(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 611 408**

(51) Int. CI.:

G06F 21/60 (2013.01)
G06F 21/72 (2013.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.10.2003 PCT/SE2003/001660**

(87) Fecha y número de publicación internacional: **13.05.2004 WO04040397**

(96) Fecha de presentación y número de la solicitud europea: **27.10.2003 E 03772980 (3)**

(97) Fecha y número de publicación de la concesión europea: **19.10.2016 EP 1556992**

(54) Título: **Implementación y utilización segura de datos de seguridad específicos de dispositivo**

(30) Prioridad:

31.10.2002 US 422498 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.05.2017

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

SMEETS, BERNARD;
SELANDER, GÖRAN y
NERBRANT, PER-OLOF

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Implementación y utilización segura de datos de seguridad específicos de dispositivo

CAMPO TÉCNICO DE LA INVENCIÓN

La presente invención se refiere en general a la gestión, implementación y utilización de datos de seguridad específicos de dispositivo para diversos fines y, más particularmente, a procedimientos seguros y eficientes para proporcionar dispositivos con tales datos de seguridad específicos de dispositivo.

ANTECEDENTES DE LA INVENCIÓN

Existe una necesidad general de implementar y utilizar datos de seguridad específicos de dispositivo en una amplia variedad de dispositivos diferentes tales como teléfonos móviles, ordenadores personales, cámaras, dispositivos de audio, servidores, estaciones base y cortafuegos. Los datos de seguridad específicos de dispositivo pueden utilizarse para diversos fines, incluida la gestión de problemas de seguridad con relación a la comunicación a través de redes inseguras, a la marcación de contenido de contenido digital y demás.

Para facilitar la comprensión de una justificación detrás de la presente invención, puede ser útil pensar en el proceso de fabricación de dispositivos en grandes volúmenes. En particular, puede ser útil, por ejemplo, considerar un fabricante de dispositivos, con una confianza limitada en cualquier tercero (en particular fabricantes de chips de terceros), que necesita producir dispositivos que contengan protección a prueba de manipulaciones indebidas y claves criptográficas únicas por dispositivo y/u otros datos de seguridad a un bajo costo.

En la comunicación en red, por ejemplo, la seguridad de los datos suele basarse en algún tipo de datos de seguridad, por ejemplo, una clave criptográfica, que se utiliza para establecer la confidencialidad de datos, integridad de datos, autenticación, autorización, no repudio y/u otros servicios de seguridad. Con el rápido desarrollo de Internet, redes de telecomunicaciones de paquetes de datos y otras redes de comunicaciones, se ha vuelto cada vez más importante poder proporcionar una seguridad de datos apropiada, tal como proteger mensajes intercambiados entre nodos y/o dispositivos en la red. Para simplificar, cualquier entidad que participe en dicha comunicación se denominará dispositivo de red, y ejemplos incluyen teléfonos móviles, ordenadores personales, puertas de enlace de seguridad, cortafuegos, estaciones base de radio y así sucesivamente.

Existen varias dificultades en la fabricación segura y rentable de dispositivos con datos de seguridad que pueden utilizarse posteriormente, por ejemplo, para problemas de seguridad relacionados con la comunicación en red:

- Para instalar o implementar datos de seguridad específicos de dispositivo, diferentes para cada dispositivo. Esto puede requerir procesos de fabricación totalmente nuevos para algunos componentes del dispositivo y, por lo tanto, resultar costosos y/o ineficientes.
- Para colocar los datos de seguridad en una ubicación dentro del dispositivo de tal forma que no puedan ser comprometidos o manipulados por personas no autorizadas.
- Para garantizar que los datos de seguridad estén protegidos de partes no autorizadas durante todo el proceso de fabricación del dispositivo. En particular, si participan partes no confiables durante la fabricación, puede ser necesaria una gestión de seguridad adicional.
- Para administrar de forma segura la información relacionada con los datos de seguridad, que es necesaria para que una parte autorizada pueda posteriormente proporcionar seguridad de datos con relación al dispositivo como, por ejemplo, configurar una conexión segura con el dispositivo. Por ejemplo, si los datos de seguridad del dispositivo son una clave secreta compartida en un protocolo criptográfico, como un protocolo de autenticación y/o encriptado, la misma clave debe estar disponible, y sólo disponible, para el(os) socio(s) de comunicaciones autorizado(s) que debe ser capaz(ces) de configurar la conexión segura con el dispositivo.

Por ejemplo, muchos sistemas de comunicación de hoy en día, incluyendo sistemas de comunicación móvil, sistemas de paginación, así como redes de datos inalámbricas y de cable, emplean procedimientos de autenticación y encriptado con el propósito de mejorar la seguridad y robustez del sistema. El problema de establecer una comunicación segura y robusta se encuentra en muchas aplicaciones técnicas, que van desde la comunicación general de la red hasta aplicaciones más específicas como la Gestión de Derechos Digitales (DRM, por sus siglas en inglés).

En general, hay dos soluciones para almacenar datos de seguridad en un dispositivo, ya sea en un chip o en un circuito integrado (CI) o en algún tipo de memoria programable, por ejemplo, una PROM, teniendo en cuenta que los datos almacenados en un CI están generalmente más protegidos.

En la referencia [1], una clave maestra se almacena en la EEPROM de una tarjeta inteligente y se utiliza para encriptar información sensible para ser almacenada en un medio de almacenamiento relativamente menos seguro.

La referencia [2] describe un procesador, que está conectado a un dispositivo externo con el propósito de descargar

un programa desde el dispositivo externo a su memoria RAM. Si el programa está encriptado, un módulo de desencriptado dispuesto en el procesador accede a una clave permanentemente almacenada en el procesador para desencriptar la información del programa.

La referencia [3] menciona la denominada generación de claves a bordo con relación a las tarjetas inteligentes.

La patente US 5 623 637A describe una tarjeta de memoria PCMCIA que incorpora un circuito integrado de tarjeta inteligente para almacenar un valor de contraseña y circuitería lógica para impedir el acceso a información, a menos que el usuario de un ordenador host al que está conectada la tarjeta de memoria suministre una contraseña que coincida con la contraseña almacenada.

El documento EP 0 750 410 A describe una disposición para generar y gestionar una clave secreta de un criptosistema de clave pública. En particular, se genera una clave secreta dentro de un dispositivo a prueba de manipulación indebida incluido en la disposición que comprende, además, medios para escribir la clave secreta y un certificado en un dispositivo personal insertado en la disposición. La escritura de información de seguridad se inicia proporcionando una contraseña. Además, la escritura y su almacenamiento en el dispositivo personal está dispuesta de tal manera que la clave secreta no se pueda leer allí mientras el dispositivo personal se inserta en la disposición.

El documento "La tarjeta inteligente en la futura red europea de telecomunicaciones móviles digitales" (SMART CARD 2000 CONFERENCE, 4 de octubre de 1989 (04-10-1989), páginas 85 - 92, XP000534136 AMSTERDAM, NL; HENNY J.W.M VAN DE PAVERT) describe una tarjeta inteligente para uso, por ejemplo, en un teléfono móvil como un testigo personal. La tarjeta inteligente contiene un secreto, compartido con una red de comunicaciones, que no está disponible en una interfaz de tarjeta. La tarjeta inteligente contiene además medios para realizar operaciones criptográficas y, en particular, se puede generar una clave disponible en una interfaz de tarjeta para encriptar datos comunicados entre un teléfono móvil y un nodo de red.

El almacenamiento de datos secretos, por ejemplo, un número aleatorio específico de dispositivo, en un CI es posible hoy en día con las herramientas estándar de producción de CI. Sin embargo, la logística para pasar de forma segura el número aleatorio o algunos datos relacionados desde el fabricante de CI al fabricante del dispositivo donde se utiliza el CI es con las técnicas actuales inviable/costoso y/o requiere una gestión de seguridad especial para manejar los datos de seguridad. En general, el fabricante del dispositivo y el fabricante del CI pueden ser partes diferentes. Si algunos datos de seguridad son administrados por el fabricante de CI, esto puede constituir una debilidad de seguridad, un posible blanco de ataques y también puede aumentar los costos del CI.

El mismo argumento se aplica al fabricante de CI que genera y/o almacena claves criptográficas en un CI en nombre de un fabricante de dispositivos.

El fabricante del dispositivo puede permitir que el fabricante de CI almacene en el CI datos que no es posible extraer después de la fabricación del CI, a menos que se trate de una ingeniería inversa muy avanzada. Sin embargo, el uso de estos datos de dispositivo en un contexto de seguridad con la ayuda de técnicas de vanguardia requiere una gestión de seguridad en y entre el fabricante de CI y el fabricante de dispositivos y no es seguro o inviable/costoso en un proceso de industrialización, en particular Para un mercado masivo.

El fabricante del dispositivo puede insertar datos de seguridad en PROM, evitando así incluir al fabricante de CI como un tercero de confianza y evitando también costosos cambios en el proceso de fabricación de CI. Sin embargo, los secretos en PROM no están tan bien protegidos contra un adversario con acceso (aunque sea sólo temporal) al dispositivo. Además, la tecnología ASIC (Circuito Integrado de Aplicación Específica) requerida para la realización de la funcionalidad PROM induce costes adicionales considerables en el CI, por ejemplo, a través de máscaras adicionales en el proceso de producción del CI.

Además, el fabricante de CI puede querer limitar el uso de sus ICs a los fabricantes de dispositivos con los que confía o tiene acuerdos comerciales.

Un problema algo diferente, pero aún relacionado, es que un tercero, con relaciones de confianza con el fabricante del dispositivo y/o el usuario, se comunique de forma segura con el dispositivo o con un usuario del dispositivo. La gestión de seguridad de los datos de seguridad específicos de dispositivo puede requerir la inclusión de otras partes.

SUMARIO DE LA INVENCIÓN

La presente invención supera estos y otros inconvenientes de las disposiciones de la técnica anterior.

Un objeto de la invención es implementar y utilizar datos de seguridad específicos de dispositivo en dispositivos tales como teléfonos móviles, ordenadores personales, cámaras, dispositivos de audio, servidores, estaciones base y cortafuegos.

