(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 792 173**

(51) Int. CI.:

G06F 21/57 (2013.01)
G06F 21/77 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.12.2007 E 07124045 (1)**

(97) Fecha y número de publicación de la concesión europea: **26.02.2020 EP 1942428**

(54) Título: **Procedimiento de verificación de conformidad de una plataforma electrónica y/o un programa informático presente en esta plataforma, dispositivo y programa de ordenador correspondientes**

(30) Prioridad:

22.12.2006 FR 0611348

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.11.2020

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

NACCACHE, M DAVID

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de verificación de conformidad de una plataforma electrónica y/o un programa informático presente en esta plataforma, dispositivo y programa de ordenador correspondientes

1.Campo del invento

El campo del invento es el de la lucha contra la falsificación de objetos de un microprocesador protegido, llamado a partir de ahora plataforma electrónica o chip electrónico, y/o de programas destinados a estar integrados en tales objetos con chip electrónico.

El invento se refiere de una manera más particular a la detección del fraude, de la tentativa de fraude o de cualquier otra acción ilegal con la ayuda de objetos con chip copiados, imitados o clonados, o que llevan un programa no auténtico, por ejemplo, malignos (virus, caballo de Troya…).

El invento se aplica especialmente a las tarjetas con chips. Se describen, por lo tanto, a continuación, esencialmente tales tarjetas con chips, pero el invento puede ser utilizado fácilmente para cualquier tipo de objetos, especialmente, portátiles, equipados con tal chip, cualquiera que sea la naturaleza de este último.

2. Técnica anterior

2.1 Las tarjetas con chip

Se utilizan desde hace mucho tiempo tarjetas con chip, especialmente para identificar o autentificar un producto, una cuenta y/o a una persona. El chip, o el microprocesador, presenta, por lo tanto, una estructura específica de los transistores, definiendo una lógica de tratamiento y de zonas de memoria, de las cuales una parte al menos está protegida, conteniendo datos secretos.

2.2 Detección de tarjetas clonadas

Una tarjeta con chip, utilizada, por ejemplo, como medio de pago, incluye, por lo tanto, un circuito electrónico, llamado chip electrónico, en el cual el comportamiento lógico de la tarjeta, es decir, las respuestas a las diversas solicitudes que pueda recibir, está programado. Tal circuito electrónico puede incluir, especialmente, unos componentes electrónicos sencillos (transistores, amplificadores operacionales), unos componentes complejos (microprocesadores, memorias) y unos componentes numéricos (puertos lógicos), combinados entre sí por una lógica de creación de los componentes, para efectuar las operaciones para las que está concebida la tarjeta.

Existen métodos de detección de las tarjetas con chip no conformes, basados en una verificación del comportamiento lógico de la tarjeta a testar.

Estos métodos permiten verificar que el comportamiento programado de la tarjeta es el correcto. Sin embargo, no permiten detectar a una tarjeta clonada.

En efecto, una tarjeta con chip clonada, si ha sido programada eficazmente, presenta el mismo comportamiento lógico que una tarjeta con chip “legítima” (es decir puesta en el mercado por fabricantes hábiles de tarjetas con chip). Se distingue, por lo tanto, por su constitución, puesto que no incluye el mismo circuito electrónico, pero no por su comportamiento.

Es efectivamente muy difícil para un falsificador hacerse con circuitos electrónicos legítimos, estando reservada su difusión a los fabricantes de tarjetas. Sin embargo, un falsificador que haya extraído de una tarjeta legítima las informaciones que le permitan reproducir su comportamiento lógico, puede programar un circuito electrónico comprado en el comercio para producir una tarjeta clonada.

Tal tarjeta clonada es difícilmente diferenciable de una tarjeta legítima, al ser idénticos sus comportamientos lógicos. Se diferencian únicamente por la “jungla” de transistores que las constituyen. Sin embargo, estas “junglas” no son fácilmente analizables, por una parte, porque son no interpretables (se trata del resultado de un tratamiento informático cuyo aspecto es aleatorio), y por otra parte, porque la comparación necesitaría la destrucción de las tarjetas y el uso de unos medios costosos tales como microscopios electrónicos.

De esta manera, es actualmente posible controlar el comportamiento lógico de una tarjeta con chip, pero no existe a día de hoy ningún método eficaz de detección capaz de detectar las tarjetas con chip clonadas, que tienen el mismo comportamiento lógico, pero componentes diferentes

WO 00/17826 A1 y US 5 570 012 A describen unos procedimientos para testar la autenticidad de una plataforma electrónica.

2.3 Detección de un programa maligno

Existen igualmente tarjetas con chip cuyo programa es falsificado de tal manera que induce a un comportamiento particular de la tarjeta como respuesta a una solicitud predefinida por un defraudador (por ejemplo, efectuar una transacción no autorizada o acceder a unos datos protegidos que permitan producir a continuación unas tarjetas clonadas).

Tales programas, llamados programas corrompidos o malignos, pueden resultar casi indetectables por un método clásico de detección de un comportamiento lógico de una tarjeta.

En efecto, el comportamiento maligno de tales programas se activa muy a menudo por una solicitud particular (por ejemplo, una secuencia binaria de gran longitud y sin ningún significado para el programa “normal”) que no puede ser detectada en las condiciones de tiempo y de recursos de los que disponen los métodos de detección existentes, pero que pueden activar un comportamiento particular pre-programado por el falsificador.

Existen, por ejemplo, métodos de detección de programas malignos basados en la retro-ingeniería, es decir, en la restitución y la verificación del programa contenido en una tarjeta a testar.

Sin embargo, algunos de estos programas malignos tienen la facultad de “contratacar” a estos métodos de detección basados en la retro-ingeniería, y de aparecer, así como unos programas legítimos.

Otra técnica de lucha contra estos programas malignos o corrompidos puede consistir en borrar el programa contenido en una tarjeta y reemplazarlo por un programa legítimo.

Sin embargo, es más, algunos programas malignos tienen la facultad de comportarse como si estuviesen efectivamente anulados de una manera total por un nuevo programa mientras que en realidad están siempre presentes en la tarjeta y prestos para ser activados.

No existe, por lo tanto, a día de hoy ningún método eficaz de detección de un programa maligno en una tarjeta con chip.

3. Objetivos del invento

El invento tiene como objetivo, especialmente, paliar al menos algunos inconvenientes de la técnica anterior.

De una manera más precisa, un objetivo del invento, según al menos un modo de realización, es el de detectar un objeto con chip clonado, de una manera sencilla y eficaz.

Otro objetivo del invento, según al menos otro modo de realización, es el de detectar un programa corrompido, o maligno, en un objeto con chip, de una manera sencilla y eficaz.

Especialmente, el invento tiene como objetivo proporcionar una técnica tal que presente mejores prestaciones en términos de eficacia de detección de objetos con chip clonados y/o de programas malignos, en términos de recursos a utilizar para tales detecciones y en términos del tiempo necesario para tales detecciones.

De esta manera, un objetivo del invento es el de proporcionar una técnica tal que, pueda ser utilizada con un coste reducido en un terminal, por ejemplo, en el local de un comerciante, y que permita un control en algunos segundos.

4. Exposición del invento

El invento propone una solución nueva que no presente al menos algunos de estos inconvenientes de la técnica anterior, bajo la forma de un procedimiento de verificación de una conformidad de una plataforma electrónica, llamada plataforma a testar, y/o de un programa informático a testar presente en la citada plataforma a testar.

Según el invento, el procedimiento incluye una etapa de transmisión, por parte de un dispositivo de verificación, de un mismo juego de informaciones, por una parte, a la citada plataforma a testar y, por otra parte, a una plataforma de referencia de conformidad presente en el citado dispositivo de verificación, y una etapa de decisión de conformidad de la citada plataforma a testar y/o del citado programa informático a testar, en función de un análisis de los comportamientos respectivos de la citada plataforma a testar y de la citada plataforma de referencia, teniendo en cuenta en el citado análisis una correlación entre al menos dos señales representativas de la medidas de la corriente efectuadas simultánea o secuencialmente de una manera respectiva en la citada plataforma a testar y en la citada plataforma de referencia, en un periodo de medidas predeterminado.

De esta manera, el invento permite verificar la conformidad de una plataforma a testar y/o de un programa a testar en una plataforma a testar, analizando su comportamiento, lógico y físico, y el de la plataforma de referencia, en las mismas condiciones del test.

