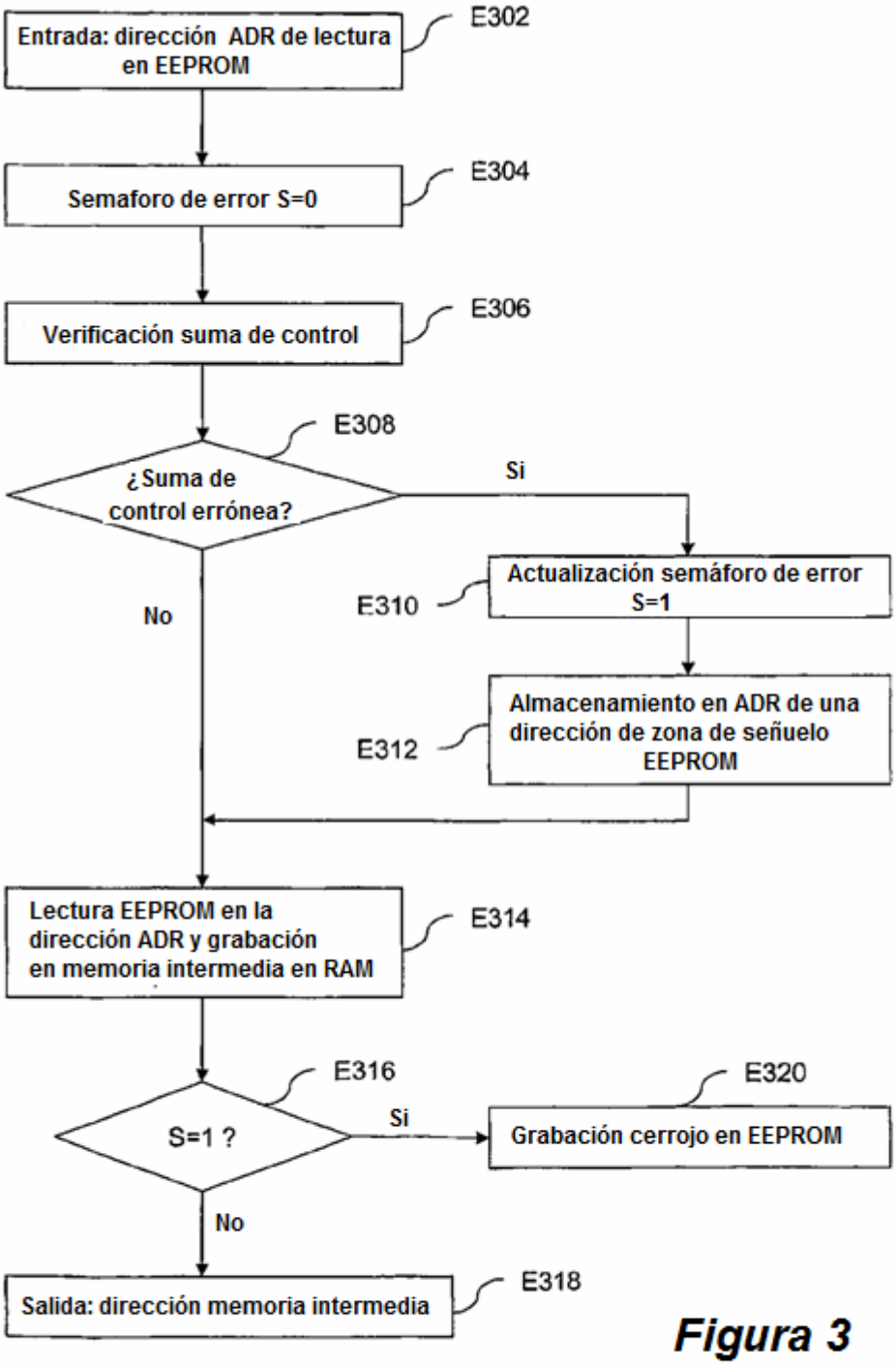
Entrada: dirección ADR de lectura en EEPROM
E302
Semaforo de error S=0
E304
Verificación suma de control
E306
E308
¿Suma de control errónea?
Si
No
E310
Actualización semáforo de error S=1
E312
Almacenamiento en ADR de una dirección de zona de señuelo EEPROM
Lectura EEPROM en la dirección ADR y grabación en memoria intermedia en RAM
E314
E316
S=1 ?
Si
E320
Grabación cerrojo en EEPROM
No
Salida: dirección memoria intermedia
E318

