(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 798 077**

(51) Int. CI.:

***H04L 9/12*** (2006.01)
***G06F 21/53*** (2013.01)
***H04L 9/14*** (2006.01)
***H04L 9/32*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.11.2012 PCT/SG2012/000429**

(87) Fecha y número de publicación internacional: **23.05.2013 WO13074041**

(96) Fecha de presentación y número de la solicitud europea: **16.11.2012 E 12849682 (5)**

(97) Fecha y número de publicación de la concesión europea: **20.05.2020 EP 2795829**

(54) Título: **Sistema criptográfico y metodología para asegurar criptografía de software**

(30) Prioridad:

**16.11.2011 SG 201108491**
**11.05.2012 US 201261645985 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**09.12.2020**

(73) Titular/es:

**V-KEY INC (100.0%)**
**Bridge Street Services Limited The Grand Pavilion Commercial Centre Oleander Way, 802 West Bay Road P.O. Box 30691**
**Grand Cayman KY1-1203, KY**

(72) Inventor/es:

**GAN, JOSEPH, CHER CHUEN**

(74) Agente/Representante:

**ISERN JARA, Jorge**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Sistema criptográfico y metodología para asegurar criptografía de software

Campo técnico

La presente solicitud se refiere en general a sistemas criptográficos y, más particularmente, a métodos para asegurar tales sistemas cuando se implementan en software.

Antecedentes de la invención

El uso de dispositivos móviles, incluyendo tanto teléfonos móviles como ordenadores de tableta, para comunicaciones de red así como para el almacenamiento y procesamiento de información personal está creciendo rápidamente. La criptografía forma la base para asegurar la información sensible de los usuarios ya que se transmite entre o almacena en tales dispositivos.

En la actualidad, existen dos enfoques generales para asegurar la información de usuario en tales dispositivos. Convencionalmente, Módulos de Seguridad de Hardware (HSM) que proporcionan contenedores seguros a prueba de manipulación para procesamiento criptográfico realizan estas operaciones en hardware, asilados de aplicaciones de software. El primer HSM documentado se describe en la patente de Estados Unidos 4.168.396, 18 de septiembre de 1979, y se diseñó para la protección de copia de software de ordenador personal. Este concepto se extendió posteriormente a un módulo de hardware que proporciona seguridad de datos (Patente de Estados Unidos 4.352.952, 3 de marzo de 1980). Ejemplos de HSM presentes incluyen "tarjetas inteligentes" incorporadas tanto en tarjetas con contacto (normas ISO/IEC 7810 y 7816) así como tarjetas sin contacto (normal ISO/IEC 14443 standard).

En teléfonos móviles y otros dispositivos informáticos, tales HSM habitualmente no están presentes o no están disponibles para aplicaciones de software, y se realiza criptografía dentro del sistema operativo anfitrión, aislado usando mecanismos de sistema operativo. Sin embargo, un atacante o pirata informático que ha obtenido acceso al sistema operativo tiene muchas técnicas disponibles para superar estos mecanismos y, por lo tanto, obtiene acceso a la información del usuario.

Se han usado máquinas virtuales como un medio para separar la ejecución entre un dispositivo informático anfitrión y un sistema operativo de invitado dentro de la máquina virtual. Esto se ha usado para seguridad en la aplicación de políticas de seguridad (Patente de Estados Unidos 2005/0257243, 29 de diciembre de 2005), para evitar que un sistema operativo invitado comprometido sea capaz de afectar al anfitrión (Patente de Estados Unidos 7.409.719, 21 de diciembre de 2004), y para permitir únicamente que aplicaciones de reproductor de medios confiable accedan a medios encriptados en DVD (Patente de Estados Unidos 7.516.331, 26 de noviembre de 2003). Sin embargo, ninguno de estos intenta proteger la información dentro de la máquina virtual cuando se ejecuta en una plataforma de software abierto tal como un sistema operativo de teléfono móvil o de escritorio.

Basándose en lo anterior, puede apreciarse que existe una necesidad de un criptosistema que tiene metodología para asegurar criptografía de software de un observador o atacante no autorizado que ha obtenido acceso al sistema operativo de un dispositivo informático, particularmente cuando el dispositivo informático no tiene los medios para asegurar la información criptográfica en un Módulo de Seguridad de Hardware separado. La presente invención satisface esta u otras necesidades en la técnica.
El documento WO 01/93212 se dirige a un aparato y método para proporcionar una tarjeta inteligente virtual. El aparato incluye una interfaz de tarjeta inteligente y una tarjeta inteligente virtual configurada para emular una tarjeta inteligente física como si se conecta una tarjeta inteligente con la interfaz de tarjeta inteligente.

Sumario de la invención

En las reivindicaciones se expone una invención.
Un sistema criptográfico y metodología construidos de acuerdo con la presente invención comprenden un entorno de pruebas de software seguro que opera como un entorno de pruebas criptográfico, con una capa virtual a prueba de manipulación que rodea el entorno de pruebas para proteger el entorno de pruebas de ingeniería inversa, depuración o manipulación. Una pluralidad de aplicaciones pueden comunicarse con el entorno de pruebas para solicitar que se realicen operaciones criptográficas, y para recuperar los resultados de las operaciones criptográficas del entorno de pruebas.