En un primer momento, el dispositivo de verificación transmite las mismas informaciones a las dos plataformas, y sigue su comportamiento según unos criterios predeterminados (tiempo de respuesta, consumo de corriente,

radiación electromagnética,.), y en un segundo momento, el dispositivo de verificación decide las conformidad de la plataforma a testar y/o del programa informático a testar, en función del análisis de los comportamientos de las dos plataformas durante la verificación. Para ello, el dispositivo de verificación efectúa unas medidas de la corriente simultánea o secuencialmente en la plataforma a testar y en la plataforma de referencia y a continuación compara las señales representativas de estas medidas de la corriente.

Según el invento, la citada comparación incluye una correlación entre las citadas señales en un periodo de tiempo predeterminado.

En otras palabras, según el invento, no se tienen en cuenta (únicamente) unas respuestas (resultados de los tratamientos lógicos) proporcionadas por las plataformas, sino su comportamiento, o su funcionamiento, su interacción con el entorno. Se puede asimilar esta aproximación a la del detector de mentiras, que no tiene en cuenta solamente la respuesta formulada, sino un análisis del comportamiento biológico y gestual del individuo.

En efecto, un principio del procedimiento de verificación según el invento se basa en la siguiente observación: una plataforma a testar, o una plataforma que tenga un programa a testar, y una plataforma de referencia tienen unos comportamientos “eléctricos” comparables cuando están sometidos a las mismas condiciones de utilización.

En particular, los consumos de la corriente en las dos plataformas deben presentar unas variaciones comparables si la plataforma a testar es conforme, y, al contrario, las dos plataformas presentan unas variaciones completamente diferentes si la plataforma a testar no es conforme.

El dispositivo de verificación se basa en una correlación de las señales representativas de las medidas de la corriente en las dos plataformas para proporcionar su decisión de conformidad. Esta correlación se efectúa en un periodo predeterminado, definido de una manera que hace óptima la verificación de conformidad. Este periodo puede ser función igualmente de una tasa de errores máxima por parte del procedimiento, y/o de un tiempo máximo aceptado para proporcionar la decisión de conformidad.

Una correlación permite observar diferencias de consumo de la corriente entre una plataforma no conforme y una plataforma conforme, teniendo en cuenta al mismo tiempo eventuales diferencias de consumo de la corriente debidas a la fabricación de los componentes de las plataformas, en el caso de dos plataformas conformes. De esta manera, una comparación estricta entre las señales mostrará unas diferencias o unas adquisiciones de los valores, mientras que una correlación mostrará unas diferencias o unas similitudes en las variaciones, teniendo en cuenta así eventuales diferencias de los valores debidas a la fabricación de los componentes.

En particular, la citada correlación utiliza al menos uno de los cálculos que pertenecen al grupo que incluye:

- un cálculo de la correlación temporal;

- un cálculo de la correlación frecuencial.

Además, según un aspecto particular del invento, las citadas medidas de la corriente sufren al menos uno de los tratamientos previos que pertenecen al grupo que incluye:

- los filtrados;

- las numeraciones;

- las transformaciones matemáticas;

- las amplificaciones.

De esta manera, según los medios utilizados en el dispositivo de verificación, la estructura de las señales de medida y los resultados esperados en términos de eficacia del procedimiento de verificación, serán adaptadas las medidas de la corriente antes de ser utilizadas en un cálculo de correlación. Un tratamiento complejo y particular de estas medidas permite una mayor fiabilidad del procedimiento de verificación. Presenta la ventaja igualmente de hacer más compleja la tares de un falsificador que intentase realizar una copia de una plataforma. Esta complejidad puede ser aumentada todavía más haciendo variar algunos tratamientos de una manera aleatoria (por ejemplo, los instantes o las frecuencias tenidas en cuenta).

Según un aspecto del invento, las citadas medidas de la corriente son efectuadas sobre las alimentaciones respectivas de las citadas plataformas a testar y de la plataforma de referencia. En efecto, la alimentación de tales plataformas es en general fácilmente accesible e identificable en el circuito electrónico, lo que permite efectuar las medidas de la corriente en los mismos lugares en las dos plataformas, garantizando así uno de los criterios de similitud de las condiciones del test para las dos plataformas.

Según otro aspecto del invento, el procedimiento de verificación incluye una etapa de estabilización del consumo de la corriente de las citadas plataformas a testar y de la plataforma de referencia, previa al citado análisis.

De esta manera, con el fin de asegurar la validez de las medidas de la corriente efectuadas en cada una de las plataformas, el consumo de corriente se estabiliza en cada una de las plataformas, que se encuentran, por lo tanto, a continuación, en unas etapas físicas, o eléctricas, similares.

En efecto, cada tares efectuada por uno de los componentes de una plataforma genera un consumo de la corriente particular, en el momento de la ejecución de la tarea, y puede igualmente activar un consumo de la corriente durante la ejecución de las siguientes tareas. Es preferible, por lo tanto, asegurar una estabilidad del consumo de la corriente en cada una de las plataformas antes de las medidas efectuadas para la verificación de conformidad.

En particular, la citada etapa de estabilización puede incluir una transmisión de una serie de órdenes idénticas a las citadas plataformas a tetar y a la plataforma de referencia.

Las ordenes pueden estar predefinidas, elegidas en función de sus consecuencias sobre el consumo de la corriente en las plataformas, o seleccionadas aleatoriamente.

Según un aspecto particular del invento, el procedimiento incluye una etapa de desactivación de una protección contra los ataques por canales escondidos, previa al citado análisis, estando condicionada la citada desactivación a una autentificación del citado dispositivo de verificación.

En efecto, algunas plataformas están protegidas contra ciertas formas de ataques por la medida de la corriente. Tal protección, llamada incluso contramedida, consiste en esconder el consumo de la corriente de una plataforma a un “observador exterior”, distorsionando este consumo o presentando un consumo caótico de la corriente, no representativo del consumo real de la corriente en la plataforma.

Con el fin de poder basar la verificación de conformidad en las medidas de la corriente, el dispositivo de verificación podrá desactivar las contramedidas, después de haberse autentificado previamente ante las plataformas.

Además, según otro aspecto particular del invento, las citadas plataformas a testar y la plataforma de referencia están sometidas, durante el citado análisis, a al menos una variación de al menos un parámetro externo que pertenece al grupo que incluye:

- el valor de la tensión de alimentación;
- la forma de la tensión de alimentación;
- la temperatura;
- la frecuencia del reloj:
- la relación cíclica del reloj;
- la forma del reloj.

De esta manera, una o unas variaciones de los parámetros externos permiten obtener una mayor fiabilidad del procedimiento de verificación, pues componentes diferentes reaccionan de una manera diferente a tales variaciones, haciendo más complejas las eventuales copias.

Según un modo particular de realización del invento, varias plataformas de referencia están presentes en el citado dispositivo de verificación, y el procedimiento de verificación incluye una etapa de selección de la plataforma de referencia correspondiente a la plataforma a testar.

Según una variante de realización, el procedimiento de verificación según el invento incluye, durante el citado análisis, una etapa de carga dinámica de al menos un programa de test simultánea o secuencialmente en las citadas plataformas a testar y en la plataforma de referencia, con emplazamientos de la memoria idénticos y una etapa de lanzamiento del citado programa de test, simultánea o secuencialmente en las citadas plataformas a testar y en la plataforma de referencia.

De esta manera, el dispositivo de verificación efectúa las medidas de la corriente durante el funcionamiento de un programa de test, cargado dinámicamente en las dos plataformas (a testar y en la de referencia).

En particular, el procedimiento de verificación puede incluir una etapa de generación aleatoria del citado programa de test, previa a la citada etapa de carga dinámica.

De esta manera, los medios utilizados en el dispositivo de verificación para efectuar una verificación de conformidad son difíciles de anticipar (por ejemplo, con vistas a fabricar plataformas fraudulentas capaces de “falsificar” tal procedimiento de verificación), puesto que el dispositivo genera, él mismo, un programa de test que tele-carga en cada una de las plataformas antes de comenzar la verificación. El programa de test no es, por lo tanto, conocido de antemano.

En este caso particular, la citada etapa de generación del citado programa de test puede tener en cuenta al menos una regla de confinamiento del citado programa aleatorio en un espacio de la memoria predeterminado, prohibiendo un acceso a unas zonas de la memoria no autorizadas de la citada plataforma a testar y de la plataforma de referencia.

De esta manera, el dispositivo de verificación se asegura que el programa que va a generar no puede degradar el funcionamiento de las plataformas en las que lo carga, por ejemplo, accediendo a unas zonas de la memoria no autorizadas.

El procedimiento de verificación incluye de una manera ventajosa una etapa de control del citado programa de test aleatorio por la plataforma en la cual ha sido tele-cargado.