Es un objeto de la invención proporcionar un método para fabricar de forma segura y rentable un dispositivo con

capacidades de datos de seguridad, así como un método para gestionar datos de seguridad. En particular, es deseable proporcionar al dispositivo protección contra manipulaciones indebidas y datos de seguridad específicos de dispositivo. También es importante garantizar que los datos de seguridad estén protegidos de partes no autorizadas durante todo el proceso de fabricación del dispositivo, sin necesidad de una gestión de seguridad extensiva.

Otro objeto de la invención es proporcionar un método mejorado para mantener la seguridad de los datos con relación a la comunicación en red entre un dispositivo de red y un socio de comunicación externo.

Otro objeto más de la invención es proporcionar un método mejorado para marcar contenido digital producido por un dispositivo productor de contenido.

Una idea básica, de acuerdo con la invención, es proporcionar un circuito electrónico a prueba de manipulación indebida que está configurado para su implementación en un dispositivo y que implementa y utiliza de forma segura datos de seguridad específicos de dispositivo durante su funcionamiento en el dispositivo. El circuito electrónico a prueba de manipulación indebida está provisto básicamente de un secreto almacenado a prueba de manipulaciones indebidas que no es accesible a través de una interfaz de circuito externo. El circuito electrónico también está provisto de funcionalidad para realizar el procesamiento criptográfico al menos parcialmente en respuesta o basado en el secreto almacenado para generar una instancia de datos de seguridad específicos de dispositivo que está internamente confinada dentro de dicho circuito electrónico durante el uso del dispositivo. El circuito electrónico está configurado además para realizar una o más operaciones o algoritmos relacionados con la seguridad en respuesta a los datos de seguridad específicos de dispositivo internamente confinados.

De esta forma, la implementación segura y la utilización de datos de seguridad específicos de dispositivo con fines de seguridad se pueden lograr de manera efectiva. La seguridad no queda comprometida, ya que el secreto almacenado nunca está disponible fuera del circuito electrónico, y los datos de seguridad específicos de dispositivo están internamente confinados dentro del circuito durante el uso o el funcionamiento del dispositivo. Esto significa que los datos de seguridad específicos de dispositivo se mantienen indisponibles desde la interfaz de programación de circuito externo y sólo pueden usarse dentro del circuito para realizar una operación relacionada con la seguridad durante el uso y el funcionamiento del dispositivo. Como ejemplo particular, los datos de seguridad específicos de dispositivo pueden usarse junto con una operación relacionada con la seguridad para convertir la información de entrada encriptada en información de salida de texto claro sin revelar el secreto almacenado o los datos de seguridad específicos de dispositivo en sí. La operación relacionada con la seguridad puede ser una operación simple, tal como el descifrado de información encriptada, o una operación compuesta más compleja.

El circuito electrónico puede ser un circuito integrado (CI), una tarjeta inteligente o cualquier otro circuito electrónico a prueba de manipulación indebida, aunque preferiblemente sea un circuito encapsulado.

El circuito electrónico a prueba de manipulación indebida, de acuerdo con la invención, es aplicable generalmente en una amplia variedad de dispositivos, produciendo datos de seguridad específicos de dispositivo internamente confinados que se pueden usar para diversos propósitos relacionados con la seguridad.

El circuito electrónico puede, por ejemplo, estar dispuesto en un dispositivo de red, y los datos de seguridad específicos de dispositivo manejados por el circuito en funcionamiento dentro del dispositivo de red pueden usarse entonces para operaciones de seguridad de datos en la comunicación de red incluyendo confidencialidad de los datos, integridad de los datos, autenticación, autorización y no repudio. Un ejemplo específico consiste en asegurar la comunicación sobre redes inseguras, incluyendo Internet y redes de comunicación celular.

En otro escenario de aplicación, el circuito electrónico está dispuesto en un dispositivo que produce contenido digital, y los datos de seguridad específicos de dispositivo manejados por el circuito en funcionamiento dentro del dispositivo productor de contenido pueden usarse entonces, por ejemplo, para marcar el contenido digital producido generando una huella digital específica del dispositivo integrada en el contenido digital.

Más específicamente, en la fabricación de circuitos, preferiblemente se almacena de forma segura un secreto aleatorio dentro del circuito electrónico tal como un CI. Esto podría ser implementado de tal manera que ni siquiera el fabricante del circuito conoce el secreto. Estos datos secretos pueden ser cualquier número arbitrario o generado aleatoriamente que pertenece típicamente a un gran conjunto de números para evitar ataques de adivinación o precomputación. Además, el circuito electrónico está preferiblemente provisto de algoritmo(s) de seguridad o criptográfico(s) implementado(s) para su ejecución en el circuito electrónico con el secreto como entrada (al menos parcial). Una vez que el fabricante del dispositivo instala el circuito electrónico para su funcionamiento en el dispositivo, el secreto almacenado puede usarse junto con el algoritmo o algoritmos de seguridad criptográfica para generar una instancia de datos de seguridad que es específica para el dispositivo particular en el cual el circuito electrónico está implementado.

De este modo, el secreto almacenado y el algoritmo o algoritmos criptográficos implementados en el circuito electrónico permiten la generación de datos de seguridad específicos de dispositivo confinados de forma segura, por

ejemplo, claves de encriptado y desencriptado, claves de enlace, claves simétricas, claves públicas privadas y asociadas y/u otros datos de seguridad específicos de dispositivo que se pueden utilizar para diversas operaciones de seguridad.

En particular, es claramente ventajoso ser capaz de generar datos de seguridad específicos de dispositivo y proporcionar funcionalidad de seguridad completa basada en cualquier dato secreto, aleatorio que se almacena originalmente en el circuito electrónico por el fabricante del circuito (CI). Es más, el circuito electrónico permite la generación y gestión de datos de seguridad específicos de dispositivo para una amplia gama de dispositivos en los que se puede disponer el circuito. Además, puesto que los datos secretos se almacenan de forma segura en el circuito, no hay necesidad de una gestión de seguridad extensiva en la fabricación del dispositivo o en la distribución de circuitos entre el fabricante del circuito (CI) y el fabricante del dispositivo.

El procesamiento criptográfico implementado en el circuito electrónico se basa preferentemente en una función o algoritmo criptográfico diseñado de manera que sea computacionalmente imposible deducir el resultado del algoritmo sin conocer el secreto, y/o deducir el secreto del resultado.

El secreto puede ser la única entrada al algoritmo o algoritmos criptográficos implementados en el circuito. Alternativamente, se pueden suministrar datos de entrada adicionales y usarse junto con el secreto del algoritmo o algoritmos para generar los datos de seguridad específicos de dispositivo. Preferentemente, los datos de activación requeridos para generar datos de seguridad específicos de dispositivo se definen durante la configuración del dispositivo, por ejemplo, en una fase de configuración durante la fabricación o durante la configuración del usuario. Durante el uso del dispositivo, los datos de activación predeterminados tienen que aplicarse sobre una interfaz de circuito externo para poder generar datos de seguridad adecuados. A menos que se apliquen los datos de activación correctos, el procesamiento criptográfico en el circuito electrónico normalmente sólo genera datos sin sentido o no funciona en absoluto. Esto implica que el circuito electrónico requiere típicamente una cierta forma de datos de activación predeterminados para volver a generar internamente los datos de seguridad específicos de dispositivo.

Si los datos de activación se definen durante la fabricación del dispositivo o en conexión al mismo, los datos de activación pueden tener que ser transferidos de forma segura desde el fabricante del dispositivo al dispositivo a través de una parte de confianza intermedia como un operador de red al que el usuario del dispositivo es asociado. Alternativamente, los datos de activación son definidos por otra parte configuradora tal como el operador de red y transferidos de forma segura al dispositivo. También es posible almacenar los datos de activación predeterminados en el dispositivo ya durante la configuración para facilitar el acceso cuando se necesita invocar los datos de seguridad específicos de dispositivo para una operación relacionada con la seguridad. Esto significa que un adversario con acceso físico al dispositivo puede obtener acceso a los datos de activación o código para realizar la operación relacionada con la seguridad. Sin embargo, el adversario nunca tendrá acceso a los datos de seguridad específicos de dispositivo en sí. Además, se puede obtener un mayor grado de seguridad protegiendo el código de activación almacenado con una contraseña seleccionada por el usuario.

Por ejemplo, los datos de activación o el código pueden definirse basándose en datos de configuración de seguridad específicos de dispositivo proporcionados durante la configuración del dispositivo. Preferentemente, el circuito electrónico está configurado para generar los datos de activación como una representación criptográfica de los datos de configuración de seguridad específicos de dispositivo, basados en el secreto almacenado, en donde la representación criptográfica es emitida a través de una interfaz de circuito externo durante la fase de configuración. Durante el uso del dispositivo, los datos de seguridad específicos de dispositivo se vuelven a generar internamente siempre que dicha entrada adicional corresponda a la representación criptográfica. Los datos de configuración de seguridad pueden proporcionarse a través de una interfaz de circuito externo durante la configuración, permitiendo al fabricante del dispositivo u otra parte de confianza seleccionar libremente datos de seguridad específicos de dispositivo para los dispositivos fabricados. Sin embargo, también es posible generar internamente los datos de configuración de seguridad en el circuito electrónico durante la fase de configuración.

En otra realización de la invención, la cual se refiere a la criptografía asimétrica, se puede aplicar al circuito una entrada adicional adecuada tal como un primo, un generador de un grupo matemático, un valor nonce y/o un código PIN durante la configuración del dispositivo, por ejemplo, durante una fase de configuración en la fabricación o durante la configuración del usuario, para generar un par de claves asimétricas y para emitir la clave pública a través de una interfaz de circuito externo. Durante el uso del dispositivo, la clave privada correspondiente se genera internamente o se vuelve a generar siempre que al menos parte de la misma entrada adicional se aplique sobre una interfaz de circuito externo.

Alternativamente, los datos de activación pueden ser una simple simiente, tal como un valor nonce, una denominada identidad de enlace o similar, que se aplica inicialmente al circuito electrónico durante la configuración del dispositivo, obligando al circuito electrónico a emitir datos de seguridad específicos de dispositivo a través de una interfaz de circuito externa en respuesta a un código de acceso del dispositivo llamado. El código de acceso de dispositivo puede utilizarse para hacer que los datos de seguridad específicos de dispositivo estén disponibles fuera del circuito bajo ciertas circunstancias, típicamente en un entorno controlado durante la fabricación del dispositivo,

mientras que los datos de seguridad siempre están internamente confinados dentro del circuito electrónico durante el uso del dispositivo.