Breve descripción de los dibujos

La Figura 1 ilustra un diagrama de bloques del sistema de procesamiento de un dispositivo que realiza sistemas y métodos de acuerdo con una realización de esta invención.

La Figura 2 ilustra un diagrama de bloques de componentes del sistema criptográfico de acuerdo con una realización de esta invención.

La Figura 3 ilustra un diagrama de flujo de un proceso de arranque de un sistema criptográfico de acuerdo con una realización de esta invención.

La Figura 4 ilustra un diagrama de flujo de un proceso para acceder a almacenamiento encriptado de acuerdo con una realización de esta invención.

La Figura 5 ilustra un diagrama de flujo de un proceso para acceso confiable del sistema criptográfico a funciones de sistema operativo de acuerdo con una realización de esta invención.

La Figura 6 ilustra un diagrama de flujo de un proceso realizado por el sistema criptográfico para buscar de forma segura actualizaciones de acuerdo con una realización de esta invención.

Descripción detallada de una realización preferida

La siguiente descripción se centrará en una realización de acuerdo con la presente invención, que está habitualmente operativa en un entorno que proporciona software de aplicación ejecutándose en sistemas operativos de iPhone® de Apple o Android® de Google. Sin embargo, realizaciones de acuerdo con esta invención no se limitan a ninguna aplicación particular o ningún entorno particular. De hecho, los expertos en la materia encontrarán que los sistemas y métodos de la presente invención pueden aplicarse de forma ventajosa a una diversidad de software de sistema y de aplicación, incluyendo testigos de seguridad, criptografía de software y encriptación de red. Además, realizaciones de acuerdo con la presente invención pueden realizarse en una diversidad de diferentes plataformas, incluyendo otros sistemas operativos de teléfono móvil tales como RIM Blackberry®, Microsoft® Windows Phone y similares, otros sistemas operativos tales como Apple Mac OS®, Microsoft® Windows, UNIX, y otros entornos operativos tales como navegadores web y dispositivos embebidos y similares. Por lo tanto, la descripción de la realización mostrada de acuerdo con la presente invención que sigue es para propósitos de ilustración y no limitación.

Los procesos para proporcionar métodos y sistemas de acuerdo con esta invención se ejecutan por un dispositivo, tal como, pero sin limitación un teléfono móvil, tableta, miniordenador, ordenador portátil u otro sistema de procesamiento. En la Figura 1 se muestran los componentes pertinentes en un dispositivo que realiza los procesos de acuerdo con una realización de la invención. Un experto en la materia reconocerá que el dispositivo puede incluir otros componentes que se omiten por brevedad sin alejarse de esta invención. El dispositivo 1 incluye un procesador 5, una memoria no volátil 10 y una memoria volátil 15. El procesador 5 es un procesador, microprocesador, controlador o una combinación de procesadores, microprocesador y/o controladores que realiza instrucciones almacenadas en la memoria volátil 15 o memoria no volátil 10 para manipular datos almacenados en la memoria. La memoria no volátil 10 puede almacenar las instrucciones de procesador utilizadas para configurar el procesador 5 para realizar procesos que incluyen procesos de acuerdo con realizaciones de la invención y/o datos para los procesos que se utilizan. En otras realizaciones, el software y/o firmware de dispositivo puede almacenarse en cualquiera de una diversidad de medios legibles por ordenador apropiados para una aplicación específica. Aunque en la Figura 1 se ilustra un dispositivo específico, puede utilizarse cualquiera de una diversidad de dispositivos configurados para almacenar datos criptográficos encriptados y realizar operaciones criptográficas de acuerdo con realizaciones de la invención.

Un sistema criptográfico y metodología construidos de acuerdo con una realización de la presente invención se proporcionan como se muestra en la Figura 2. En la realización descrita, un entorno de pruebas criptográfico 108 proporciona un método para almacenar de forma segura y procesar claves y datos criptográficos para una pluralidad de aplicaciones de cliente 104, con una capa virtual a prueba de manipulación 110 dentro del entorno de pruebas para proteger el procesamiento y datos de observadores no autorizados. El entorno de pruebas criptográfico 108 puede comprender tanto un procesador virtual seguro 109 así como un almacenamiento virtual seguro 119 para permitir que las aplicaciones de cliente 104 realicen tanto procesamiento seguro así como almacenamiento seguro.