De esta manera, una plataforma de referencia (respectivamente una plataforma a testar) incluye unos medios para asegurarse de que el programa de test aleatorio que recibe está conforme con su funcionamiento, y, por ejemplo, no acepta instrucciones que accedan a zonas de memoria no autorizadas.

Según un modo de realización ventajoso, el citado dispositivo de verificación transmite al menos un dato aleatorio al citado programa de test durante el citado análisis.

De esta manera, el dispositivo de verificación permanece en comunicación con cada una de las plataformas durante el desarrollo del programa de test.

Según otro aspecto del invento, el procedimiento según el invento incluye, durante el citado análisis, una etapa de lanzamiento de un programa de verificación que escruta simultánea o secuencialmente, el comportamiento de un programa a testar en la citada plataforma a testar y de un programa correspondiente presente en la citada plataforma de referencia, llamado programa de referencia.

En este caso, el dispositivo de verificación verifica la conformidad de un programa a testar, en una plataforma a testar, comparando su comportamiento con el de una plataforma de referencia, que incluye un programa de referencia. Para ello, el dispositivo de verificación dispone de un programa de verificación que accede simultáneamente al programa a testar y al programa de referencia, y efectúa las medidas de la corriente, respectivamente en la plataforma a testar y en la plataforma de referencia, durante el funcionamiento del programa de verificación.

Preferentemente, el citado programa de verificación incluye unas instrucciones de manipulación de sus propios octetes, y, respectivamente, de todos los octetes del conjunto de los espacios de memoria de la plataforma a testar y de la plataforma de referencia, y, por lo tanto, especialmente, los octetes del citado programa a testar y del citado programa de referencia, al menos algunas de las citadas instrucciones de manipulación pertenecen al grupo que incluye:

- un cálculo efectuado en los octetes;

- una carga y una descarga de los octetes en la memoria.

De esta manera, el procedimiento de verificación analiza las medidas de la corriente de las dos plataformas mientras que el programa de verificación accede simultánea o secuencialmente a todos los octetes de la plataforma a testar y de la plataforma de referencia, activando cada instrucción del programa de verificación un comportamiento particular, en términos de consumo de la corriente de las plataformas.

De esta manera, si los octetes del programa de referencia y los del programa a testar son diferentes, el procedimiento de verificación puede detectar variaciones diferentes de las medidas de la corriente en el momento en el que el programa de verificación accede a estos octetes diferentes, y, de esta manera, suponer que los dos programas son diferentes.

Según un aspecto particular de esta variante, el citado programa de verificación es almacenado en cada una de las citadas plataformas.

Por ejemplo, el programa de verificación puede formar parte del programa de referencia, lo que supone formar parte del programa a testar.

En este caso, el procedimiento incluye, antes de la citada etapa de lanzamiento del citado programa de verificación, una etapa de lanzamiento de un programa que incluya al menos una instrucción de acceso al citado programa a testar y al citado programa de referencia que permita lanzar el citado programa de verificación.

Esta etapa de lanzamiento permite al dispositivo de verificación configurar, respectivamente en cada plataforma, el programa de referencia, y el programa a testar, de tal manera que ejecuten su parte del programa correspondiente al programa de verificación.

El invento se refiere igualmente a un dispositivo de verificación de una conformidad de una plataforma electrónica, llamada plataforma a testar, y/o de un programa informático a testar, presente en la citada plataforma a testar según el procedimiento descrito anteriormente.

En particular, tal dispositivo incluye unos medios de CONSUMO de una tarjeta bancaria que soporta la citada plataforma a testar, controlados por los citados medios de decisión. Puede tratarse especialmente de un terminal de pago por tarjeta bancaria, preparado para verificar la conformidad de una tarjeta bancaria, o de un programa presente en tal tarjeta.

El invento se refiere igualmente a los programas de ordenador tele-cargables desde al menos una red de comunicaciones y/o registrados sobre un soporte legible por ordenador y/o ejecutables por un procesador, que incluye unas instrucciones de un código de un programa para la utilización de al menos ciertas etapas del procedimiento de verificación descrito precedentemente.

Finalmente, el invento se refiere además a una plataforma electrónica optimizada, preparada para ser verificada según el procedimiento de verificación descrito anteriormente, y que incluye unos medios de amplificación y/o de aumento de las variaciones de al menos una de las características del citado comportamiento.

El procedimiento descrito anteriormente puede aplicarse con toda seguridad a todos los tipos de plataformas, sin una adaptación particular. Sin embargo, es posible facilitar la verificación (simplificando los dispositivos de verificación o el procedimiento de verificación asociado), o aumentar la fiabilidad de esta verificación, previendo que las plataformas mismas estén adaptadas, durante su concepción y/o su producción, para reforzar ciertos comportamientos, y facilitar, por lo tanto, las comparaciones.

Por ejemplo, estas adaptaciones pueden conseguir que las variaciones de la corriente sean amplificadas, o más rápidas.

5. Lista de las figuras

Otras características y ventajas del invento aparecerán de una manera más clara con la lectura de la descripción siguiente de un modo de realización particular, dado a título de simple ejemplo ilustrativo y no limitativo, y de los dibujos anexos, entre los cuales:

- la figura 1 presenta un ejemplo de un dispositivo de verificación según un modo de realización particular del invento;

- la figura 2 es un organigrama simplificado que ilustra el principio general del invento;

- las figuras 3a y 3b presentan las diferentes etapas utilizadas según dos variantes de un primer modo de realización particular del invento;

- la figura 4 presenta las diferentes etapas utilizadas según un segundo modo de realización particular del invento.

6. Descripción de un modo de realización del invento

6.1 Aspectos generales

El principio general del invento se basa en una comparación del comportamiento de una plataforma electrónica a testar con respecto al de una plataforma de referencia de conformidad.

En los modos de realización descritos, estos comportamientos estudiados corresponden a unas medidas de la corriente efectuadas sobre unas plataformas en funcionamiento.

De esta manera, el procedimiento de verificación de la conformidad según el invento toma en consideración las características de consumo de la corriente (o de unas informaciones relacionadas o similares, tales como el tiempo de respuesta o la radiación emitida) del circuito electrónico presente en cada plataforma, en unas condiciones idénticas, para detectar a una plataforma no conforme y/o a un programa no conforme presente en una plataforma.

En otras palabras, el procedimiento de verificación según el invento considera al circuito electrónico presente en una plataforma como una “huella digital” de esta plataforma, su estructura particular (“jungla” de transistores) que inducen un comportamiento particular, en términos de consumo de la corriente, que no puede ser reproducido por un circuito y/o un programa fraudulento o imitado, incluso aunque el resultado lógico proporcionado sea idéntico.

Dos modos de realización particulares son descritos a continuación:

- verificación de conformidad de una tarjeta con chip (en relación con las figuras 3a y 3b),

- verificación de conformidad de un programa presente en una tarjeta con chip (en relación con la figura 4).

Estos dos modos de realización pueden ser, llegado el caso, combinados, y utilizados por un mismo dispositivo de verificación.

De una manera general, un circuito electrónico utilizado en una tarjeta con chip está constituido especialmente por una pluralidad de componentes electrónicos, que tienen cada uno un comportamiento dado para efectuar una tares dada, y conectados entre sí. Estos componentes están integrados en un circuito de tal manera que satisfagan el comportamiento lógico esperado para la tarjeta.

A continuación, con el fin de optimizar el tamaño del componente y, por lo tanto, de aumentar su rendimiento (cuanto más pequeño es un circuito mayor es su rendimiento en términos de desechos en la fabricación, por ejemplo), el circuito está "sintetizado", es decir, que cada componente, cada conexión, están colocados de manera óptima sobre el circuito, los componentes que tienen las mismas funciones están "factorizados" si fuese posible, etc. Se obtiene entonces un circuito optimizado, llamado incluso "netlist" (por "lista de interconexiones, en francés).

Tal circuito responde especialmente a las diferentes exigencias esperadas para la tarjeta tales como su comportamiento lógico, el tamaño y el rendimiento del circuito, y posee unas características eléctricas muy particulares, por ejemplo, en términos de consumo de corriente.

Además, una ventaja de este circuito optimizado radica en el hecho de que es muy difícilmente reproducible como idéntico por parte del falsificador, y que se diferencia, por lo tanto, de un circuito falsificado por sus características eléctricas, especialmente en términos de consumo de corriente.

En efecto, el circuito obtenido está formado por un ensamblaje, no interpretable directamente por un humano, de millones de transistores combinados entre sí de una manera particular (siendo inútiles algunos quizás, otros utilizados eficazmente varias veces, para distintas funciones).