Figura 3

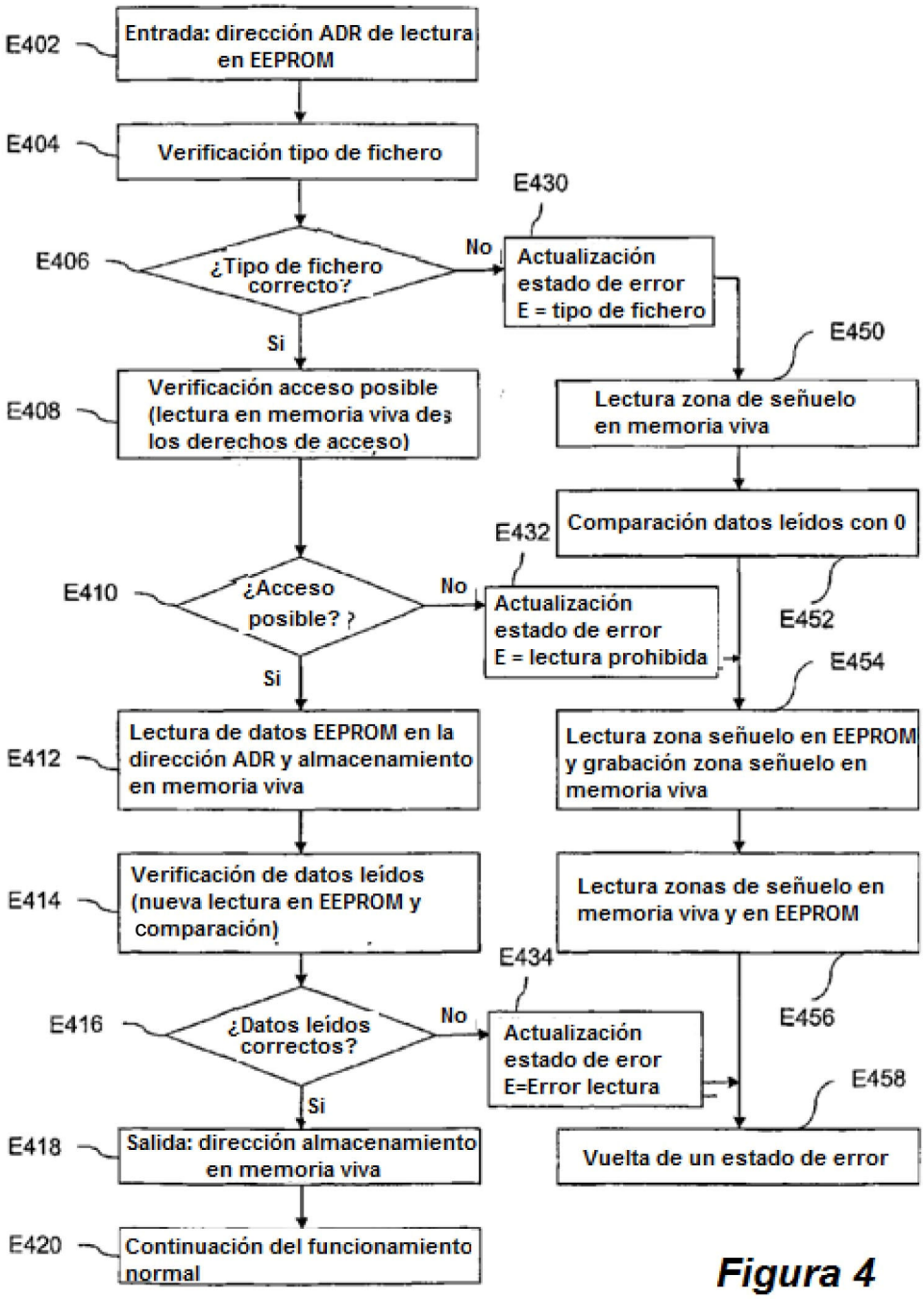
E402
Entrada: dirección ADR de lectura en EEPROM
E404
Verificación tipo de fichero
E406
¿Tipo de fichero correcto?
No
Si
E430
Actualización estado de error E = tipo de fichero
E408
Verificación acceso posible (lectura en memoria viva des los derechos de acceso)
E450
Lectura zona de señuelo en memoria viva
Comparación datos leídos con 0
E432
E410
¿Acceso posible? ?
No
Si
Actualización estado de error E = lectura prohibida
E452
E454
E412
Lectura de datos EEPROM en la dirección ADR y almacenamiento en memoria viva
Lectura zona señuelo en EEPROM y grabación zona señuelo en memoria viva
E414
Verificación de datos leídos (nueva lectura en EEPROM y comparación)
Lectura zonas de señuelo en memoria viva y en EEPROM
E434
E416
¿Datos leídos correctos?
No
Si
Actualización estado de eror E=Error lectura
E456
E458
E418
Salida: dirección almacenamiento en memoria viva
Vuelta de un estado de error
E420
Continuación del funcionamiento normal