El entorno de pruebas criptográfico 108 puede incluir una máquina virtual criptográfica 109 para actuar como el procesador virtual seguro. La máquina virtual criptográfica puede incluir un módulo criptográfico seguro 115 para realizar operaciones criptográficas, incluyendo almacenamiento, recuperación y procesamiento de las claves y datos criptográficos. Estas operaciones criptográficas pueden incluir rutinas criptográficas públicamente disponibles, incluyendo criptografía de clave simétrica tal como AES, criptografía de clave asimétrica tal como RSA, funciones de troceo tal como SHA-1, SHA-2 y HMAC, así como funciones de generación de número pseudoaleatorio y de generación de claves. Esta máquina virtual puede recibir peticiones 106 desde una pluralidad de aplicaciones de cliente para realizar estas operaciones criptográficas procesando de forma segura estas operaciones criptográficas dentro de la máquina virtual y enviando los resultados de estas operaciones criptográficas como una respuesta 107 de vuelta a los clientes. Esta máquina virtual también puede usarse para realizar otras funciones de procesamiento no criptográficas pero críticas para la seguridad.

La máquina virtual 109 puede comprender un intérprete de máquina virtual 111 y un conjunto de códigos de máquina virtual 112. Estos códigos de máquina virtual pueden basarse en arquitectura de conjunto de instrucciones RISC de 32 bits construida solamente para el propósito de ejecución dentro del intérprete de máquina virtual. Esta arquitectura de conjunto de instrucciones puede incluir instrucciones de montaje requeridas para un procesador de ordenador de

fin general, incluyendo instrucciones para el tratamiento de memoria, llamada de función, comparación de resultados, aritmética binaria y aritmética de enteros. La máquina virtual y sistema operativo subyacente 101 pueden ejecutarse en un procesador informático 124. Este procesador informático puede comprender una unidad de procesamiento central de fin general dentro de un teléfono móvil. El sistema operativo subyacente puede comprender un sistema operativo de teléfono móvil. El intérprete de máquina virtual puede incluir adicionalmente técnicas de ocultación 114 para ocultar sus operaciones del sistema operativo subyacente y cualquier observador no autorizado en el mismo. Estas técnicas de ocultación pueden incluir una técnica para cambiar dinámicamente el flujo de ejecución en respuesta a cambios en el sistema operativo subyacente. Esta técnica puede implicar un manejador de retrollamada de función de sistema pasado a la máquina virtual para que la máquina virtual ejecute funciones desde el sistema operativo subyacente y detectar si se han producido estos cambios. El manejador de retrollamada de función de sistema puede proporcionar acceso desde la máquina virtual al sistema de archivos, procesos y memoria del sistema operativo subyacente. El manejador de retrollamada de función de sistema puede proporcionar acceso a funciones de huella de sistema tales como recuperación de identificadores de dispositivo en el sistema operativo subyacente. La máquina virtual determinará, a continuación, basándose en los cambios, si hubiera alguno, cuál debería ser el nuevo flujo de ejecución.

La máquina virtual puede proporcionar un medio para el almacenamiento encriptado seguro 119 de claves y datos criptográficos dentro de la máquina virtual. El almacenamiento seguro puede usarse adicionalmente para almacenar otros datos no criptográficos pero críticos para la seguridad. Este medio puede proporcionarse mediante la escritura 117 en y lectura 118 desde el almacenamiento encriptado. Este archivo encriptado puede almacenarse dentro del sistema de archivos del sistema operativo o dentro de un almacenamiento confiable proporcionado por el sistema operativo. El archivo puede encriptarse por la máquina virtual usando un cifrado de bloques simétrico tal como AES usando una clave de AES. Esta clave de AES puede basarse en una clave secreta conocida únicamente por la máquina virtual. Esta clave de AES puede basarse en una contraseña introducida por el usuario a través de la aplicación de cliente. Esta clave de AES puede generarse basándose en identificadores de hardware y software extraído a partir del dispositivo subyacente. Esta clave de AES puede generarse basándose en una respuesta desde un servidor remoto.

Las aplicaciones de cliente pueden enviar la petición a la máquina virtual y recibir los resultados de las operaciones criptográficas desde la máquina virtual a través de una interfaz de entorno de pruebas 105. La interfaz puede comprender o bien una interfaz de programación tal como una librería de software o una interfaz de red tal como una conexión de red de TCP/IP. Esta interfaz puede comprender un conjunto de llamadas de función de programa para que las aplicaciones de cliente realicen funciones criptográficas o críticas para la seguridad dentro de la máquina virtual. Estas llamadas de función pueden incluir llamadas de función normalmente hechas para el sistema operativo subyacente para tales funciones. Estas llamadas de función también pueden incluir llamadas de función para funciones adicionales realizadas específicamente por la máquina virtual. Estas llamadas de función pueden interceptarse de forma transparente por la máquina virtual de modo que las aplicaciones de cliente pueden continuar usando las llamadas de función nativas expuestas por el sistema operativo subyacente.