En general, el circuito electrónico puede estar provisto de un protocolo de autenticación para requerir autenticación para conceder acceso a cierta funcionalidad en el circuito, restringiendo con ello de manera efectiva el uso del circuito a partes autorizadas. Típicamente, el circuito electrónico está configurado para autenticar al fabricante del dispositivo u otra parte configuradora, y para proporcionar un código de acceso del dispositivo al fabricante del dispositivo en respuesta a una autenticación exitosa. Por ejemplo, el código de acceso del dispositivo puede ser generado como un par de respuestas-desafío basado en un desafío del fabricante del dispositivo y el secreto almacenado en el circuito electrónico. El circuito electrónico también se puede configurar para desactivar el acceso interno al secreto almacenado y/o los datos de seguridad específicos de dispositivo, a menos que se introduzca un código de acceso de dispositivo predeterminado en el circuito electrónico. De esta forma, se puede garantizar que sólo una parte autorizada, como el fabricante del dispositivo y/o una parte de confianza, pueda utilizar el secreto almacenado para generar datos de seguridad específicos de dispositivo y/o utilizar los datos de seguridad en sí.

Debe entenderse que pueden definirse múltiples señales individuales de datos de activación durante la configuración del dispositivo, en la que cada señal de datos de activación está asociada con un respectivo dato de seguridad específico del dispositivo. El circuito electrónico se configura entonces para generar datos de seguridad específicos de dispositivo, siempre que la señal de datos de activación asociada se aplique al circuito. Esta característica puede utilizarse para proporcionar un módulo de identidad multiusuario, tal como un SIM multiusuario (Módulo de Identidad del Subscriptor) para autenticación y propósitos de acuerdo clave, o un decodificador multicanal, tal como un decodificador de televisión por satélite o por cable, donde se requieren múltiples claves de seguridad únicas.

La invención también se refiere a una gestión de seguridad adicional asociada con los datos de seguridad específicos de dispositivo, por ejemplo, certificación y delegación de confianza, con el fin de permitir que terceros de confianza se comuniquen de forma segura con el dispositivo de red y/o el usuario.

La invención ofrece las siguientes ventajas:

- Implementación y utilización seguras y rentables de datos de seguridad específicos de dispositivo con fines de seguridad;
- Seguridad rigurosa, ya que el secreto almacenado nunca está disponible fuera del circuito y los datos de seguridad específicos de dispositivo están internamente confinados dentro del circuito durante el uso del dispositivo;
- Protección eficiente de los datos de seguridad específicos de dispositivo dentro de un circuito electrónico a prueba de manipulación indebida;
- Capacidad para generar datos de seguridad específicos de dispositivo y proporcionar funcionalidad de seguridad total basada en cualquier información aleatoria secreta que originalmente se almacena en el circuito por el fabricante del circuito (CI);
- Requiere solo una muy limitada confianza en el fabricante del circuito (CI);
- No es necesaria una gestión de seguridad extensiva en la fabricación del dispositivo y/o entre el fabricante del circuito y el fabricante del dispositivo;
- Uso eficiente de datos de activación para permitir la generación de datos de seguridad específicos de dispositivo;
- Posibilidad de restringir el uso de ciertas funcionalidades en el circuito a las partes autorizadas;
- La provisión de datos de seguridad específicos de dispositivo en combinación con el denominado protocolo de delegación de confianza genérica o una estructura de certificación de dispositivo proporciona una solución factible y aplicable al problema de la gestión de claves para la gestión segura de derechos digitales; y
- Se abre para módulos de identidad multiusuario y decodificadores multicanal.

Otras ventajas ofrecidas por la presente invención se apreciarán tras la lectura de la siguiente descripción de las realizaciones de la invención.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La invención, junto con otros objetivos y ventajas de la misma, se entenderán mejor con referencia a la siguiente descripción tomada junto con los dibujos adjuntos, en los cuales:

La Figura 1 es un diagrama de bloques esquemático de un dispositivo general provisto de un circuito electrónico a prueba de manipulación indebida de acuerdo con una realización básica preferida de la invención;

La Figura 2 es un diagrama de bloques esquemático de un circuito electrónico para su implementación en un dispositivo de red, y configurado para realizar operaciones de seguridad de datos en comunicación de red basadas en datos de seguridad específicos de dispositivo;

La Figura 3 es un diagrama de bloques esquemático de un circuito electrónico para su implementación en un dispositivo productor de contenido digital, y configurado para realizar marcado de contenido basado en datos

de seguridad específicos de dispositivo;
La Figura 4 es un diagrama de flujo esquemático de un método para fabricar un dispositivo con capacidades de datos de seguridad, incluyendo la gestión de datos de seguridad específicos de dispositivo, de acuerdo con una realización preferida de la invención;
La Figura 5 es un diagrama de flujo esquemático que ilustra la configuración y el uso de datos de activación de acuerdo con una realización ejemplar de la invención;
La Figura 6 es un diagrama de bloques esquemático de un circuito electrónico a prueba de manipulación indebida provisto de funcionalidad para encriptar datos de seguridad configuracionales en datos de activación, de acuerdo con una realización preferida de la invención;
La Figura 7 es un diagrama de bloques esquemático de una realización particular del circuito de la Figura 6 con otras mejoras de seguridad utilizando una clave de entrada adicional;
La Figura 8 es un diagrama de bloques esquemático de un circuito electrónico a prueba de manipulación indebida provisto de la funcionalidad de código de acceso del dispositivo para permitir el acceso externo a los datos de seguridad generados durante la configuración, de acuerdo con otra realización preferida de la invención;
La Figura 9 es un diagrama de bloques esquemático de un circuito electrónico a prueba de manipulación indebida capaz de responder a datos de activación para generar selectivamente un par de claves asimétricas/clave privada de acuerdo con otra realización preferida de la invención;
La Figura 10 es un diagrama de bloques esquemático de una realización particular del circuito de la Figura 9, implementado para la generación de claves privadas y públicas;
La Figura 11 es un diagrama de bloques esquemático de un circuito electrónico implementado para la generación de claves compartidas (por ejemplo, Diffie - Hellman) basado en la generación de claves públicas y privadas;
La Figura 12 es un diagrama de bloques esquemático de una realización de un circuito integrado implementado para la generación de claves privadas y públicas, y provisto de un algoritmo de encriptado para proteger criptográficamente la clave privada de salida;
La Figura 13 es un diagrama de bloques esquemático de una realización de un circuito electrónico implementado con un protocolo de autenticación y un gestor/controlador de código de acceso a dispositivo asociado;
La Figura 14 es un diagrama de bloques esquemático de una realización de un circuito electrónico provisto de la funcionalidad para inhabilitar el acceso a datos secretos o datos de seguridad a menos que el código de acceso de dispositivo correcto se aplique al gestor/controlador de código de acceso a dispositivo;
La Figura 15 es un diagrama de bloques esquemático de una realización básica de un circuito electrónico configurado para la generación de una cadena de claves de enlace; y
La Figura 16 es un diagrama de bloques esquemático de otra realización de un circuito electrónico provisto de una implementación iterativa para la generación de una cadena de claves de enlace.

DESCRIPCIÓN DETALLADA DE REALIZACIONES DE LA INVENCIÓN

En todos los dibujos se utilizarán los mismos caracteres de referencia para elementos correspondientes o similares.

Visión General

La Figura 1 es un diagrama de bloques esquemático de un dispositivo general provisto de un circuito electrónico a prueba de manipulación indebida, de acuerdo con una realización básica preferida de la invención. El dispositivo general 100 incluye un circuito electrónico a prueba de manipulación indebida 10 y, típicamente, también una unidad general de entrada/salida 20 para transferir datos hacia/desde el dispositivo. Por supuesto, el dispositivo puede estar equipado con unidades adicionales, por ejemplo, para realizar diversos tipos de procesamiento de datos, todos dependiendo del dispositivo particular y de la función general del mismo.

El circuito electrónico a prueba de manipulación indebida 10 puede ser un circuito integrado (CI), una tarjeta inteligente o cualquier otro circuito electrónico a prueba de manipulación indebida y, preferiblemente, comprende una unidad de entrada/salida 11, una unidad de almacenamiento 12 para un secreto C, un motor o unidad para el procesamiento criptográfico 13 y una realización práctica de una operación relacionada con la seguridad 14. El secreto almacenado C no es accesible a través de una interfaz de circuito externo y, por lo tanto, no está disponible fuera del circuito electrónico 10. El motor criptográfico 13 está conectado a la unidad de almacenamiento 12 y configurado para realizar el procesamiento criptográfico al menos parcialmente en respuesta al secreto almacenado a fin de generar una instancia de datos de seguridad específicos de dispositivo que está internamente confinada dentro del circuito electrónico 10 durante el uso del dispositivo 100. Generalmente esto significa que los datos de seguridad específicos de dispositivo generados por el motor criptográfico 13 no están disponibles en la interfaz de programación externa del circuito electrónico durante el uso normal del dispositivo 100. La unidad de operación de seguridad 14 está enlazada a la salida del motor criptográfico 13 y configurada para realizar una o más operaciones relacionadas con la seguridad, en respuesta a los datos de seguridad específicos de dispositivo internamente confinados.

Es una gran ventaja ser capaz de generar datos de seguridad específicos de dispositivo y proporcionar una funcionalidad de seguridad total basada en cualquier información secreta C que se almacena originalmente en el

circuito electrónico 10. La seguridad es rigurosa puesto que el secreto almacenado nunca está disponible fuera del circuito electrónico 10, y los datos de seguridad específicos de dispositivo generados internamente sólo pueden usarse dentro del circuito para realizar una operación relacionada con la seguridad durante el funcionamiento normal del dispositivo.

El circuito electrónico a prueba de manipulación indebida, de acuerdo con la invención, es aplicable generalmente en una amplia variedad de dispositivos, produciendo datos de seguridad específicos de dispositivo internamente confinados que se pueden usar para diversos propósitos relacionados con la seguridad. Ejemplos de dispositivos adecuados para implementar un circuito electrónico de acuerdo con la invención incluyen teléfonos móviles, ordenadores personales, cámaras, dispositivos de audio, servidores de red, puertas de enlace de seguridad, cortafuegos, estaciones base y así sucesivamente.