La figura 1 ilustra un ejemplo de dispositivo de verificación que utiliza el procedimiento según el invento. En este ejemplo, el dispositivo de verificación es un terminal 10 de pago, utilizado para los pagos con ayuda de tarjetas con chip. Tal terminal 10 contiene una tarjeta con un chip de referencia 11 y un acceso exterior para una tarjeta con un chip a testar 12. El terminal 10 incluye unos medios de utilización del procedimiento de verificación de conformidad 13 según el invento.

En el caso en el que el terminal pueda se vea obligado a verificar tarjetas emitidas por varios fabricantes, podrá incluir varias tarjetas con un chip de referencia, correspondientes respectivamente a los diferentes tipos de tarjetas con las cuales acepta efectuar transacciones.

En efecto, de una manera general, un terminal de pago está preparado para efectuar unas transacciones con varios tipos de tarjetas con un chip, correspondientes, por ejemplo, a unos organismos bancarios diferentes, y que incluyan unos circuitos electrónicos diferentes.

De esta manera, tal terminal de pago puede verse obligado a verificar la conformidad de tarjetas con chip de diferentes tipos, y, por lo tanto, obligado a comparar las tarjetas a testar con varias tarjetas de referencia. Como cada tipo de tarjetas presenta un comportamiento particular, el dispositivo o terminal de verificación utiliza una etapa de identificación del tipo de la tarjeta a testar O del tipo pretendido, si se trata de una tarjeta no conforme) y selecciona en consecuencia la tarjeta de referencia.

Se considera, a continuación, el caso particular en el que un terminal está dedicado específicamente a un tipo de tarjetas con chip y verifica la conformidad de una tarjeta a testar comparándola con una sola tarjeta de referencia. Se trata, por lo tanto, de detectar una tarjeta a testar que tuviese un comportamiento lógico correcto, pero cuya constitución, la estructura al nivel de los transistores que la componen, sería diferente.

El procedimiento según el invento incluye tres etapas principales, como está ilustrado en la figura 2.

Una primera etapa 20 de transmisión de un juego de informaciones permite al dispositivo de verificación señalar a las tarjetas de referencia y a testar las que van a entrar en un modo de funcionamiento específico, llamado modo de test, diferente del modo de funcionamiento habitual de las tarjetas, por ejemplo, el que permite efectuar transacciones.

Este modo de test permite al dispositivo verificar una conformidad de una tarjeta a testar, utilizando el procedimiento de verificación según el invento.

Las informaciones transmitidas en esta primera etapa 20 son, por ejemplo, una orden que pide a las tarjetas ponerse "a la escucha" del dispositivo de verificación. A la recepción de esta orden, las tarjetas se ponen en modo de test y esperan otras informaciones procedentes del dispositivo de verificación.

El juego de informaciones transmitido puede incluir igualmente unas órdenes necesarias para la preparación de las tarjetas antes de las siguientes etapas de análisis 21 de los componentes y de la decisión de conformidad 22.

En efecto, según el invento, el procedimiento de verificación puede incluir algunas etapas previas a la misma verificación, necesarias para su eficacia, y que permiten especialmente no causar daños a las tarjetas con un chip concernidas (a la de testar y a la (s) de referencia).

Estas etapas son presentadas más adelante, en relación con las figuras 3a, 3b y 4.

Después de la etapa 20 de transmisión de un juego de informaciones, las tarjetas a testar y la de referencia se encuentran en un mismo estado de test. La siguiente etapa es una etapa de análisis 21 de los comportamientos de las dos tarjetas, con vistas a una etapa 22 de decisión de la conformidad, durante la cual el dispositivo valida o no la conformidad de la tarjeta a testar.

Estas dos etapas 21 y 22 serán igualmente detalladas más adelante, en relación con las figuras 3a, 3b y 4.

Se describe ahora, en relación con las figuras 3a, 3b y 4, las etapas previas a la verificación de conformidad.

Una primera etapa previa a la verificación es una etapa (31a, 31b, 41) de desactivación de las contramedidas.

En efecto, una tarjeta con un chip puede estar protegida contra una forma de ataque particular, llamada “ataque por medida de corriente” o “ataque por canales escondidos”. Una de estas protecciones es llamada “contramedidas” y puede ser vista como un “distorsionador” de la corriente, es decir, un método que permite esconder, por ejemplo, a un analizador de corriente, el consumo de la tarjeta durante su funcionamiento o presentar un consumo de corriente caótico de la tarjeta durante su funcionamiento.

Tales protecciones deben se desactivadas durante la utilización del procedimiento según el invento, al estar basado éste en las medidas de la corriente en las tarjetas a testar y en la de referencia.

Sin embargo, para evitar cualquier desactivación no autorizada de las contramedidas, ésta debe estar condicionada a una autentificación del dispositivo, aquí el terminal de pago, el solicitante.

Esta autentificación puede utilizar unos procedimientos de autentificación bien conocidos por el experto, tales como unos procedimientos de criptografía, y, por lo tanto, no detallados aquí.

De esta manera, una vez autentificado el terminal como apto para desactivar las contramedidas, éste puede comenzar la verificación de conformidad según el invento.

Una segunda etapa previa a la verificación puede ser una etapa (32a, 32b, 42) de estabilización de la corriente en las tarjetas.

En efecto, con el fin de asegurar una buena eficacia de las medidas de la corriente efectuadas, es deseable que el consumo de la corriente en las tarjetas sea previamente estabilizado, de tal manera que no tenga en cuenta las variaciones debidas a las acciones precedentes de las tarjetas.

En efecto, el consumo de la corriente en un instante t en una tarjeta depende de la tarea efectuada por el circuito electrónico en el instante t y de las tareas precedentes. Por ejemplo, una tarea efectuada en el instante t-1 puede activar unas descargas de capacidades en el instante t.

La etapa de estabilización de la corriente del procedimiento consiste en transmitir simultáneamente a cada una de las tarjetas (de referencia y a testar) un cierto número de ordenes predeterminadas, típicamente idénticas, que permitan utilizar las dos tarjetas en un mismo estado de consumo de la corriente.

Estas órdenes pueden ser solicitudes enviadas a las tarjetas que activan en ellas unas acciones particulares, incluso unas respuestas de las tarjetas.

Una vez estabilizado el consumo de la corriente en las tarjetas, el dispositivo comienza la verificación de conformidad, pues las dos tarjetas se supone que se encuentran en un mismo estado “físico”.

Se presenta ahora, en relación con las figuras 3a y 3b, un primer modo de realización particular del invento en el cual el procedimiento de verificación se utiliza en un terminal de pago para verificar la conformidad de una tarjeta con un chip.

6.2 Detección de una tarjeta clonada

6.2.1 Primera variante

Según una primera variante, ilustrada en la figura 3a, la etapa 21 de análisis de los comportamientos (véase la figura 2) consiste en medir el consumo de la corriente en cada una de las dos tarjetas y en efectuar una correlación de estas medidas durante un periodo determinado.

En esta variante, las etapas 30a de transmisión de un juego de informaciones, 31a de desactivación de las contramedidas y 32a de estabilización de la corriente son las mismas que las descritas anteriormente.

La etapa 21 de análisis de los comportamientos incluye en esta variante las etapas 33a de medidas de la corriente y 34a de análisis de estas medidas.

De una manera más precisa, el terminal dialoga simultáneamente con cada una de las dos tarjetas, por ejemplo, transmitiendo unas informaciones, unas órdenes, o simplemente unos datos aleatorios a las dos tarjetas, y mide la corriente en cada una de las tarjetas durante una etapa 33a de medidas de la corriente, de tal manera que disponga de una serie de medidas o de una curva del consumo de la corriente para cada una de las tarjetas.

Según otro modo de realización, estos diálogos idénticos pueden ser efectuados secuencialmente (o de forma alterna) en la plataforma de referencia, y a continuación, en la plataforma a testar. De una manera más general, los diferentes aspectos del invento pueden ser utilizados simultáneamente en las dos plataformas, o secuencialmente, desde el momento en el que las condiciones externas permanecen constantes.

Estas medidas de la corriente son efectuadas en el mismo emplazamiento sobre cada tarjeta, por ejemplo, al nivel de sus alimentaciones respectivas, de tal manera que puedan ser comparadas de una manera eficaz.