El intérprete de máquina virtual también puede proporcionar una función 123 para actualizar de forma segura el conjunto de códigos de máquina virtual desde una parte confiable 122. Los códigos pueden firmarse por la parte confiable y verificarse por la máquina virtual antes de que se permita que el proceso de actualización sustituya el conjunto de códigos de máquina virtual usado por la máquina virtual. El intérprete de máquina virtual puede proporcionar acceso seguro 103 a las funciones 102 en el sistema operativo subyacente. Este acceso puede protegerse por el uso de técnicas para detectar cuándo se han modificado o movido las funciones por un observador externo. Estas técnicas pueden incluir una técnica antienganche, que puede incluir una comprobación de que la dirección de función no se ha cambiado. Estas técnicas pueden incluir un análisis del tiempo que tarda la función en devolver un resultado, que puede incluir una comprobación de que la función no tarda más de una cierta cantidad de tiempo para devolver un resultado. Estas técnicas pueden incluir adicionalmente una técnica para variar la trayectoria de ejecución de modo que un atacante no puede falsificar fácilmente el tiempo transcurrido, ya que el tiempo transcurrido variará con cada ejecución. Esta técnica puede implicar ejecutar un número aleatorio de instrucciones dentro de la máquina virtual entre comprobar el tiempo de sistema de tal forma que la longitud de la trayectoria de ejecución variará con cada ejecución y el tiempo transcurrido también variará con cada ejecución. Esta técnica también puede implicar ejecutar diferentes tipos de instrucciones dentro de la máquina virtual, con el tiempo transcurrido por cada tipo de instrucción conocido para los códigos de máquina virtual, de tal forma que la trayectoria de ejecución incorporará diferentes instrucciones en cada ejecución y el tiempo transcurrido variará con cada ejecución.

La capa virtual a prueba de manipulación 110 puede proteger la máquina virtual de ingeniería inversa almacenando el conjunto de códigos de máquina virtual en una forma encriptada, y desencriptando estas instrucciones en tiempo de ejecución para permitir operación normal de la máquina virtual. La encriptación y desencriptación puede conseguirse a través de la automodificación de códigos de máquina virtual. El intérprete de máquina virtual puede desencriptar estos códigos de máquina virtual de automodificación ejecutando los mismos dentro de la máquina virtual. Puede haber más de una ronda de automodificación realizada por los códigos de máquina virtual para retardar adicionalmente los intentos en ingeniería inversa. Puede haber diferentes datos y algoritmos criptográficos usados en cada ronda de automodificación. Los códigos de automodificación pueden implicar diferentes rutinas de desencriptado con claves de desencriptado, que desencriptan un bloque de código desde una forma encriptada de vuelta a la forma de texto plano,

antes de pasar control de ejecución a los códigos desencriptados. Los códigos de automodificación también pueden implicar sustituir conjuntos de secuencias de instrucciones con otros conjuntos de secuencias de instrucciones que consiguen el mismo resultado de ejecución.

La capa virtual a prueba de manipulación puede proteger la máquina virtual de análisis de tiempo de ejecución empleando técnicas 116 para evitar la depuración de la máquina virtual. Estas técnicas pueden incluir una técnica para evitar que un depurador se acople a la máquina virtual. Estas técnicas pueden incluir una técnica para detectar cuándo se está intentando el uso de un depurador a través del uso de llamadas de autodepuración. Estas técnicas pueden incluir una técnica para redirigir la ejecución de la máquina virtual cuando se usa un depurador explotando diferencias en la ejecución de procesador bajo un depurador. La capa virtual a prueba de manipulación puede detectar manipulación de la máquina virtual a través del uso de múltiples capas de seguridad dentro del código de máquina virtual. Estas capas pueden incluir una capa con comprobaciones de manipulación adicionales dentro de la máquina virtual. Estas comprobaciones de manipulación pueden incluir una comprobación de identificadores de dispositivo únicos para garantizar que la máquina virtual no se ha copiado en una máquina no autorizada. Estas comprobaciones de manipulación pueden incluir una comprobación de las funciones de entorno operativo nativo para garantizar que estas funciones no se han modificado. Estas comprobaciones de manipulación pueden incluir una comprobación del entorno operativo para garantizar que el entorno no se ha modificado. Estas comprobaciones de manipulación pueden incluir una comprobación de la memoria de aplicación para garantizar que la aplicación no se ha modificado. La capa virtual a prueba de manipulación puede proporcionar una función para responder a la manipulación de la máquina virtual. Esta función puede incluir la puesta a cero de información dentro de la máquina virtual. Esta función puede incluir el procesamiento de un conjunto diferente de datos o algoritmos criptográficos.

La capa virtual a prueba de manipulación puede intercalar las técnicas de protección contra ingeniería inversa y las técnicas de protección contra análisis de tiempo de ejecución para convertir inefectiva cualquiera de las formas de análisis. Esto puede incluir una técnica para intercalar las técnicas de análisis de tiempo de ejecución con técnicas de ingeniería inversa que requieren ingeniería inversa manual que requiere mucho tiempo para que un atacante lo eluda. Esto puede incluir una técnica para separar las técnicas de ingeniería inversa con técnicas de análisis de tiempo de ejecución que evitan análisis de tiempo de ejecución automatizado. Esto puede incluir una técnica para repetir estas técnicas múltiples veces dentro de la capa virtual a prueba de manipulación de tal forma que el tiempo total de análisis requerido sería inviable.