Aplicación de dispositivo de red

Tal como se ilustra en la Figura 2, el circuito electrónico 10 puede estar dispuesto, por ejemplo, en un dispositivo de red y los datos de seguridad específicos de dispositivo generados internamente por el circuito en funcionamiento dentro del dispositivo de red 100 pueden usarse entonces para operaciones de seguridad de datos en comunicación de red. El dispositivo de red 100 mostrado en la Figura 2 incluye generalmente un circuito electrónico 10 a prueba de manipulación indebida, una interfaz de usuario 20-1 y una unidad de comunicación de red 20-2 para la comunicación con otros dispositivos de red o entidades en una o más redes. Ejemplos de operaciones de seguridad de datos en la comunicación en red incluyen la confidencialidad de los datos, la integridad de los datos, la autenticación, la autorización y el no repudio, como se define comúnmente, por ejemplo en las referencias [4-6]. En otro escenario de aplicación, el secreto almacenado C puede incluso usarse para generar una dirección de terminal, que es (única) para el dispositivo/terminal y puede utilizarse para una comunicación de red eficiente.

Aplicación de marcado de contenido

Tal como se ilustra en la Figura 3, el circuito electrónico 10 puede alternativamente estar dispuesto en un dispositivo 100 que produce contenido digital tal como audio digital, vídeo, imágenes, texto, etc. Ejemplos de tales dispositivos productores de contenido incluyen cámaras fotográficas digitales, cámaras de video, grabadoras de audio, escáneres digitales y cualquier equipo de digitalización que represente contenido en forma digital. Los datos de seguridad específicos de dispositivo generados internamente y mantenidos por el circuito en funcionamiento dentro del dispositivo productor de contenido pueden usarse entonces, por ejemplo, para marcar el contenido digital producido generando una huella digital específica del dispositivo integrada en el contenido digital. Esto significa que el contenido puede estar vinculado al dispositivo particular que realmente produjo el contenido, y la huella digital puede ser usada posteriormente como evidencia de producción. Esta función se hace cada vez más importante en particular en los juicios legales, ya que la posibilidad o falsificación de imágenes se ha extendido ampliamente a través del software de procesamiento de imágenes avanzado disponible a un bajo costo. Por ejemplo, puede generarse una instancia de datos de seguridad específicos de dispositivo, ya sea únicamente en respuesta al secreto almacenado C o en respuesta al secreto almacenado en combinación con datos de entrada adicionales tales como algunos datos de activación predeterminados y/o el propio contenido. Los datos de seguridad específicos de dispositivo generados internamente se utilizan entonces como entrada para la operación relacionada con la seguridad implementada en la unidad 14 para integrar una huella digital específica del dispositivo en el contenido digital basada en los datos de seguridad específicos de dispositivo generados. El contenido marcado es entonces emitido desde el circuito electrónico 10.

El marcado de contenido, como se sugiere por la invención, puede ser particularmente útil en una combinación de un dispositivo de red y un dispositivo productor de contenido, tal como un teléfono móvil con una cámara integrada, pero también es aplicable en cámaras independientes o imágenes similares, vídeo o dispositivos de audio.

Escenario de fabricación

En lo que sigue, la invención se describirá principalmente con un escenario ejemplar particular en mente, a saber, la fabricación de dispositivos (también a veces denominados entidades), incluyendo la gestión de secretos iniciales y/o datos de seguridad específicos de dispositivo y el uso posterior de dichos datos de seguridad dentro de los dispositivos. Sin embargo, debe entenderse que la invención no está limitada a la misma y que el escenario de fabricación sirve meramente como base para una mejor comprensión de los conceptos y principios básicos de la invención.

La Figura 4 es un diagrama de flujo esquemático de un método para fabricar un dispositivo con capacidades de datos de seguridad, incluyendo la gestión de datos de seguridad específicos de dispositivo, de acuerdo con una realización preferida de la invención.

En la etapa S1, en la fabricación del circuito, preferiblemente se almacena de forma segura un secreto más o menos aleatorio dentro del circuito electrónico a prueba de manipulación. Esto podría ser implementado de tal manera que ni siquiera el circuito o fabricante de chips conoce el secreto. Estos datos secretos pueden ser cualquier número arbitrario o generado aleatoriamente. En la etapa S2, que también se realiza en la fabricación de circuitos, el circuito electrónico está provisto de algoritmos criptográficos implementados para su ejecución en el circuito electrónico con

el secreto como entrada o parte de la entrada. Una vez que el circuito electrónico es instalado por el fabricante del dispositivo para su funcionamiento en un dispositivo, el secreto almacenado puede usarse junto con el algoritmo o algoritmos criptográficos para generar una instancia de datos de seguridad que es específica para el dispositivo particular en el que está el circuito electrónico implementado. El procesamiento algorítmico criptográfico se basa preferentemente en una función criptográfica diseñada para que sea computacionalmente imposible deducir el resultado del algoritmo sin conocer el secreto, y/o deducir el secreto del resultado. En la etapa S3, se implementa una operación relacionada con la seguridad en el circuito electrónico a prueba de manipulación. La operación está configurada para utilizar los datos de seguridad específicos de dispositivo como entrada y puede estar relacionada con, por ejemplo, encriptado/desencriptado, integridad de datos, autenticación, no repudio, autorización y marcado de contenido. El circuito electrónico está diseñado de tal manera que los datos de seguridad específicos de dispositivo generados por el algoritmo o algoritmos criptográficos durante el uso del dispositivo global están internamente confinados dentro del circuito electrónico. Esto puede lograrse utilizando un registro restringido dentro del circuito electrónico a prueba de manipulación indebida que sólo puede ser accedido por el algoritmo criptográfico para acceso de escritura y la operación relacionada con la seguridad para acceso de lectura durante el uso del dispositivo. Con tecnología de vanguardia, es hoy posible almacenar por ejemplo una clave de seguridad de 128 bits en un registro de hardware dedicado en un circuito integrado. Alternativamente, el confinamiento interno se asegura mediante técnicas de protección de la memoria. Por ejemplo, se puede definir un área protegida en una memoria interna dentro del circuito electrónico para el almacenamiento de datos de seguridad específicos de dispositivo. El acceso a esta área protegida sólo se permite a partir de una o más áreas de dirección de memoria especificadas, en las que el algoritmo criptográfico mencionado anteriormente y la operación relacionada con la seguridad se mantienen en forma ejecutable.

De este modo, el secreto almacenado y el algoritmo o algoritmos criptográficos implementados en el circuito electrónico permiten la generación de datos de seguridad específicos de dispositivo confinados de forma segura, por ejemplo, claves de encriptado y desencriptado, claves de enlace, claves simétricas, claves públicas privadas y asociadas y/u otros datos de seguridad específicos de dispositivo, que sólo se pueden utilizar para diversas operaciones de seguridad dentro del circuito electrónico.

En la etapa S4, en la fabricación del dispositivo, el fabricante del dispositivo instala el circuito en un dispositivo dado. En la etapa S5, el fabricante del dispositivo también puede ser responsable de la gestión general de los datos de seguridad específicos de dispositivo y de la información complementaria generada durante una fase opcional de configuración estrictamente controlada, como se explicará en detalle más adelante.

En particular, es claramente ventajoso ser capaz de generar datos de seguridad específicos de dispositivo y proporcionar una funcionalidad de seguridad completa basada en cualquier dato secreto, aleatorio que sea originalmente almacenado en el circuito electrónico por el fabricante del circuito. Además, el circuito electrónico permite la generación y gestión de datos de seguridad específicos de dispositivo para una amplia gama de dispositivos en los que se puede disponer el circuito. Además, puesto que los datos secretos se almacenan de forma segura en el circuito, no hay necesidad de una gestión de seguridad extensiva en la fabricación del dispositivo o en la distribución de circuitos entre el fabricante del circuito y el fabricante del dispositivo.

De hecho, se requiere una gestión de seguridad muy limitada entre el fabricante del circuito y el fabricante del dispositivo. El valor particular de C no es normalmente relevante mientras no se conozca a las partes no autorizadas, especialmente si nadie sabe o tiene acceso a C. Basta con que el secreto almacenado C sea suficientemente aleatorio sobre un conjunto suficientemente grande e imposible de enlazar al circuito en particular. Dado que no es necesario registrar o derivar información de C durante la fabricación del circuito, esto puede implementarse eficazmente dentro de un entorno controlado en el fabricante del circuito.

Si se desea o de otra forma apropiado, se puede obtener una gestión de seguridad adicional entre el fabricante del circuito y el fabricante del dispositivo implementando en el circuito un encriptado de clave pública (por ejemplo encriptado RSA) del secreto C basado en la clave pública del fabricante del dispositivo, La clave pública se almacena en el circuito, y la salida del secreto encriptado. La salida encriptada sólo puede ser desencriptada por el fabricante del dispositivo utilizando la clave privada correspondiente. De esta manera, C será conocido por el fabricante del dispositivo.

Como se describirá más adelante, la invención también está bien adaptada para la gestión de seguridad adicional de los datos de seguridad específicos de dispositivo, por ejemplo, certificación y delegación de confianza, con el fin de permitir que terceros de confianza se comuniquen de forma segura con el dispositivo de red y/o el usuario.

El tipo de gestión de seguridad que es apropiado depende de las amenazas o ataques específicos que el sistema se requiere para ser resistente y contra qué partes en el sistema que en cierta medida se confía. Por ejemplo, la gestión de datos de seguridad para dispositivos de red es una tarea muy importante, ya que la seguridad de toda la comunicación puede confiar en ella.

Por consiguiente, las partes autorizadas con datos de seguridad específicos de dispositivo pueden ser diferentes

para diferentes instancias del problema descrito. Se supone a lo largo de los siguientes ejemplos que se confía al fabricante del dispositivo los datos de seguridad específicos de dispositivo, aunque la invención no se limita realmente a esa suposición. Como se indicó anteriormente, el fabricante de chips no tiene que confiar en los datos de seguridad, aunque normalmente se asume algún tipo de relación de confianza, por ejemplo, que el fabricante de chips implementa lo que se acuerda y no introduce ningún secreto "puertas traseras" y así sucesivamente. También es común que el propietario o usuario del dispositivo se considere un grupo de confianza, ya que normalmente es de su interés asegurarse de que la transferencia de mensajes sea segura. Sin embargo, esto no es necesariamente cierto y no se asumirá; Un escenario de excepción particular es el de DRM.