Una vez efectuadas estas medidas de la corriente el terminal dispone, por lo tanto, de una serie de medidas, o de una curva, de la corriente para cada tarjeta, correspondiendo cada una al consumo de la tarjeta en las mismas condiciones de test. En efecto, es importante observar que, según el invento, no se busca verificar que la tarjeta a testar se presente bien, en absoluto y en una situación determinada, un valor de la corriente, que podría ser imitado, o simulado, por una tarjeta falsa hábilmente realizada. Se verifica, por el contrario, que el comportamiento es el esperado en el momento del test, en las condiciones del test, y, llegado el caso, en función de las solicitaciones y/o de unas condiciones variables, de manera predeterminada o aleatoria.

La etapa siguiente 34a de análisis de las medidas de la corriente, efectuada paralelamente por la tarjeta a testar y por la tarjeta de referencia, asegura, por lo tanto, una comparación de los comportamientos eléctricos de cada tarjeta en las mismas condiciones del test.

Esta etapa 34a puede tener en cuenta directamente, por ejemplo, las medidas de la corriente de cada tarjeta y compara sus valores y/o sus evoluciones. En ciertos casos, podrá tratarse de comparaciones en el sentido estricto, con un umbral de tolerancia predeterminado. Para evitar errores en la decisión debido, por ejemplo, a unas variaciones de las condiciones externas con respecto a un escalonamiento previo, o a unas diferencias del consumo debidas a la fabricación, podrá ser preferible que la comparación utilice una correlación entre las medidas. Esta correlación puede ser especialmente temporal y/o frecuente (después de la transformación de la señal medida, por ejemplo, por una FFT), y puede descansar sobre las medidas mismas de la corriente o sobre unas señales representativas de estas medidas, o incluso sobre cualquier función matemática de una señal física o de una información del tiempo resultante del comportamiento de cada tarjeta.

En efecto, el terminal puede utilizar sobre las medidas de la corriente efectuadas, un tratamiento previo a la correlación, con el fin de obtener mejores resultados en términos de eficacia y/o hacer todavía más compleja la simulación para una tarjeta o un programa no conforme.

De esta manera, las medidas de la corriente pueden ser filtradas, numeradas, amplificadas y/o sufrir unas transformaciones matemáticas antes de ser correlacionadas.

Por ejemplo, el terminal puede aplicar una transformada de Fourier sobre las medidas de la corriente y obtener así dos curvas de señales representativas de las medidas de la corriente de cada tarjeta, con el fin de poder comparar las variaciones de las amplitudes de cada curva a diferentes frecuencias.

Si las curvas de las medidas de la corriente, o las curvas de las señales representativas de las medidas de la corriente, obtenidas después del tratamiento de las medidas de la corriente, evolucionan de una manera sensiblemente idénticas (con unos umbrales de tolerancia que serán fijados en función de las tecnologías utilizadas especialmente) en un periodo determinado, el terminal va a decidir que la tarjeta a testar es una tarjeta válida y a proporcionar una decisión de conformidad positiva, durante la etapa 25a de decisión de conformidad.

En efecto, dos tarjetas que incluyen dos circuitos electrónicos optimizados idénticos van a presentar un comportamiento idéntico en términos de consumo de la corriente.

Por el contrario, dos tarjetas que incluyen dos circuitos electrónicos optimizados diferentes van a comportarse de una manera diferente en términos de consumo de corriente, incluso aunque los comportamientos lógicos programados sean los mismos, pues una misma orden enviada a cada tarjeta no utilizará los mismos componentes de los circuitos electrónicos u activará consumos de corriente diferentes para cada tarjeta.

Para obtener mejores prestaciones, las medidas de la corriente pueden ser sometidas a unas variaciones (predeterminadas o aleatorias) de los parámetros externos, tales como la tensión de alimentación, la temperatura o el reloj (la frecuencia del reloj, la relación cíclica el reloj, la forma del reloj…).

En efecto, tales variaciones van a influir en las variaciones de la corriente de las dos tarjetas, pero, si los circuitos optimizados son idénticos en las dos tarjetas, la influencia de estas variaciones de los parámetros externos será la misma, pues dependerá de los mismos componentes y de su organización en el circuito. Por el contrario, si los circuitos optimizados son diferentes, estas variaciones no tendrán las mismas consecuencias en las medidas de la corriente en las dos tarjetas.

6.2.2 Segunda variante

Según una segunda variante, ilustrada en la figura 3b, las medidas de la corriente no son efectuadas durante un periodo determinado de dialogo entre el terminal y las tarjetas, sino durante un periodo determinado de funcionamiento de un programa de test previamente cargado en cada una de las tarjetas.

Las etapas de transmisión de un juego de informaciones 30b, de desactivación de las contramedidas 31b y de estabilización de la corriente 32b, han sido ya descritas precedentemente, especialmente en la descripción de la primera variante del primer modo de realización particular.

Sin embargo, la etapa 30b de transmisión de un juego de informaciones puede incluir, por ejemplo, igualmente la transmisión de las informaciones que indican a las tarjetas que van a recibir un programa de test que deberán ejecutar a continuación.

Tal programa de test puede ser, según un primer ejemplo, conocido y estar contenido en el terminal o, según un segundo ejemplo, aleatorio y generado dinámicamente por el terminal en el momento de la utilización del procedimiento de verificación según el invento.

En este segundo ejemplo, el terminal genera, por lo tanto, aleatoriamente, durante una etapa 33b de generación, un programa de test. Este programa aleatorio está destinado a ser cargado en cada una de las dos tarjetas a testar y de referencia durante una etapa 34b de carga.

Tal programa de test incluye unas instrucciones que serán ejecutadas, por lo tanto, por estas tarjetas, durante una etapa 36b de lanzamiento del programa de test.

La ejecución de tal programa en las tarjetas permite automatizar especialmente las acciones efectuada por las tarjetas durante el periodo de medidas de la corriente, reemplazando a la etapa de dialogo descrita anteriormente en la primera variante.

Pueden tomarse unas precauciones, sin embargo, relativas a este programa de test, de tal manera que no engendre degradaciones en el funcionamiento o en la seguridad de las tarjetas en las cuales está tele-cargado.

En efecto, el procedimiento de verificación según el invento puede asegurarse de que el programa de test utilizado no accede a las zonas no autorizadas en la memoria de las tarjetas, que no modifica el comportamiento de las tarjetas y que no destruye el contenido de las tarjetas.

Para ello, el procedimiento descrito prevé la puesta en marcha de unas reglas de seguridad durante la etapa de generación aleatoria 33b del programa de test.

De esta manera, el programa de test se genera de tal manera que tiene en cuenta unos criterios predeterminados, por ejemplo, las direcciones de las zonas de la memoria no autorizadas de las tarjetas. El programa de test generado puede estar restringido, por ejemplo, en tamaño, y/o contener una dirección de carga en las tarjetas predeterminada y reservada, de tal manera que el programa de test esté confinado en un espacio de la memoria reservado en la memoria de las tarjetas.

Otro medio de control del programa de test puede ser utilizado en las tarjetas mismas, después de su carga, durante una etapa 35b de control. Esta solución permite de esta manera a las tarjetas verificar, por sí mismas, por ejemplo, que el programa de test no contiene instrucciones agresivas que le permitan acceder a unas zonas de la memoria no autorizadas. Este control puede detectar igualmente desde la carga del programa una eventual dirección de carga no autorizada o un tamaño del programa no conforme.

De una manera alternativa, el programa de test aleatorio puede contener una firma, o un “MAC”, (Message Authentication Code”), que controla la tarjeta en la que está telecargada. En este caso, el dispositivo de verificación se supone qyue es digno de confianza.

Una vez efectuada esta etapa de control del programa de test aleatorio, el terminal puede transmitir a cada una de las tarjetas una orden de lanzamiento del programa, y definir el comienzo y el final del periodo de medidas de la corriente, en función de ña ejecución del programa de test. Este lanzamiento puede ser efectuado igualmente por parte de las tarjetas mismas.

De esta manera, las medidas de la corriente efectuadas durante la etapa 37b en cada una de las dos tarjetas son función de unas instrucciones del programa de test. Por ejemplo, se observan los dos siguientes casos:

- el caso en el que la tarjeta a testar es conforme e incluye el mismo circuito electrónico optimizado que la tarjeta de referencia: las instrucciones del programa de test tienen los mismos efectos sobre los diferentes componentes de las dos tarjetas y las medidas de la corriente están correlacionadas;

- el caso en el que la tarjeta a testar no es conforme y no incluye el mismo circuito electrónico optimizado que la tarjeta de referencia: las instrucciones del programa de test no tienen los mismos efectos pues los componentes de las dos tarjetas son diferentes y/o están colocados en lugares diferentes en las tarjetas y las medidas de la corriente no están correlacionadas.