La Figura 3 ilustra cómo se inicia este sistema criptográfico de acuerdo con una realización de la invención. El procesador informático 124' inicia el sistema operativo subyacente 101', que a continuación ejecuta las aplicaciones de cliente 104'. Las aplicaciones de cliente pueden enviar peticiones 106' y recibir respuestas 107' a través de una interfaz de entorno de pruebas 105' que inicia y proporciona acceso al entorno de pruebas criptográfico 108'.

Dentro del entorno de pruebas, la máquina virtual criptográfica 109' se inicia cuando se inicia la aplicación, que carga la capa virtual a prueba de manipulación 110'. La máquina virtual, a continuación, carga los códigos encriptados 112' que proporcionan las funciones criptográficas seguras 115', y realiza la desencriptación de tiempo de ejecución 113' usando el intérprete de máquina virtual 111', que expone la capa de ocultación 114' en los códigos encriptados. Los códigos proporcionan, a continuación, las técnicas antidepuración 116' a ejecutarse en la máquina virtual.

La Figura 4 ilustra cómo accede el sistema criptográfico al almacenamiento encriptado de acuerdo con la realización. El intérprete de máquina virtual 111', después de arrancar, realiza escrituras encriptadas 117' en y lecturas encriptadas 118' desde un almacenamiento encriptado 119'. Las lecturas encriptadas y escrituras encriptadas pueden usar una clave de AES almacenada en los códigos encriptados. La información en el almacenamiento encriptado puede comprender otras claves criptográficas 120' u otros datos criptográficos 121'.

La Figura 5 ilustra cómo el sistema criptográfico tiene acceso confiable a funciones de sistema operativo de acuerdo con una realización de esta invención. El intérprete de máquina virtual 111', después de arrancar, verifica las funciones 102' del sistema operativo subyacente 101' antes de llamar a estas funciones para asegurar que el acceso confiable 103' a estas funciones es posible. Esta verificación de funciones puede comprender comprobaciones de apuntador de funciones.

La Figura 6 ilustra cómo el sistema criptográfico busca de forma segura actualizaciones de acuerdo con una realización de esta invención. El intérprete de máquina virtual 111', después de arrancar, se conecta a una parte confiable 112'. Esta conexión puede comprender una conexión de Capa de Conexión Segura (SSL). Si la parte confiable indica que hay disponible una actualización, el intérprete de máquina virtual descargará un conjunto nuevo de códigos encriptados 112' para su uso en la máquina virtual.

**REIVINDICACIONES**

1. Un producto para proporcionar criptografía a aplicaciones realizándose en un dispositivo (1) que comprende:
instrucciones para dirigir una unidad de procesamiento (124) para:
proporcionar un entorno de pruebas criptográfico que incluye:

una máquina criptográfica virtual que realiza operaciones criptográficas, en el que la máquina criptográfica virtual incluye un intérprete de máquina virtual que oculta operaciones de la máquina criptográfica virtual de un sistema operativo subyacente,
una capa a prueba de manipulación dentro de la máquina criptográfica virtual que protege el procesamiento y datos criptográficos de usuarios no autorizados,
una interfaz de entorno de pruebas que recibe peticiones de operaciones criptográficas desde una aplicación de cliente y transmite resultados de las operaciones criptográficas realizadas por la máquina criptográfica virtual a la aplicación de cliente; y
un medio legible por la unidad de procesamiento (124) para almacenar las instrucciones.

2. El producto de la reivindicación 1 en el que las instrucciones para proporcionar el entorno de pruebas criptográfico comprenden además instrucciones para que el entorno de pruebas criptográfico incluya:
un almacenamiento virtual seguro para almacenar claves y datos criptográficos.

3. El producto de la reivindicación 2 en el que el almacenamiento virtual seguro está dentro de un espacio de memoria de la máquina criptográfica virtual.

4. El producto de la reivindicación 2 en el que el almacenamiento virtual seguro está fuera de la máquina criptográfica virtual.

5. El producto de la reivindicación 5 en el que las instrucciones para proporcionar el intérprete de máquina virtual incluyen instrucciones para dirigir la unidad de procesamiento (124) para:

recibir una llamada de función desde un sistema operativo subyacente en el intérprete de máquina,
verificar la llamada de función con el intérprete de máquina, y
realizar la llamada de función en la máquina criptográfica virtual en respuesta a la llamada de función que se verifica.

6. El producto de la reivindicación 1 en el que las instrucciones para proporcionar el entorno de pruebas criptográfico comprenden además instrucciones para proporcionar a la máquina criptográfica virtual un módulo criptográfico que realiza las operaciones criptográficas.

7. El producto de la reivindicación 1 en el que las instrucciones para proporcionar la capa a prueba de manipulación incluyen instrucciones que proporcionan un conjunto de códigos de máquina virtual en una forma encriptada que se desencriptan en tiempo de ejecución para permitir operación normal de la máquina criptográfica virtual.