Gestión de Derechos Digitales (DRM, por sus siglas en inglés), por ejemplo, es una tecnología para proteger los activos de un proveedor de contenido/propietario en un sistema de distribución de contenido digital. En la mayoría de los casos, la tecnología se implementa encriptando el contenido y asociando a este contenido una llamada licencia que incluye la clave de desencriptado (normalmente en formato encriptado) y los derechos de uso que describen lo que se permite hacer con el contenido.

En el equipo que se utilizará para renderizar el contenido, se implementará un módulo/agente de DRM para asegurar que la representación sigue lo que se prescribe por los derechos de uso. Este agente se implementa típicamente como un módulo de software y/o hardware, aplicando la política de uso como se indica en la licencia. El módulo/agente DRM constituye la parte de confianza dentro del equipo de usuario, desde el punto de vista del proveedor de contenido. Tenga en cuenta que el usuario no es una parte de confianza, ya que el usuario puede querer eludir la protección del contenido y utilizar el contenido sin las restricciones prescritas en la licencia.

El problema de asegurar el contenido es en parte para administrar la confidencialidad del contenido y la integridad de la licencia durante el transporte desde el distribuidor de contenido al dispositivo donde se utilizará el contenido. Una solución posible a este problema es que el proveedor/distribuidor de contenido entregue de forma segura al módulo/agente de DRM en el equipo de representación una "clave de encriptado clave", que puede utilizarse para derivar la clave de encriptado de contenido y comprobar la integridad de la licencia. Para proteger la clave de encriptado clave, los datos de seguridad del dispositivo, no disponibles para el usuario, podrían ser utilizados por el módulo/agente DRM. Además, el proveedor/distribuidor de contenido de confianza necesita alguna información relacionada con estos datos de seguridad para asegurar la transferencia a este dispositivo en particular. Por ejemplo, si los datos de seguridad son una clave de desencriptado, la clave de encriptado correspondiente es normalmente necesaria por el distribuidor/proveedor de contenido.

Datos de activación - configuración vs. uso

Con referencia una vez más a la Figura 1, el secreto almacenado C puede ser la única entrada al motor criptográfico. Alternativamente, sin embargo, se puede aplicar entrada adicional a través de la unidad de entrada/salida 11 del circuito electrónico 10 y usarse junto con el secreto almacenado C en el motor criptográfico 13 para generar los datos de seguridad específicos de dispositivo. En una realización preferida de la invención, se define durante la configuración del dispositivo 100, por ejemplo en una fase de configuración durante la fabricación o durante la configuración del usuario, datos de activación opcionales (indicados por la línea discontinua en la figura 1) necesarios para generar datos de seguridad adecuados En la aplicación particular.

Durante el uso posterior del dispositivo 100, se deben aplicar los mismos datos de activación al circuito electrónico 10 al motor criptográfico 13 para poder generar los datos de seguridad específicos de dispositivo.

Como se ilustra esquemáticamente en el diagrama de flujo básico de la Figura 5, los datos de activación se determinan durante la configuración del dispositivo, tal vez en una fase de configuración durante la fabricación del dispositivo o durante la configuración del usuario (S11), como se ejemplificará más adelante. Durante el uso posterior, se generan datos de seguridad específicos de dispositivo internamente confinados siempre que se apliquen los mismos datos de activación sobre una interfaz de circuito externo. En otras palabras, tanto el secreto almacenado C como los datos de activación predeterminados son necesarios para poder generar datos de seguridad apropiados (S12). Finalmente, se realiza una operación relacionada con la seguridad en respuesta a los datos de seguridad específicos de dispositivo (S13) generados internamente e internamente confinados. Si los datos de activación se definen durante la fabricación del dispositivo, es posible que los datos de activación tengan que transferirse de forma segura del fabricante del dispositivo al dispositivo, por ejemplo a través de un interlocutor intermedio como un operador de red al que está asociado el usuario del dispositivo.

Alternativamente, los datos de activación predeterminados se almacenan en el dispositivo para facilitar el acceso cuando se necesita invocar los datos de seguridad específicos de dispositivo para una operación relacionada con la seguridad. En algunas aplicaciones, los datos de entrada adicionales pueden incluso ser información públicamente conocida, ya que sólo el propietario del dispositivo que comprende el circuito particular es capaz de generar el resultado debido al secreto almacenado implicado. Esto significa que un adversario con acceso físico al dispositivo, puede obtener acceso a los datos de activación o código para realizar la operación relacionada con la seguridad. Sin embargo, el adversario nunca tendrá acceso a los datos de seguridad específicos de dispositivo en sí, que siempre está internamente confinado dentro del circuito durante el uso del dispositivo en general. En algunas aplicaciones,

puede ser ventajoso proteger el código de activación almacenado, por ejemplo, por medio de una contraseña seleccionada por el usuario.

Activaciones múltiples

También es posible definir múltiples señales individuales de datos de activación durante la configuración del dispositivo, en la que cada señal de datos de activación está asociada con unos datos de seguridad específicos de dispositivo individuales respectivos. El circuito electrónico de acuerdo con la invención se configura entonces para generar un dato de seguridad específico del dispositivo, siempre que la señal de datos de activación asociada se aplique al circuito. Esto puede utilizarse para proporcionar un módulo de identidad multiusuario, tal como un SIM multiusuario (Subscriber Identity Module) para propósitos de autenticación y acuerdo clave, o un decodificador multicanal, tal como un decodificador de televisión por satélite o cable, en el que varios Se requieren claves de seguridad únicas. Una determinada clave se activa simplemente aplicando los datos de activación correspondientes.

En general, los datos de activación pueden definirse de varias maneras. A modo de ejemplo, los datos de activación pueden definirse basándose en datos de seguridad de configuración específicos de dispositivo proporcionados durante la configuración del dispositivo, como se describirá a continuación principalmente con referencia a las Figuras 6 y 7. Los datos de activación también pueden ser una simiente simple inicialmente aplicada al circuito electrónico durante la configuración del dispositivo, forzando al circuito electrónico a emitir datos de seguridad específicos de dispositivo a través de una interfaz de circuito externo en respuesta a un llamado acceso de dispositivo, Como se describirá principalmente con referencia a la Figura 8. Alternativamente, para aplicaciones basadas en criptografía asimétrica, se puede usar como datos de activación una entrada adicional adecuada tal como un primo, un generador de un grupo matemático, un nonce y/o un código PIN, como se describirá más adelante con referencia a las Figuras 9-12.

Encriptación/desencriptación de datos de seguridad configuracionales

La Figura 6 es un diagrama de bloques esquemático de un circuito electrónico a prueba de manipulación indebida provisto de funcionalidad para encriptar datos de seguridad configuracionales en datos de activación de acuerdo con una realización preferida de la invención. Preferiblemente, el circuito electrónico 10 está configurado para generar datos de activación como una representación criptográfica de algunos datos de seguridad específicos de dispositivo configuracionales, basados en el secreto almacenado. La representación criptográfica se envía entonces a través de una interfaz de circuito externo durante la fase de configuración. Durante el uso del dispositivo, los datos de seguridad específicos de dispositivo se vuelven a generar internamente siempre que dicha entrada adicional corresponda a la representación criptográfica. Esto permite al fabricante del dispositivo u otra parte de confianza en el control de los dispositivos, como un operador de red, seleccionar libremente datos de seguridad específicos de dispositivo para dispositivos fabricados durante la configuración del dispositivo. Esto puede ser ventajoso en ciertas aplicaciones donde se requiere que los datos de seguridad tengan un formato particular. Por ejemplo, en criptografía asimétrica como RSA o curvas elípticas, las claves no son sólo cadenas aleatorias, sino que tienen que ser elegidas con precaución.

Además del secreto aleatorio C implementado por el fabricante del circuito en la unidad de almacenamiento 12, el circuito electrónico 10 incluye una realización práctica 15 de una función unidireccional de trampilla, en este caso representada como un algoritmo de encriptado E que usa el secreto C como encriptado llave. El circuito electrónico 10 también incluye una realización práctica 13 del correspondiente algoritmo inverso de trampilla, realizando en este caso el desencriptado D, así como una realización 14 de una operación relacionada con la seguridad.

Durante la configuración, el fabricante del dispositivo u otra parte de configuración genera cualquier dato K de seguridad específico del dispositivo, por ejemplo, una clave criptográfica, y la aplica al circuito 10 para el encriptado. Debe entenderse que la configuración no tiene necesariamente que realizarse durante la fabricación, sino que puede realizarse más tarde, por el fabricante del dispositivo en una fase de configuración separada o por una parte separada, tal como un operador de red, que controla la fabricación Dispositivos. La representación de resultados criptográficos E (C, K) = X es registrada por el fabricante del dispositivo u otra parte configuradora en un entorno controlado y opcionalmente almacenada en el dispositivo. El par así generado (X, K) puede ser utilizado, por ejemplo, más tarde por la parte configuradora o un tercero de confianza para comunicarse de forma segura con el dispositivo. Si es apropiado, considerando el modelo de confianza, la representación de resultados X y/o los datos de seguridad configuracionales K correspondientes pueden ser gestionados por un operador de red de confianza. La representación de resultados X puede ser transferida de forma segura desde el operador al dispositivo, tal como un teléfono móvil o un dispositivo de red similar asociado con el operador, en base a una clave de sesión obtenida de un procedimiento de autenticación y acuerdo clave.

Alternativamente, la representación criptográfica X se almacena en el dispositivo ya durante la configuración. A menos que K esté internamente confinado durante el uso del dispositivo, un adversario con acceso al dispositivo y los datos de activación almacenados X pueden obtener la llave de dispositivo K. Por lo tanto, la clave de dispositivo generada internamente K nunca se muestra fuera del circuito durante el uso de El dispositivo, pero sólo se utiliza dentro del circuito para cualquier operación de seguridad o las operaciones que se requieren. Esto significa que la representación criptográfica X puede ser almacenada, por ejemplo en una PROM en el dispositivo y al mismo tiempo

la clave de dispositivo sensible K resistirá ataques de un adversario con acceso al dispositivo ya la interfaz de programación del circuito electrónico. Opcionalmente, si el modelo de confianza así lo admite, X puede incluso ser protegido por el usuario, de modo que la autenticación por medio de una contraseña o PIN debe ser llevada a cabo para poder recuperar X para la entrada en el circuito electrónico, opcionalmente junto con una limitación Número de ensayos antes de que sea necesario un código especial de autenticación.