Figura 4

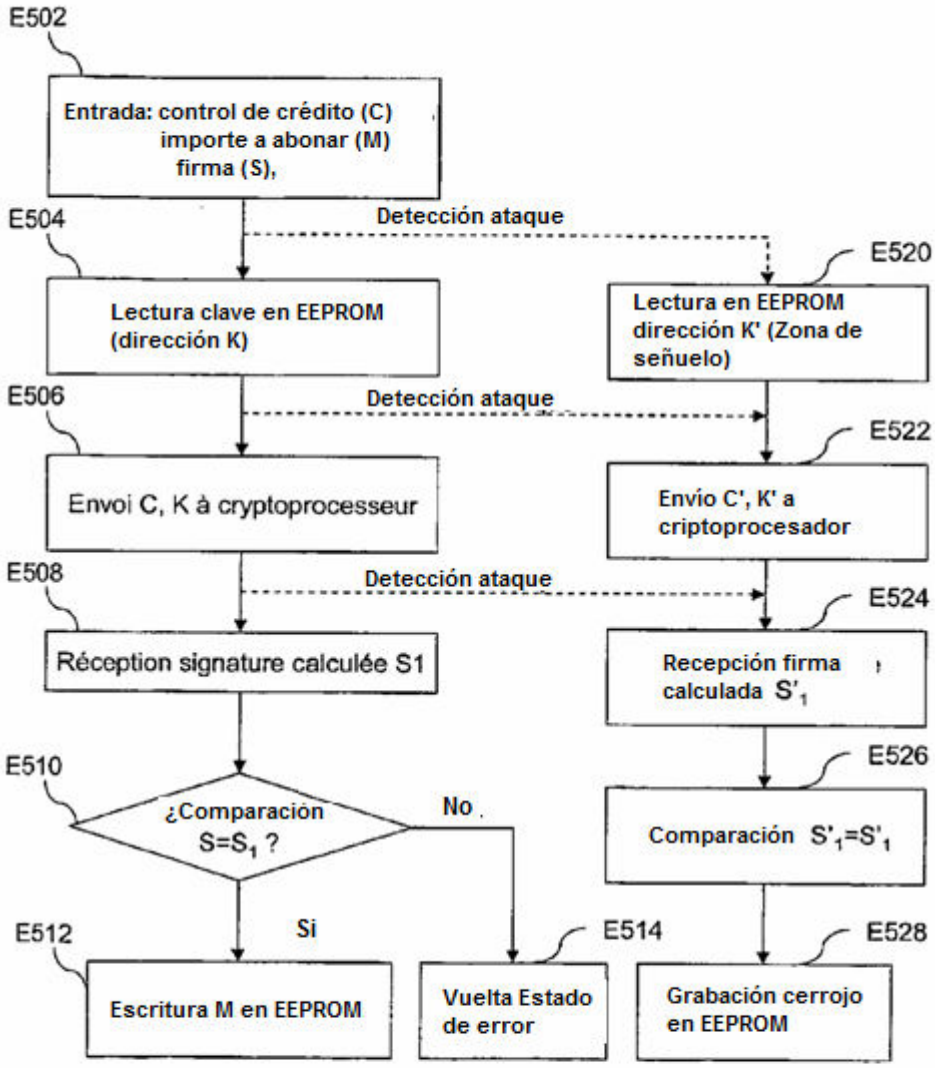
E502
Entrada: control de crédito (C)
importe a abonar (M)
firma (S),
E504
Detección ataque
E520
Lectura clave en EEPROM (dirección K)
Lectura en EEPROM dirección K' (Zona de señuelo)
E506
Detección ataque
E522
Envoi C, K à cryptoprocesseur
Envío C', K' a criptoprocesador
E508
Detección ataque
E524
Réception signature calculée S1
Recepción firma calculada S'1
E526
E510
¿Comparación S=S1 ?
No
Comparación S'1=S'1
Si
E512
E514
E528
Escritura M en EEPROM
Vuelta Estado de error
Grabación cerrojo en EEPROM

Figura 5