8. Un método para proporcionar un entorno de pruebas criptográfico virtual que incluye una máquina criptográfica virtual para realizar operaciones criptográficas en un dispositivo con un sistema de procesamiento, comprendiendo el método:

recibir una petición para realizar una operación criptográfica desde una aplicación en una interfaz de entorno de pruebas realizada por el sistema de procesamiento;
realizar la operación criptográfica usando la máquina criptográfica virtual que se realiza por el sistema de procesamiento,
ocultar, usando un intérprete de máquina virtual proporcionado dentro de la máquina criptográfica virtual, las operaciones de la máquina criptográfica virtual de un sistema operativo subyacente,
proporcionar una capa a prueba de manipulación dentro de la máquina criptográfica virtual que protege el procesamiento y datos criptográficos de usuarios no autorizados, y transmitir un resultado de la operación criptográfica usando la interfaz de entorno de pruebas.

9. El método de la reivindicación 8, que comprende adicionalmente:

almacenar claves y datos encriptados y un almacenamiento encriptado, y
acceder a las claves y datos encriptados para realizar la operación criptográfica.

10. El método de la reivindicación 9 en el que el almacenamiento encriptado está dentro de un espacio de memoria de la máquina criptográfica virtual.

11. El método de la reivindicación 9 en el que el almacenamiento encriptado está dentro de un espacio de memoria de un sistema operativo subyacente.

12. El método de la reivindicación 11, que comprende adicionalmente:

recibir una llamada de función desde un sistema operativo subyacente en el intérprete de máquina,
verificar la llamada de función con el intérprete de máquina, y
realizar la llamada de función en la máquina criptográfica virtual en respuesta a la llamada de función que se verifica.

13. El método de la reivindicación 8, que comprende adicionalmente:
realizar las operaciones criptográficas en un módulo criptográfico de máquina criptográfica virtual.

14. Un medio legible por ordenador que almacena software para provocar que se efectúe el método de cualquiera de las reivindicaciones 8-13.

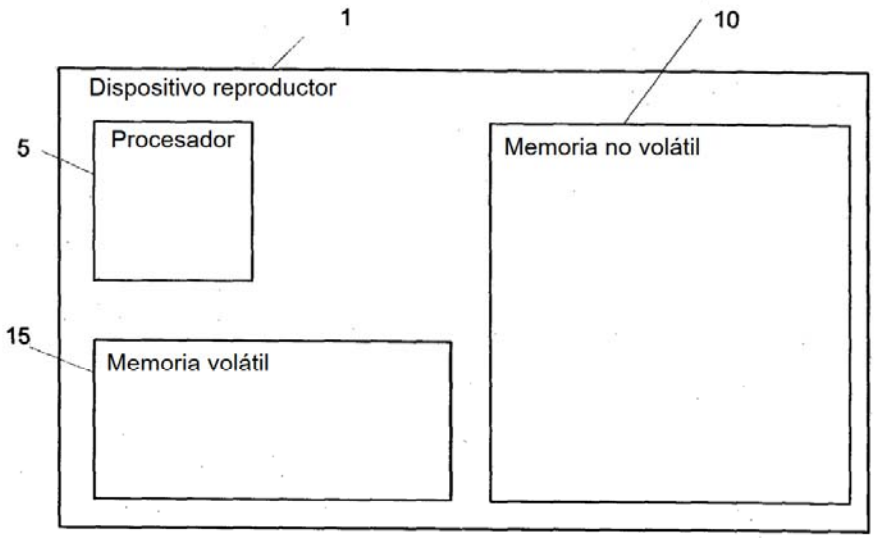
1
10
Dispositivo reproductor
5
Procesador
Memoria no volátil
15
Memoria volátil