En resumen, el circuito ilustrado en la Figura 6 implica varias capas de operaciones en dos fases diferentes: Durante una fase de configuración, los datos configuracionales en forma de una clave de dispositivo K se cifran con el algoritmo E. Posteriormente, durante el uso del dispositivo, la representación de resultado encriptada se descifra con el algoritmo D, Y la instancia de clave de dispositivo resultante se utiliza entonces como entrada para la operación relacionada con la seguridad, tal como desencriptado de información encriptada en texto claro, autenticación de origen de datos, protección de integridad de mensaje o una combinación de tales operaciones de seguridad, como queda claro para cualquiera familiarizado Con el campo. Opcionalmente, la operación D podría incorporar una funcionalidad no relacionada con la seguridad criptográfica que sea sensible con respecto al modelo de confianza, por ejemplo, gestión de los datos que deberían estar disponibles sólo para las partes autorizadas y por lo tanto permanecer en el circuito. DRM da un ejemplo particular a esto donde se puede requerir que el contenido de texto claro de alta calidad (como texto, audio y video) permanezca confidencial, aunque se permite que una copia de resolución inferior alcance el dispositivo de representación. De este modo, la operación relacionada con la seguridad podría configurarse para reducir selectivamente la resolución o realizar selectivamente la conversión D/A y así sucesivamente, controlada en base a la información relativa a la clave de dispositivo K.

Naturalmente, el procedimiento anterior se puede extender a múltiples pares (K, X) y/o múltiples secretos C. De nuevo, el valor real de C no es generalmente relevante mientras no sea conocido por ninguna parte no autorizada.

También debe entenderse que es posible generar internamente los datos de configuración de seguridad en el circuito electrónico durante la fase de configuración, como se explicará más adelante con relación a la Figura 12.

La Figura 7 es un diagrama de bloques esquemático de una realización particular del circuito de la Figura 6 con otras mejoras de seguridad utilizando una clave de entrada adicional. Con el fin de mejorar aún más la seguridad del circuito electrónico a prueba de manipulación indebida de la Figura 6, se puede emplear una clave de entrada adicional como se ilustra en la Figura 7. Al igual que en la Figura 6, durante la configuración, por ejemplo, en la fabricación, el fabricante del dispositivo u otra parte de configuración utiliza el algoritmo E implementado en la unidad 15 y la clave C para encriptar los datos de seguridad K1. La salida codificada X1 obtenida puede ser almacenada en el dispositivo durante la configuración o transferida de otra manera segura al dispositivo y posteriormente introducida en el algoritmo de desencriptado asociado D1 implementado en la unidad 13. También se podrían generar datos de seguridad adicionales K2 e internamente confinados dentro del circuito electrónico 10 Una representación encriptada X2 de los datos de seguridad K2 se proporciona preferiblemente al dispositivo para su uso como entrada al circuito electrónico 10. K2 inicialmente puede ser generado por el fabricante del dispositivo u otra parte configuradora, por ejemplo, en conexión con el encriptado de K1. Alternativamente, K2 puede ser inicialmente generado por un tercero, por ejemplo, un proveedor de contenido o distribuidor, que desea distribuir de forma segura los datos digitales al dispositivo. En tal caso, el proveedor de contenidos representa K2 como X2 de tal manera que el acceso interno a K1 es necesario para reproducir internamente K2, por ejemplo, si K1 es una clave privada entonces X2 es el encriptado de clave pública correspondiente de la clave K2. La clave privada puede ser una clave privada del fabricante del dispositivo y no tiene que ser conocida por el usuario. La clave pública podría estar disponible, por ejemplo, de una Autoridad de Certificación de una infraestructura de clave pública. El proveedor de contenido entonces distribuye X2 al dispositivo. Un algoritmo de desencriptado asociado D2 se implementa en la unidad 14-1 en el circuito electrónico para desencriptar la entrada encriptada recibida X2 por medio del K1 generado internamente. Desencriptado de datos (u otra operación de seguridad) recibida del fabricante del dispositivo o de un tercero, por ejemplo, el proveedor de contenidos, basado en el algoritmo de seguridad D 'implementado en la unidad 14-2, está disponible entrando X1 y X2 y los datos recibidos, cip, en la interfaz de circuito relevante para obtener el texto cle claro.

Permitiendo selectivamente el acceso externo a datos de seguridad durante la configuración

La Figura 8 es un diagrama de bloques esquemático de un circuito electrónico a prueba de manipulación indebida provisto de funcionalidad de código de acceso del dispositivo para permitir el acceso externo a los datos de seguridad generados durante la configuración, de acuerdo con otra realización preferida de la invención. Como se ha mencionado anteriormente, los datos de activación pueden alternativamente ser una simiente simple, tal como un nonce, una identidad de enlace o datos similares, que se aplica inicialmente al circuito electrónico durante la configuración del dispositivo para generar datos de seguridad B específicos del dispositivo basados en el secreto almacenado C y los datos de activación de entrada R. Por ejemplo, R puede ser una cadena de bits aleatoria y/o alguna identidad de dispositivo única. El motor criptográfico 13 se implementa preferiblemente con una aproximación de una función criptográfica unidireccional f utilizando el secreto C y los datos de activación R como entrada. Por ejemplo, la función unidireccional criptográfica podría ser un MAC con clave (Código de autenticación de Mensaje), véase [7, 8], de los datos de entrada R usando C como clave.

Además de la unidad de almacenamiento básico 12 para mantener el secreto C, el motor criptográfico 13 y la operación relacionada con la seguridad 14, el circuito electrónico 10 resistente a las manipulaciones mostrado en la Figura 8 también comprende un controlador 16 y una disposición de conmutación 17 para forzar selectivamente al circuito electrónico para que emita los datos de seguridad B específicos del dispositivo a través de una interfaz de circuito externo durante la configuración. El controlador 16 opera preferiblemente en respuesta a un llamado código de acceso de dispositivo (DAC) y cierra el conmutador 17 para hacer que los datos de seguridad B específicos del dispositivo estén disponibles fuera del circuito cuando el DAC se aplica al circuito durante la fase de configuración. Por ejemplo, el DAC puede ser dado al fabricante del dispositivo u otra parte configuradora por el fabricante del circuito en un procedimiento de autorización, como se describirá en detalle más adelante. Si no se introduce el DAC correcto durante la configuración, el conmutador 17 permanece abierto y los datos de seguridad B específicos del dispositivo sólo están disponibles en las interfaces internas apropiadas y, por consiguiente, nunca abandonan el circuito electrónico 10. Después de la configuración, puede ser incluso deseable desactivar el controlador 16 para asegurar que un adversario con acceso físico al dispositivo no pueda atacar el circuito 10 probando diferentes códigos en un intento de obtener datos de seguridad específicos de dispositivo.

Por ejemplo, la configuración puede realizarse durante la fabricación, en la que el fabricante del dispositivo inserta el circuito electrónico tal como un CI recibido de un fabricante de circuitos integrados en un dispositivo particular. Mediante el uso de la función criptográfica implementada f, se pueden obtener datos de seguridad específicos de dispositivo: En un entorno controlado, el fabricante del dispositivo introduce algunos datos R como entrada al algoritmo implementado en el motor criptográfico en el circuito para generar el resultado f (C, R) = B, y también aplica un DAC predeterminado al controlador 16 para permitir la salida externa de los datos de seguridad B resultantes.

En el ejemplo de la Figura 8, el fabricante del dispositivo u otra parte configuradora generalmente no puede elegir datos de seguridad específicos de dispositivo, sino que tiene que aceptar lo que sale de la función unidireccional f, mientras que en los ejemplos de las Figuras 6 y 7, el participante de configuración es libre de seleccionar los datos de seguridad específicos de dispositivo.

El par (R, B) se puede usar más tarde, por ejemplo, después de que el dispositivo haya sido vendido a un usuario, por el fabricante del dispositivo u otra parte configuradora, o incluso a un tercero confiado por el configurador del dispositivo para comunicarse de forma segura con el dispositivo. Los datos de seguridad específicos de dispositivo B se pueden usar para asegurar la comunicación, por ejemplo, como una clave criptográfica en un algoritmo de encriptado simétrico o en un código de autenticación de mensajes. Durante el uso, los datos de activación R son requeridos por el dispositivo para recrear internamente B en el circuito electrónico 10. Por ejemplo, si R es igual a un RAND en un procedimiento de acuerdo de clave tal como GSM AKA (Acuerdo de Clave y Autenticación) o UMTS AKA, los datos de seguridad específicos de dispositivo resultantes serán una clave de sesión AKA.

Los datos de activación R pueden almacenarse en el dispositivo durante la fabricación y/o la configuración, o suministrados antes del establecimiento de la comunicación segura. Aunque se prefiere la alta confidencialidad, los datos de activación R no necesariamente deben mantenerse confidenciales ya que sólo con acceso al circuito electrónico correcto pueden producirse los datos de seguridad relevantes B, y durante el uso del dispositivo, los datos de seguridad B nunca salen el circuito. Sin embargo, R está preferiblemente protegido contra la integridad, por ejemplo, con B o mediante algún mecanismo fuera de banda, para proteger de, por ejemplo, disturbios en la comunicación, manipulación y/o ataques de denegación de servicio.

Un ejemplo de una aplicación particular podría ser una compañía que posee/gestiona una serie de nodos de red que se comunican a través de una red no segura. Por ejemplo, los nodos/dispositivos podrían ser estaciones base de radio en una red móvil, dispositivos de dosificación de consumo de electricidad, máquinas automáticas de venta de bebidas/alimentos, todas provistas de circuitos electrónicos con la estructura general de la Figura 8. Durante la configuración de los nodos por el personal de confianza de la empresa, el fabricante genera una serie de claves B específicas del nodo en respuesta a uno o más números de entrada R, utilizando uno o más DAC para extraer los datos de seguridad de la Circuitos Durante el uso, el número o números de entrada R se distribuyen (preferiblemente protegidos contra la integridad) a los nodos de la red (o almacenados en ellos durante la fabricación/configuración), y se introducen en los circuitos electrónicos correspondientes para generar la clave o claves específicas del nodo B. Una vez que la o las claves secretas B se comparten de forma segura entre los nodos implicados, se puede establecer una comunicación segura mediante cualquier protocolo criptográfico convencional utilizando B.