Estas etapas de medida de la corriente 37b, de análisis 38b de las medidas de la corriente y de decisión de conformidad 39b, pueden ser las mismas que las descritas en la primera variante de este modo de realización (véase la figura 3a), y no son, por lo tanto, descritas de nuevo.

Además, las medidas de la corriente pueden depender igualmente de variaciones de los parámetros externos, tales como la tensión de alimentación, la temperatura o el reloj, como ya se ha descrito en relación con la figura 3a.

Como ya se ha mencionado, estas variantes pueden ser amplificadas y reforzadas, por una concepción y/o una producción adaptada a las plataformas.

6.3 Detección de un programa no conforme

Se presenta ahora, en relación con la figura 4, un segundo modo de realización particular del invento en el cual el procedimiento de verificación se utiliza en un terminal de pago para verificar la conformidad de un programa presente en una tarjeta con un chip.

Este modo de realización particular permite al dispositivo de verificación, por ejemplo, un terminal de pago, asegurarse de que el programa a testar contenido en una tarjeta con un chip es conforme con un programa de referencia esperado y no incluye instrucciones “maliciosas”.

Tales instrucciones maliciosas pueden permitir, por ejemplo, a una tarjeta fraudulenta acceder a los secretos contenidos en la tarjeta con vistas a duplicarla, efectuar transacciones no autorizadas con la tarjeta, etc.

En este modo de realización particular, las etapas 41 de desactivación de las contramedidas, 42 de estabilización de la corriente, 44 de medidas de la corriente, 45 de análisis de las medidas de la corriente y 46 de decisión de conformidad pueden ser parecidas a las descritas en el modo de realización particular precedente.

La etapa 40 de transmisión de un juego de informaciones consiste especialmente en indicar a la tarjeta a testar y a la tarjeta de referencia que van a entrar en un modo de test de los programas presentes en cada una de ellas, es decir, el programa a testar (en la tarjeta a testar) y el programa de referencia (en la tarjeta de referencia). Las tarjetas se ponen, de esta manera, a la escucha del dispositivo de verificación, en un modo de test y no en un modo de funcionamiento normal.

Una vez efectuadas las etapas de desactivación de las contramedidas 41 y de estabilización de la corriente 42 (ya descritas precedentemente), el dispositivo de verificación ejecuta un programa de verificación durante una etapa 43 de lanzamiento, accediendo simultáneamente al programa a testar y al programa de referencia.

Las medidas de la corriente (etapa 44) son efectuadas durante un periodo determinado de ejecución del programa de verificación.

En efecto, tal programa de verificación incluye unas instrucciones que permiten manipular sus propios octetes y todos los octetes del programa contenidos en la plataforma a testar y en la plataforma de referencia, y si los dos programas son idénticos. Las manipulaciones de los octetes deben tener, por lo tanto, las mismas consecuencias en los consumos de la corriente en las dos tarjetas, pues estas manipulaciones de los octetes activan unas tareas ejecutadas por los diferentes componentes de los circuitos electrónicos de las tarjetas.

De esta manera, si los programas (a testar y de referencia) son idénticos, las medidas de la corriente de las dos tarjetas están correlacionadas, sino diferentes.

Las etapas de análisis 45 de las medidas de la corriente y de decisión de la conformidad 46 son las mismas que las descritas para el primer modo de realización particular.

Según una primera variante de este segundo modo de realización particular, el programa de verificación está presente en el terminal que utiliza el procedimiento de verificación.

De esta manera, la etapa de lanzamiento 43 corresponde a la ejecución, en el terminal, de un programa que accede simultáneamente a sus propios octetes y respectivamente a los de los programas a testar y de referencia.

Según una segunda variante, el programa de verificación está contenido en el programa de referencia (el programa de funcionamiento de la tarjeta) y, por lo tanto, se supone contenido igualmente en el programa a testar.

En este caso, la etapa de lanzamiento 43 corresponde a la emisión de una orden, del terminal hacia las tarjetas, para el lanzamiento de sus programas de verificación internos. De esta manera, a la recepción de sta orden, un programa de referencia presente en una tarjeta ejecuta su parte de verificación que contiene, como en la primera variante, unas instrucciones de manipulación de sus propios octetes y del resto de los octetes del programa presente en la tarjeta.

Las medidas de la corriente se efectúan durante la ejecución de este programa de verificación y se pueden distinguir varios casos diferentes:

- el caso en el que el programa a testar es un programa conforme y contiene, por lo tanto, un programa de verificación: los programas de verificación se ejecutan en las dos tarjetas y las medidas de la corriente de las tarjetas a testar y de referencia están correlacionadas;

- el caso en el que el programa a testar es un programa conforme, pero contiene un programa de verificación: los programas de verificación se ejecutan en las dos tarjetas, pero las medidas de la corriente en las dos tarjetas no están correlacionadas, especialmente cuando el programa de verificación debe manipular unos octetes “maliciosos” del programa a testar;

- el caso en el que el programa a testar no es un programa conforme y no contiene programas de verificación: el programa de verificación se lanza en la tarjeta de referencia únicamente y las medidas de la corriente de las dos tarjetas no están correlacionadas.

6.4 Complementos y variantes

Los modos de realización descritos anteriormente presentan la utilización en tarjetas con un chip, en particular para aplicaciones bancarias. Está claro, sin embargo, que el invento puede ser utilizado igualmente en numerosas otras aplicaciones, desde el momento en el que sea necesario autentificar el origen y/o la conformidad de una tarjeta y/o de un programa presente en ella.

Por otra parte, el invento no se limita a las tarjetas con un chip, sino que, por el contrario, puede ser utilizado en otros tipos de plataformas electrónicas, desde el momento en el que es necesario validar su origen y su conformidad. Por ejemplo, es posible verificar según el invento elementos RFID. En este caso, la comparación de los comportamientos podrá tener en cuenta las radiaciones electromagnéticas de un elemento RFID de referencia y de un elemento RFID a testar, utilizando una aproximación similar a la descrita precedentemente.

REIVINDICACIONES

1. Procedimiento de verificación (13) de una conformidad de una plataforma electrónica, llamada plataforma a testar (12), y/o de un programa informático a testar, presente en la citada plataforma a testar, incluyendo el citado procedimiento:

- una etapa de transmisión (20; 30a; 30b; 40), por parte de un dispositivo de verificación (10), de un mismo juego de informaciones, por una parte, a la citada plataforma a testar y, por otra parte, a una plataforma de referencia de conformidad (11) presente en el citado dispositivo de verificación, y

- una etapa de decisión de conformidad (22, 35a; 39b; 46) de la citada plataforma a testar y/o del citado programa informático a testar, en función de un análisis (21) de los respectivos componentes de la citada plataforma a testar y de la citada plataforma de referencia,

utilizando el citado análisis una correlación entre al menos dos señales representativas de las medidas de la corriente efectuadas simultánea o secuencialmente de una manera respectiva en la citada plataforma a testar y en la citada plataforma de referencia, en un periodo de medida predeterminado,

caracterizado por que incluye, además.

- una etapa de desactivación de una protección contra los ataques por canales escondidos, previa al citado análisis, estando condicionada la citada desactivación a una autentificación del citado dispositivo de verificación.

2. Procedimiento de verificación según la reivindicación 1, caracterizado por que la citada correlación utiliza al menos uno de los cálculos que pertenecen al grupo que incluye:

- un cálculo de correlación temporal;

- un cálculo de verificación frecuencial.

3. Procedimiento de verificación según una cualquiera de las reivindicaciones 1 a 2, caracterizado por que las citadas medidas de la corriente sufren al menos uno de los tratamientos previos que pertenecen al grupo que incluye:

- los filtrados;

- las numeraciones;

- las transformaciones matemáticas;

- las amplificaciones.

4. Procedimiento de verificación según una cualquiera de las reivindicaciones 1 a 3, caracterizado por que las citadas medidas de la corriente son efectuadas sobre las alimentaciones respectivas de las citadas plataformas a testar y de la plataforma de referencia.

5. Procedimiento de verificación según una cualquiera de las reivindicaciones 1 a 4, caracterizado por que incluye una etapa de estabilización del consumo de corriente de las citadas plataformas a testar y de referencia, previa al citado análisis.

6. Procedimiento de verificación según la reivindicación 5, caracterizado por que la etapa de estabilización incluye una transmisión de una serie de órdenes idénticas simultáneamente a las citadas plataformas a testar y de referencia.

7. Procedimiento de verificación según una cualquiera de las reivindicaciones 1 a 6, caracterizado por que las citadas plataformas a testar y de referencia están sometidas, durante el citado análisis, a al menos una variación de al menos un parámetro externo que pertenece al grupo que incluye:

- el valor de la tensión de alimentación;

- la forma de la tensión de alimentación;

- la temperatura;

- la frecuencia del reloj:

- la relación cíclica del reloj;

- la forma del reloj.