**Figura 1**

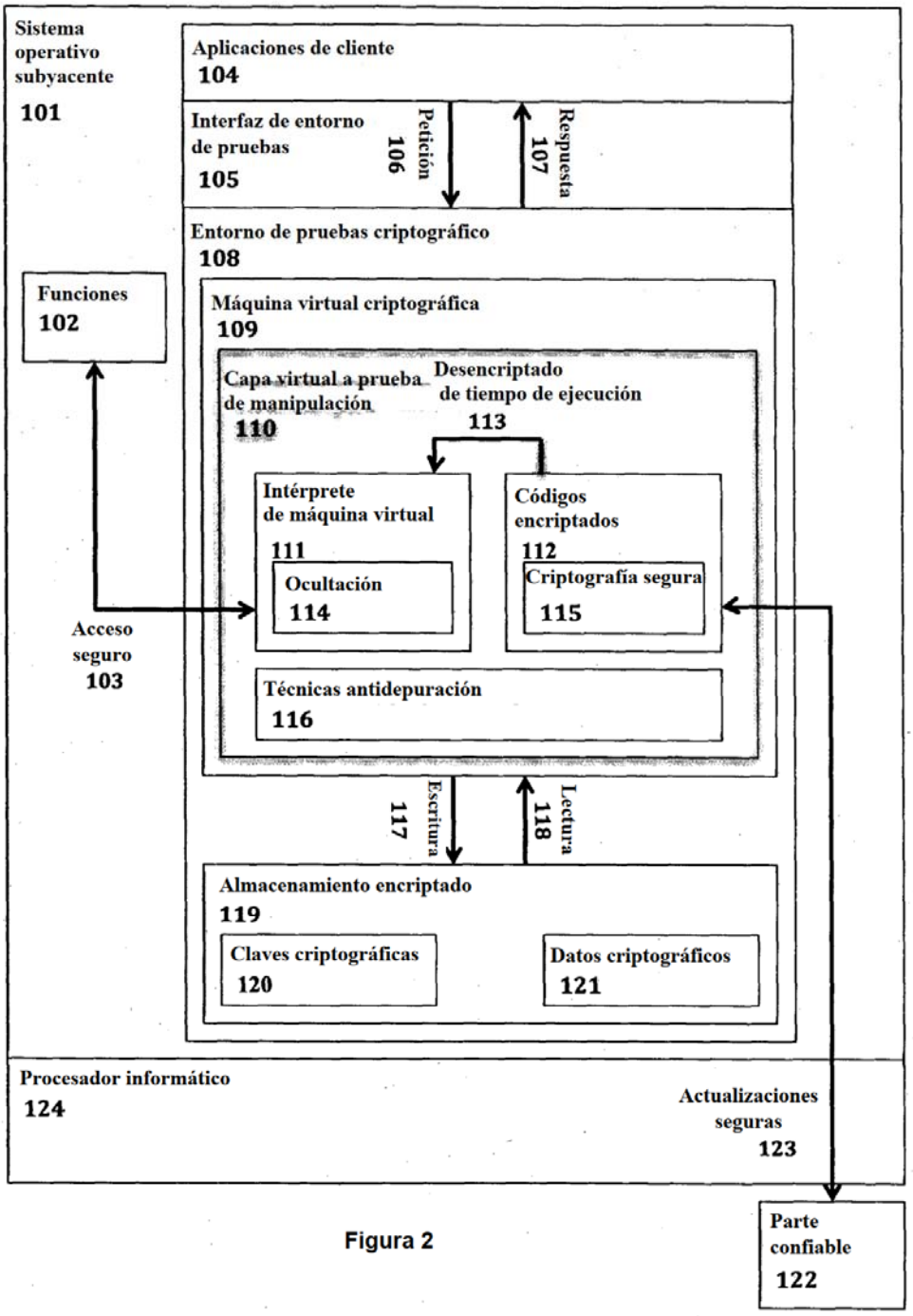
Sistema operativo subyacente
101
Aplicaciones de cliente
104
Interfaz de entorno de pruebas
105
Petición
106
Respuesta
107
Entorno de pruebas criptográfico
108
Funciones
102
Máquina virtual criptográfica
109
Capa virtual a prueba de manipulación
110
Desencriptado de tiempo de ejecución
113
Intérprete de máquina virtual
111
Ocultación
114
Códigos encriptados
112
Criptografía segura
115
Técnicas antidepuración
116
Acceso seguro
103
Escritura
117
Lectura
118
Almacenamiento encriptado
119
Claves criptográficas
120
Datos criptográficos
121
Procesador informático
124
Actualizaciones seguras
123
Parte confiable
122

Figura 2

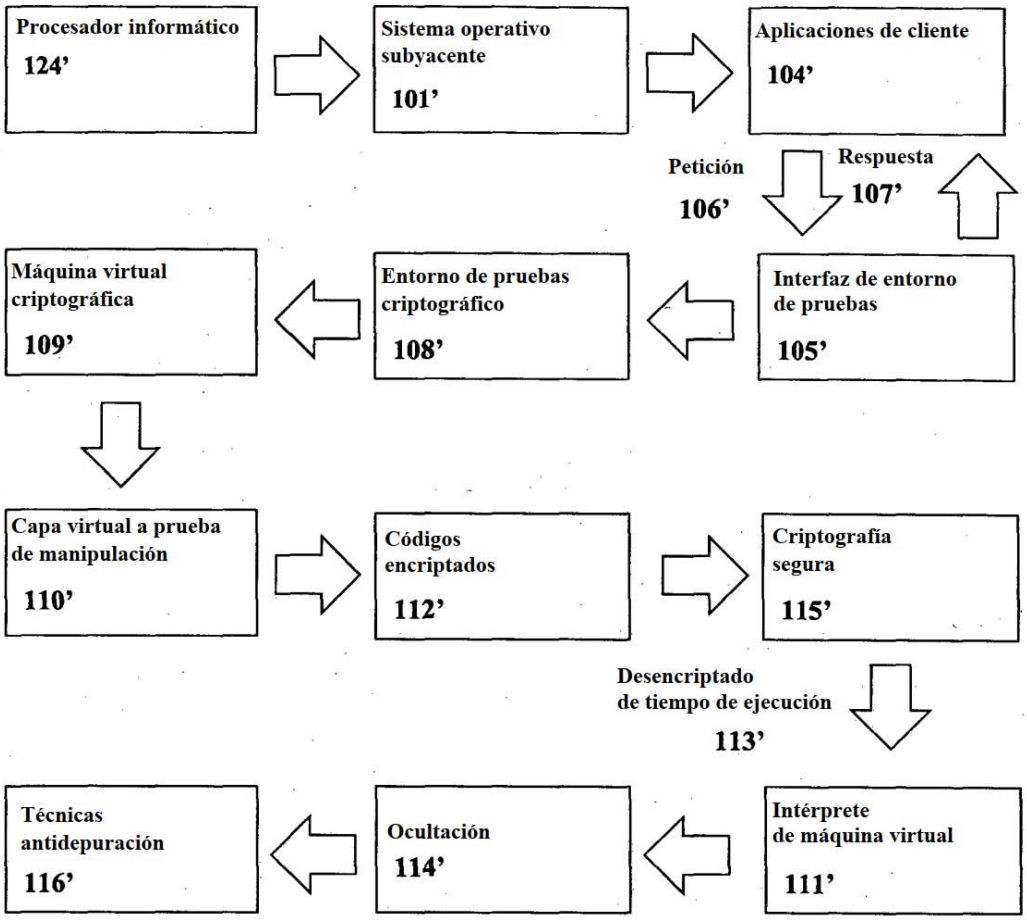
Procesador informático
124'
Sistema operativo subyacente
101'
Aplicaciones de cliente
104'
Petición
106'
Respuesta
107'
Máquina virtual criptográfica
109'
Entorno de pruebas criptográfico
108'
Interfaz de entorno de pruebas
105'
Capa virtual a prueba de manipulación
110'
Códigos encriptados
112'
Criptografía segura
115'
Desencriptado de tiempo de ejecución
113'
Técnicas antidepuración
116'
Ocultación
114'
Intérprete de máquina virtual
111'