Se pueden generar múltiples pares (R, B) y/o múltiples secretos C, por ejemplo, para permitir la revocación de determinados datos de seguridad o para diferenciar entre partes de comunicaciones.

En otro ejemplo particular, el par (R, B) puede constituir un par identidad de enlace-clave de enlace. Un ejemplo de delegación de confianza, que implica la generación de pares identidad de enlace-clave de enlace, es un protocolo llamado el protocolo Generic Trust Delegation (GTD). Puede ser útil dar una visión general de los fundamentos del protocolo GTD. El mecanismo para establecer y delegar confianza en el protocolo GTD se basa en el supuesto de

que dos partes P1, normalmente un fabricante de dispositivos, y P2, normalmente un dispositivo asociado, comparten un secreto (simétrico). El protocolo aprovecha el hecho de que el fabricante de dispositivos P1 ha asignado normalmente una clave de dispositivo secreto al dispositivo P2, que está protegida adecuadamente en el dispositivo. Un tercero P3, que tiene una relación de confianza con P1, quiere comunicarse de forma segura con P2. Como componente principal, el protocolo GTD incluye un protocolo de petición-respuesta básico, en el que P3 solicita, desde P1, una clave de enlace para una comunicación segura con P2. La parte P1 genera una identidad de enlace, única para el par P2 y P3. Entonces, la parte P1 deriva una clave de enlace basada en la identidad de enlace y el secreto que P1 comparte con P2, preferiblemente usando una función criptográfica unidireccional. La clave de enlace, normalmente junto con la identidad de enlace, se envía de forma segura de P1 a P3 (la seguridad se basa en claves derivadas de la relación de confianza existente entre P1 y P3). Dado que P2 conoce el secreto compartido entre P1 y P2, la parte P2 también puede calcular la misma clave de enlace dada la anterior identidad de enlace. Este último generalmente no es confidencial y puede enviarse a P2 desde P1 o P3. Por consiguiente, P2 y P3 pueden comunicarse de forma segura usando la clave de enlace. Naturalmente, en lugar de la clave específica del dispositivo en sí, otra clave derivada de la misma podría utilizarse en ambos lados para calcular la clave de enlace. En este procedimiento, P1 "delega confianza" a P3 en forma de la clave de enlace entre P2 y P3.

El fabricante del dispositivo nunca tiene que revelar la clave específica del dispositivo (o más generalmente la clave de entidad) a ninguna otra parte, ya que no es necesario transferir la clave específica del dispositivo fuera del dispositivo y del fabricante del dispositivo (u otro dispositivo configurador). Además, el protocolo GTD no requiere un solo tercero confiado en todos los fabricantes de dispositivos.

El secreto desconocido nunca tiene que abandonar el dominio del fabricante, excepto en el área protegida dentro del circuito electrónico del dispositivo donde el fabricante (del circuito) almacenó el secreto durante la fabricación. Por lo tanto, el fabricante tiene más posibilidades y todos los incentivos para mantener el secreto confidencial, comparado con el estado de la técnica.

Generación del par clave privada y/o clave asimétrica

La Figura 9 es un diagrama de bloques esquemático de un circuito electrónico a prueba de manipulación indebida en respuesta a datos de activación para generar selectivamente un par de claves privadas/asimétricas de acuerdo con otra realización preferida de la invención. En la Figura 9, se puede aplicar al circuito una entrada adicional adecuada tal como un primo, un generador de un grupo matemático, un noce y/o un código PIN durante la configuración del dispositivo, ya sea durante una fase de configuración en la fabricación o durante la configuración del usuario, para Generar un par de claves asimétricas (A, PA) y para emitir la clave pública PA a través de una interfaz de circuito externo. Durante la utilización del dispositivo, la correspondiente clave privada A se vuelve a generar internamente siempre que al menos una parte de la misma entrada adicional se aplique como datos de activación a través de una interfaz de circuito externo. La clave privada A generada internamente puede utilizarse entonces para operaciones PKI (Infraestructura de Clave Pública), tales como encriptado/desencriptado y autenticación.

La Figura 10 es un diagrama de bloques esquemático de una realización particular del circuito de la Figura 9 para la generación de claves privadas y públicas. A continuación, consideramos el caso ejemplar de la criptografía basada en logaritmos discretos. A modo de ejemplo, es posible utilizar el problema de logaritmos discretos sobre el grupo multiplicativo de enteros modulo un P grande con el generador G. Un entero elegido al azar de 1, ..., P-2 puede usarse como una clave privada . Como se ilustra en la Figura 10, designaremos este número A, que puede ser idéntico al número secreto C desconocido o derivado del secreto del chip junto con la entrada opcional. Como antes, el número A está oculto dentro del circuito electrónico y no debe ser posible extraer, ni ninguna información (excepto insignificante) de A.

El motor criptográfico 13 se basa en una función general Z para generar la clave A basada al menos en el secreto C. Un primo grande P podría ser opcionalmente introducido en el motor 13, que entonces tiene que generar una A adecuada. Entrada, pero el circuito debería entonces preferiblemente comprobar si G es un generador del grupo. Un nonce generado, por ejemplo, por el fabricante del dispositivo también se puede opcionalmente introducir en el circuito para su uso en la generación de la clave A.

También debería ser posible generar y emitir una clave pública P_A correspondiente del circuito, esto podría, por ejemplo, ser G^A mod P y/u otra información tal como G o, por ejemplo, el motor criptográfico 13 también incluye entonces una función general Y para generar esta clave pública P_A, preferentemente basada en P, G y A. La clave pública debe ser distribuida en una De manera autenticada al interlocutor relevante para que pueda ser utilizado de forma segura, más de los cuales se describirá más adelante. El circuito electrónico 10 puede realizar una o más operaciones de clave pública D' tales como, por ejemplo, encriptado o funciones de firma digital basadas en la clave privada A. Ejemplos específicos son el encriptado ElGamal y la firma ElGamal.

El secreto C desconocido se genera y almacena fácilmente en el circuito 10 (por ejemplo, CI) durante la fabricación del circuito, y con la nueva funcionalidad mostrada en la Figura 10, es así posible generar un par de claves asimétrico que puede ser utilizado por el dispositivo en el que el CI está dispuesto para una comunicación segura.

Otro uso de este par de claves público-privado es la generación de claves compartidas, como se ilustra esquemáticamente en la Figura 11. Por ejemplo, para la generación de claves compartidas Diffie-Hellman, la clave pública del dispositivo PA = GA mod P se intercambia por la clave pública del interlocutor PB = GB mod P, donde B es la clave privada correspondiente. PB se alimenta a una unidad de generación de clave compartida 14-3 en el circuito 10 y se calcula el secreto compartido GAB mod, por ejemplo, un nonce aleatorio opcional se puede también utilizar en un algoritmo junto con el secreto compartido para garantizar frescura y para restringir la filtración de la información de las claves privadas. El resultado es una clave secreta compartida KAB, que no está disponible externamente. La clave establecida puede utilizarse entonces para una operación relacionada con la seguridad D 'tal como la conversión de la información codificada CIP en la salida de texto claro CLE, tal como se implementa en la unidad 14-2.

Más en general, si A es una clave privada con la correspondiente clave pública PA en un esquema criptográfico asimétrico, con A protegida dentro de un circuito electrónico a prueba de manipulación, la invención cubre también el caso de que una clave criptográfica simétrica K encriptada por la clave pública PA, Se descifra y se utiliza dentro del circuito, y no se expone fuera del circuito, en analogía con los ejemplos anteriores.

Dependiendo del uso, la clave privada puede utilizarse como clave de dispositivo. Opcionalmente, la clave pública correspondiente puede ser certificada por el fabricante del dispositivo, como se ejemplificará más adelante.

En una realización alternativa, el usuario genera una clave privada, no necesariamente derivada directamente del secreto del chip. Por ejemplo, el motor criptográfico 13 se puede implementar con un generador de números pseudoaleatorios, que utilizando el secreto de fichas como simiente podría ser iterado un número de veces, posiblemente con alguna entrada adicional para generar una clave privada. Como en ejemplos anteriores, la clave privada puede estar oculta dentro del circuito electrónico y la correspondiente clave pública disponible fuera.

Opcionalmente, un usuario adicional puede insertar un nonce adicional durante la generación de la clave. Alternativamente, o como complemento, un PIN (número de identificación personal) o una contraseña asignada a un número puede ser el nonce o parte del nonce para habilitar la autenticación del usuario en el sentido de que el PIN o la contraseña es necesaria para producir la clave privada dentro el circuito.

Otra opción que puede utilizarse conjuntamente con los métodos anteriores es encriptar la clave privada, generada como en uno de los casos anteriores, con el algoritmo de encriptado E y el secreto de chip C 'y emitir la clave privada encriptada X, como se ilustra en la Figura 12. En similitud con las realizaciones de las Figuras 9-11, el circuito electrónico 10 resistente a las manipulaciones ilustrado en la Figura 12 incluye una unidad de almacenamiento 12-1, un motor criptográfico 13 para generar un par de claves asimétricas y una operación relacionada con la seguridad 14. Además, sin embargo, el circuito 10 de la Figura 12 incluye también una unidad de encriptado 15 que implementa el algoritmo E, una unidad de almacenamiento adicional 12-2 para un secreto C adicional y una unidad de desencriptado 13-2 para desencriptar una clave privada encriptada. Esto es en realidad un híbrido de la realización de la Figura 9 o Figura 10 y la realización de la Figura 6, pero donde la llamada clave específica del dispositivo configuracional, aquí la clave privada A, se genera internamente en respuesta a datos de entrada opcionales y posteriormente se cifra en una representación de resultado X. Cuando la clave privada necesita ser utilizada dentro del circuito electrónico Durante el uso del dispositivo global, X se inserta en la unidad de desencriptado 13-2 a través de una interfaz especial y luego se descifra por D basado en C'. La clave privada A generada internamente puede utilizarse posteriormente en el algoritmo D'. Opcionalmente, X puede estar protegido por contraseña o requerir autenticación de otro usuario.