8. Procedimiento de verificación según una cualquiera de las reivindicaciones 1 a 7, caracterizado por que varias plataformas de referencia están presentes en el citado dispositivo de verificación,

y por que incluye una etapa de selección de la plataforma de referencia correspondiente a la plataforma a testar.

9. Procedimiento de verificación según una cualquiera de las reivindicaciones 1 a 8, caracterizado por que incluye, durante el citado análisis, las siguientes etapas:

- una etapa de carga dinámica de al menos un programa de test simultánea o secuencialmente en las citadas plataformas a testar y de referencia, en unos emplazamientos de la memoria idénticos;

- una etapa de lanzamiento del citado programa de test, simultánea o secuencialmente en las citadas plataformas a testar y de referencia,

10. Procedimiento de verificación según la reivindicación 9, caracterizado por que incluye una etapa de generación aleatoria del citado programa de test, previa a la citada etapa de carga dinámica.

11. Procedimiento de verificación según la reivindicación 10, caracterizado por que la citada etapa de generación del citado programa de test tiene en cuenta al menos una regla de confinamiento del citado programa aleatorio en un espacio de la memoria predeterminado, prohibiendo un acceso a las zonas de la memoria no autorizadas de la citada plataforma a testar y de la citada plataforma de referencia.

12. Procedimiento de verificación según una cualquiera de las reivindicaciones 10 y 11, caracterizado por que incluye una etapa de control del citado programa de test aleatorio por parte de la plataforma en la que es telecargado.

13. Procedimiento de verificación según una cualquiera de las reivindicaciones 9 a 12, caracterizado por que el citado dispositivo de verificación transmite al menos un dato aleatorio al citado programa de test durante el citado análisis.

14. Procedimiento de verificación según una cualquiera de las reivindicaciones 1 a 7, caracterizado por que incluye, durante el citado análisis, una etapa de lanzamiento de un programa de verificación que accede simultáneamente a un programa a testar en la citada plataforma a testar y a un programa correspondiente presente en la citada plataforma de referencia, llamado programa de referencia.

15. Procedimiento de verificación según la reivindicación 14, caracterizado por que el citado programa de verificación incluye unas instrucciones de manipulación de sus propios octetes y, respectivamente, de todos los octetes del conjunto de los espacios de la memoria de la citada plataforma a testar y de la citada plataforma de referencia, al menos ciertas instrucciones de manipulación que pertenecen al grupo que incluye:

- un cálculo efectuado sobre los octetes;

- una carga y una descarga de los octetes de la memoria.

16. Procedimiento de verificación según una cualquiera de las reivindicaciones 14 y 15, caracterizado por que el citado programa de verificación está almacenado en cada una de las citadas plataformas.

17. Procedimiento de verificación según la reivindicación 16, caracterizado por que incluye, antes de la citada etapa de lanzamiento del citado programa de verificación, una etapa de lanzamiento de un programa que incluye al menos una instrucción de acceso al citado programa a testar y al citado programa de referencia que permita lanzar el citado programa de verificación.

18. Dispositivo de verificación de una conformidad de una plataforma electrónica, la citada plataforma a testar, y/o de un programa informático a testar, presente en la citada plataforma a testar según el procedimiento según una cualquiera de las reivindicaciones 1 a 18, incluyendo el citado dispositivo de verificación:

- unos medios de transmisión de un mismo juego de informaciones, por una parte, a la citada plataforma a testar y, por otra parte, a una plataforma de referencia de conformidad presente en el citado dispositivo de verificación, y

unos medios de decisión de conformidad de la citada plataforma a testar y/o del citado programa informático a testar, en función de un análisis de los comportamientos respectivos de la citada plataforma a testar y de la citada plataforma de referencia, utilizando el citado análisis una correlación entre al menos dos señales representativas de las medidas de la corriente efectuadas simultánea o secuencialmente de una manera respectiva sobre la citada plataforma a testar y sobre la citada plataforma de referencia, en un periodo de medida predeterminado,

caracterizado por que incluye además:

- unos medios de desactivación de una protección contra unos ataques por parte de unos canales escondidos, previa al citado análisis, estando condicionada la citada desactivación a una autentificación del citado dispositivo de verificación.

19. Dispositivo de verificación según la reivindicación 18, caracterizado por que incluye unos medios de consumo de una tarjeta bancaria que soporta a la citada plataforma a testar, controlados por los citados medios de decisión.

20. Producto de un programa de ordenador de verificación telecargable desde una red de comunicaciones y/o almacenado sobre un soporte legible por parte de un ordenador y/o ejecutable por parte de un microprocesador, caracterizado por que incluye unas instrucciones de un código de un programa para la ejecución del procedimiento de verificación según una al menos de las reivindicaciones 1 a 17.

21, Plataforma electrónica configurada para ser verificada según el procedimiento de verificación según una cualquiera de las reivindicaciones 1 a 17, caracterizada por que incluye unos medios de amplificación y/o de aumento de las variaciones de al menos unas características del citado comportamiento.

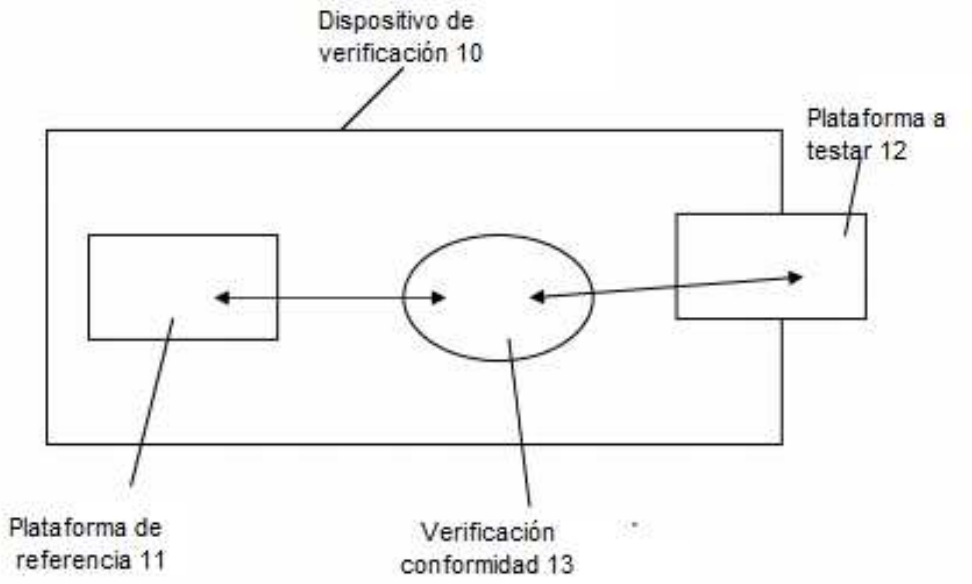

Dispositivo de verificación 10
Plataforma a testar 12
Plataforma de referencia 11
Verificación conformidad 13

FIG. 1

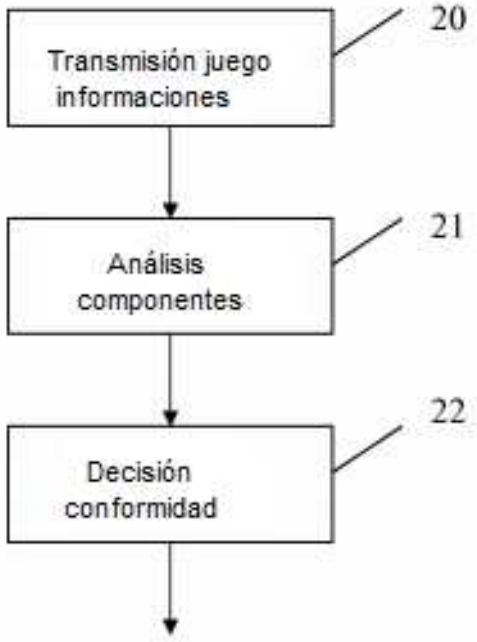

Transmisión juego informaciones
20
Análisis componentes
21
Decisión conformidad
22