**Figura 3**

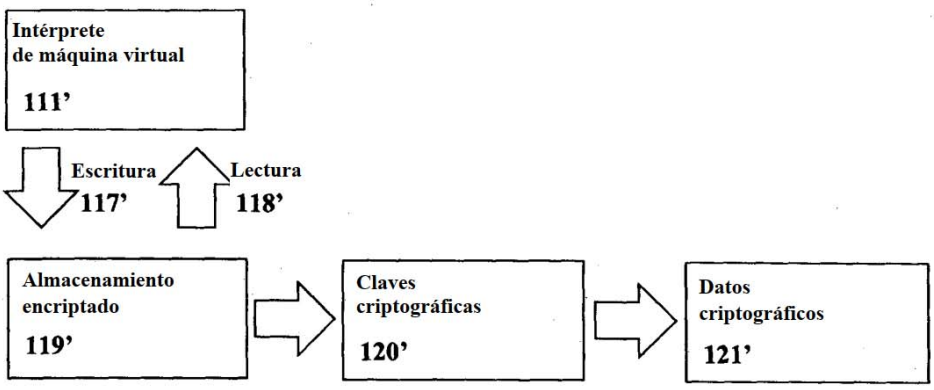


Figura 4

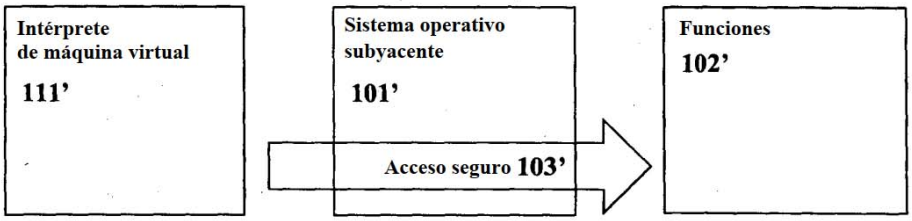


Figura 5

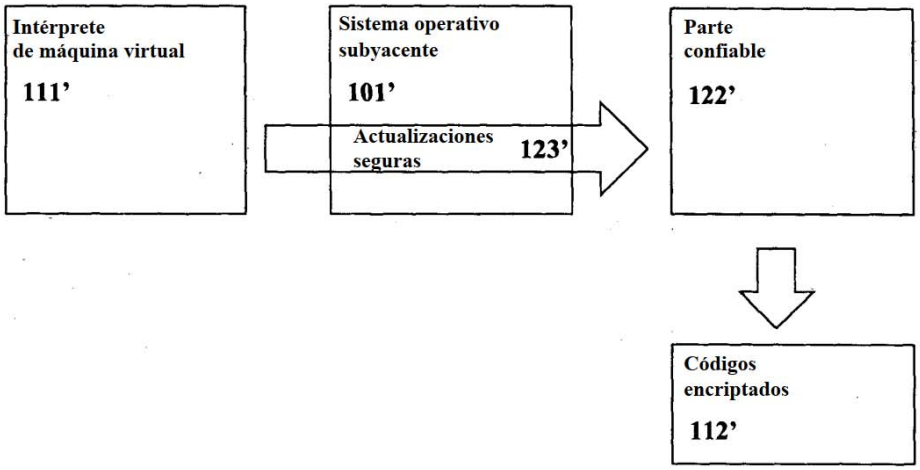


Figura 6