FIG.2

FIG.3a

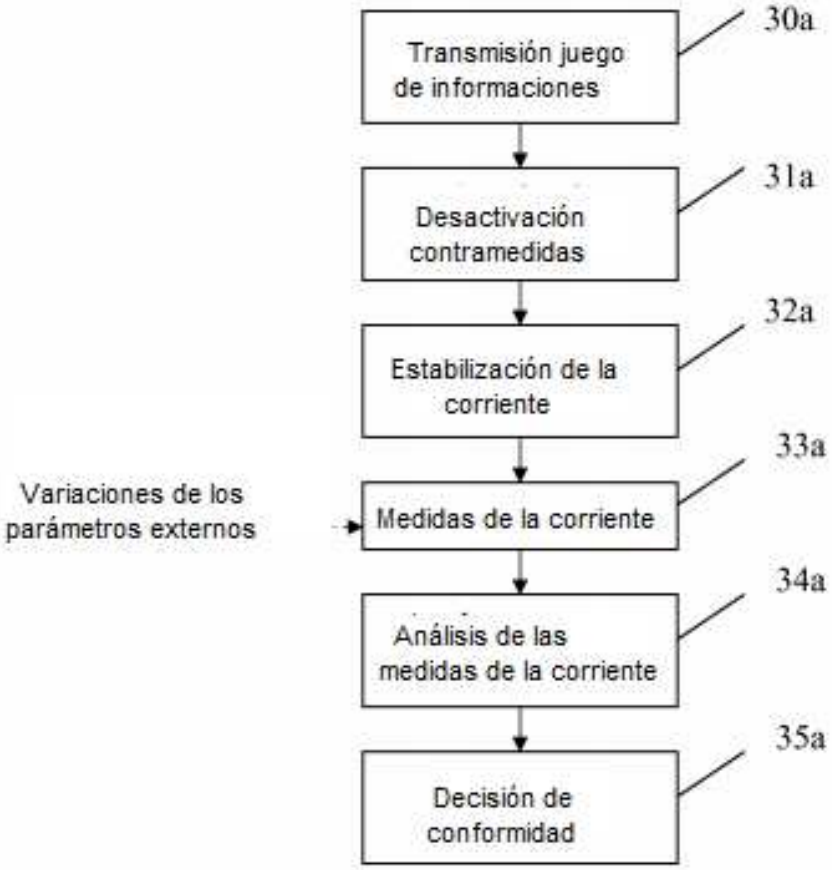

Transmisión juego de informaciones
30a
Desactivación contramedidas
31a
Estabilización de la corriente
32a
Variaciones de los parámetros externos
Medidas de la corriente
33a
Análisis de las medidas de la corriente
34a
Decisión de conformidad
35a

FIG.3b

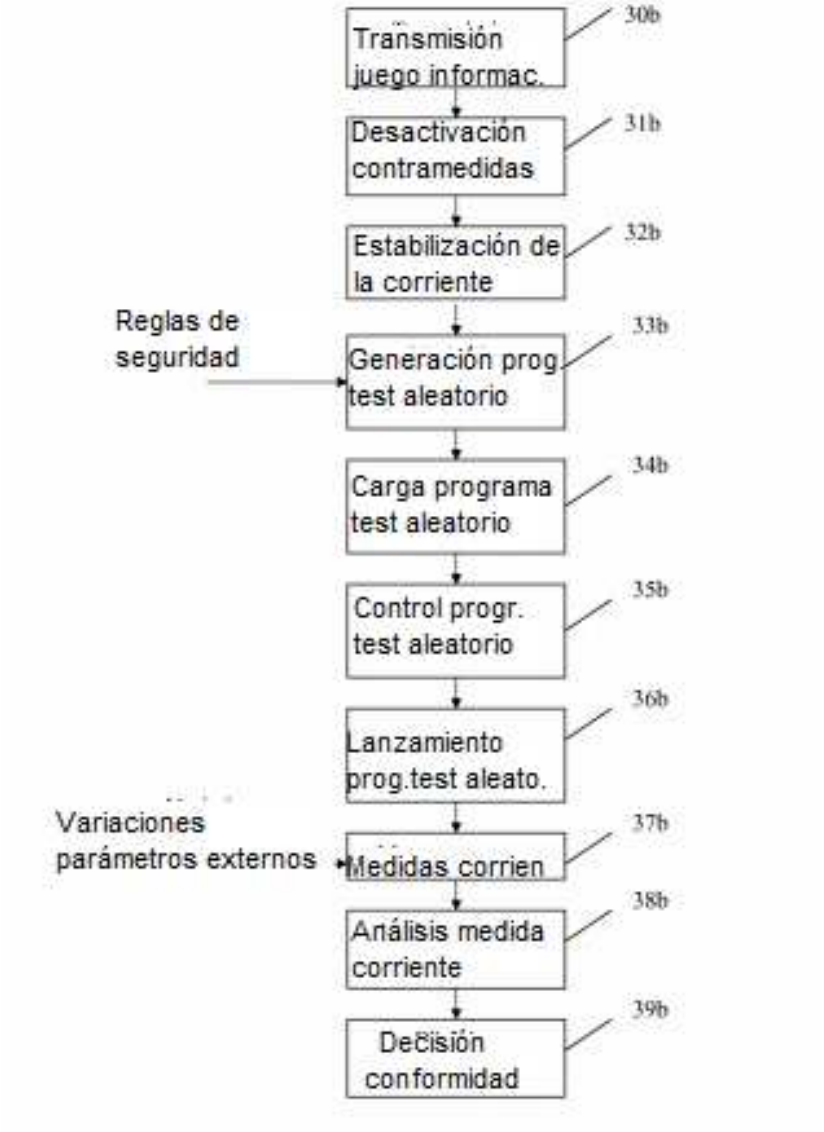
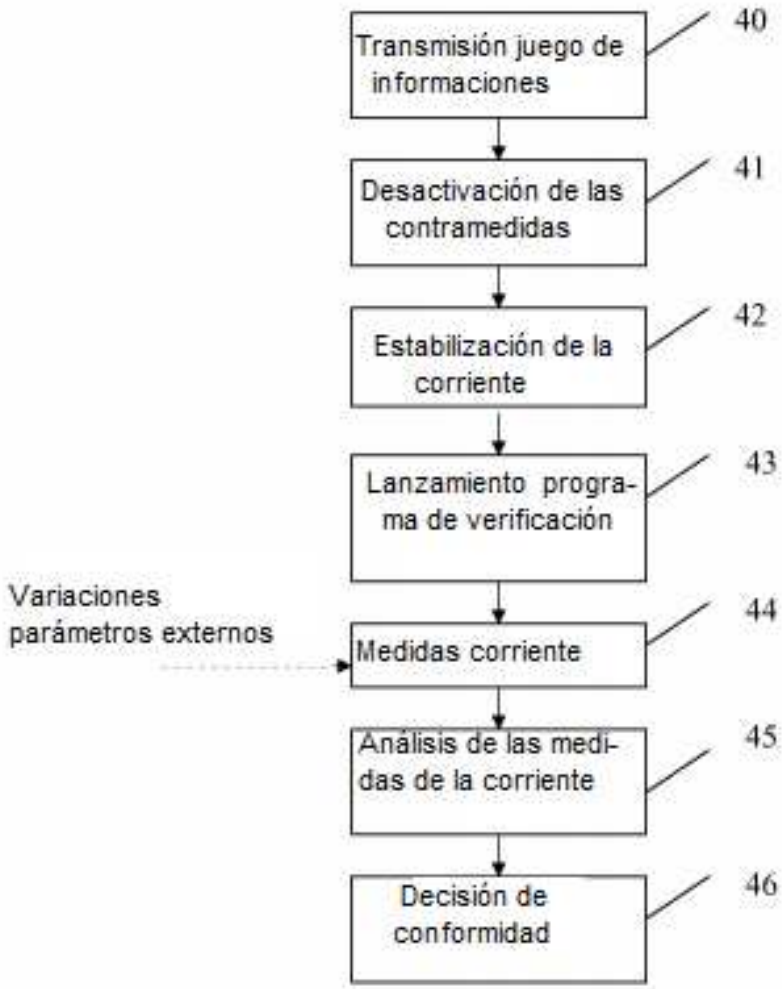

Transmisión juego informac.
30b
Desactivación contramedidas
31b
Estabilización de la corriente
32b
Reglas de seguridad
Generación prog. test aleatorio
33b
Carga programa test aleatorio
34b
Control progr. test aleatorio
35b
Lanzamiento prog.test aleato.
36b
Variaciones parámetros externos
Medidas corrien
37b
Análisis medida corriente
38b
Decisión conformidad
39b

FIG.4


Transmisión juego de informaciones
40
Desactivación de las contramedidas
41
Estabilización de la corriente
42
Lanzamiento programa de verificación
43
Variaciones parámetros externos
Medidas corriente
44
Análisis de las medidas de la corriente
45
Decisión de conformidad
46