Aunque las realizaciones ilustradas en las Figuras 10-12 se basan en logaritmos discretos, debe entenderse que otros esquemas para generar un par de clave asimétrica son también factibles.

Autorización del uso de las capacidades del circuito

Como se mencionó anteriormente brevemente, podría ser en el interés del fabricante del circuito hacer cumplir que el fabricante del dispositivo u otra parte configuradora sólo pueda utilizar el circuito electrónico a prueba de manipulación cuando así lo autorice el fabricante del circuito. También o alternativamente, dependiendo del modelo de confianza, el fabricante del dispositivo puede desear autorizar qué (otras) partes (si hay) que deberían tener acceso a las capacidades del circuito electrónico. Esto puede lograrse "acondicionando" ciertas operaciones dentro del circuito electrónico, basándose en un proceso de autenticación. Tales operaciones podrían ser, por ejemplo, acceso al valor C para ciertos algoritmos, e incluso salida de ciertos valores, posiblemente incluyendo también C, del circuito. El proceso de autenticación podría ser una simple contraseña de mantenimiento/usuario, pero preferiblemente implica un mecanismo de autenticación segura como el protocolo Fiat-Shamir [9] u otro protocolo de conocimiento cero.

La Figura 13 es un diagrama de bloques esquemático de una realización de un circuito electrónico implementado con un protocolo de autenticación y un gestor/controlador de código de acceso de dispositivo (DAC) asociado. Por simplicidad, sólo las partes del circuito que son relevantes para la autenticación y el código de acceso al dispositivo se ilustran en la Figura 13. Ahora damos un ejemplo de un procedimiento de autenticación para proporcionar un

código de acceso de dispositivo. Preferiblemente, se implementa un protocolo de autenticación 18 tal como el protocolo Fiat-Shamir en el circuito electrónico 10. Esto permite que el circuito electrónico 10 autentique al fabricante del dispositivo u otra parte configuradora basado en una clave pública PK implementada en el circuito 10. El dispositivo Fabricante u otra parte de configuración utiliza una estación de programación 110 para transferir información firmada por una clave privada SK al circuito electrónico 10 para verificación en la unidad de protocolo de autenticación 18 basada en la clave pública PK correspondiente. Esto implica aparentemente que la clave pública PK tiene que ser introducida en el circuito electrónico 10 ya durante la fabricación del circuito. El fabricante del dispositivo u otra parte configuradora normalmente genera pares de claves asimétricas (SK, PK) y proporciona al fabricante del circuito una clave pública PK o una lista de dichas claves públicas. La clave pública es, por supuesto, la información pública y no requiere gestión de seguridad adicional. Además, el circuito electrónico 10 está también provisto de un gestor/controlador de DAC 16. Un desafío R se introduce en el gestor de DAC 16 desde la estación de programación 110. Por ejemplo, R puede ser un número aleatorio, contener información de la identidad del dispositivo o Ser un valor hash de dicha información. Si la autenticación precedente tuvo éxito, como se indica mediante una señal de la unidad de protocolo de autenticación 18, el gestor DAC 16 genera una respuesta S, por ejemplo, empleando una función MAC. La respuesta S es entonces transferida por el circuito electrónico 10 a la estación de programación 110. El par (R, S) constituye un código de acceso de dispositivo, DAC, que posteriormente puede ser utilizado por la parte autorizada para acceder a ciertas capacidades de circuito. Por ejemplo, el DAC puede ser utilizado por el fabricante del dispositivo u otra parte configuradora para hacer que los datos de seguridad específicos de dispositivo estén disponibles en una interfaz de circuito externo durante la configuración del dispositivo, como se ha ejemplificado anteriormente en la Figura 8.

Dado el modelo de confianza adecuado, el fabricante del dispositivo, por ejemplo, puede otorgar/autorizar el DAC a un tercero de confianza. El DAC también puede usarse para "re-programar" el dispositivo, por ejemplo reemplazando datos de seguridad comprometidos por nuevos.

Como se ilustra en la Figura 14, el circuito electrónico también se puede configurar para inhabilitar el acceso interno al secreto almacenado y/o a los datos de seguridad específicos de dispositivo, a menos que se introduzca un código de acceso de dispositivo predeterminado DAC en el circuito electrónico. Por ejemplo, esto puede conseguirse disponiendo un conmutador en la ruta de señal desde la unidad de almacenamiento 12 al motor criptográfico 13 y/o en la ruta de señal desde el motor criptográfico 13 a la operación relacionada con la seguridad 14. Los conmutadores son típicamente controlados Por un gestor/controlador de DAC 16, que funciona en respuesta a un código de acceso de dispositivo (R, S). Por ejemplo, el gestor DAC 16 podría correlacionar el valor R recibido con una respuesta esperada S 'calculando el MAC con clave:

$$\mathbf{S'=MAC(R, C),}$$

y luego comparar la respuesta recibida S con la respuesta esperada calculada S 'para verificar el código de acceso del dispositivo (R, S). De forma predeterminada, el conmutador o los interruptores están abiertos para deshabilitar el acceso a las capacidades del circuito. Una vez que se ha introducido y verificado el código de acceso de dispositivo correcto, el controlador/controlador DAC 16 cierra el conmutador o los interruptores para permitir el acceso a las capacidades del circuito.

De esta manera, se puede garantizar que sólo un tercero autorizado, como el fabricante del dispositivo y/o cualquier otra parte que confía en el código de acceso del dispositivo, pueda utilizar el secreto almacenado para generar datos de seguridad específicos de dispositivo y/o utilizarlos Los propios datos de seguridad.

Los mecanismos anteriores para proporcionar acceso condicional a las capacidades del circuito tras la autenticación son características generales de la invención y pueden aplicarse a cualquiera de los ejemplos dados en la presente solicitud.

Jerarquía de las claves de enlace

El protocolo GTD descrito anteriormente también puede aplicarse iterativamente, dando como resultado una cadena de claves de enlace compartidas. El protocolo GTD básico comienza con dos partes que comparten una clave secreta y termina con una de las partes iniciales que comparten otra clave secreta con un tercero. El procedimiento podría ser repetido iterativamente, involucrando a una cuarta parte que tendrá, después de la segunda aplicación del protocolo, una clave secreta compartida con una de las partes anteriores, y así sucesivamente para iteraciones de orden superior.

Se ha reconocido que también el protocolo iterado de GTD podría ser implementado enteramente dentro de un circuito electrónico que no tolera interferencias, como se ilustra en la Figura 15. El motor criptográfico 13 ahora incluye múltiples instancias de una función unidireccional criptográfica, f, para producir una cadena de k bind claves B1, ..., Bk en respuesta a las correspondientes identidades de enlace R1, ..., Rk de acuerdo con la siguiente fórmula:

$$\mathbf{B_i = F(b_{i-1}, R_i) \text{ para } i=1, \ldots, k,}$$

donde $B_0 = C$.

La primera clave B1 de enlace se deduce típicamente por el fabricante del dispositivo u otra parte configuradora durante la configuración del dispositivo, por ejemplo en una fase de configuración durante la fabricación, introduciendo el código correcto de acceso al dispositivo DAC en el controlador DAC 16. Una vez que el DAC correcto es Verificada por el controlador 16, el conmutador 17 se cierra para permitir la salida de la primera clave B1 de enlace fuera del circuito electrónico 10. Si no se introduce el DAC correcto, la clave de enlace no está disponible fuera del circuito.

Al suministrar una secuencia de identidades de enlace, el dispositivo puede posteriormente calcular las claves de enlace correspondientes y finalmente realizar una operación de seguridad, tal como el desencriptado de datos encriptados CIP en la salida de texto claro CLE por medio de un algoritmo de desencriptado D '. Las claves de enlace están internamente confinadas dentro del circuito 10 y no pueden ser transferidas a través de una interfaz de CI externa por un tercero que no conoce el código de acceso del dispositivo. Con esta implementación, un atacante, con acceso físico al dispositivo, podrá a lo sumo desencriptar un mensaje encriptado dado, pero no acceder a las claves de enlace reales.

De este modo, hemos establecido, sin ninguna gestión de seguridad entre el fabricante del circuito y el fabricante del dispositivo, todo un conjunto de claves específicas del dispositivo (Bi, i = 1, ..., k) que están disponibles sólo dentro del circuito electrónico.

En la realización de la Figura 15, las identidades de enlace R1, ..., Rk se insertan "en paralelo". Alternativamente, las claves de enlace pueden generarse mediante una implementación "iterativa", como se ilustra esquemáticamente en la Figura 16. En el ejemplo de la Figura 16, las identidades de enlace R1, ..., Rk, junto con un número k que indica el número de iteraciones requeridas, se insertan "en serie", por ejemplo, concatenado en una interfaz de entrada de CI. Un algoritmo incorporado dentro del circuito electrónico 10 entonces itera la función f tantas veces como se indica por el número k insertado, procesando sucesivamente las entradas relevantes (Bi = f (Bi-1, Ri) para i = 1, ..., K y donde B0 = C) a la salida Bk a la operación D 'o cualquier otra operación o algoritmo adecuado relacionado con la seguridad. Con esta modificación, cualquier clave de enlace intermedio puede generarse para uso protegido con D'. Como antes, se puede introducir un DAC para proporcionar acceso externo a la clave de enlace inicial.

Gestión de datos de seguridad para incluir a terceros de confianza
A continuación, nos centraremos un poco más en cómo manejar la administración de seguridad si un tercero de confianza desea comunicarse de forma segura con el dispositivo con o sin que un usuario esté involucrado/de confianza.

El usuario involucrado/de confianza es un escenario común y no necesita más explicaciones. Sin embargo, en el ajuste de DRM, el usuario no es de confianza, tal como describimos anteriormente. En otros ajustes, puede no haber un usuario durante el funcionamiento normal, por ejemplo, si el dispositivo se ejecuta independiente. En todos los casos que involucren a un tercero, el tercero debe tener acceso a alguna información para poder asegurar una comunicación segura con el dispositivo deseado. Esta información puede ser, por ejemplo, ser una clave simétrica para un dispositivo garantizado por una entidad de confianza y autorizada o por un dispositivo firmado por el fabricante, certificado de clave pública utilizado para autenticar una entidad de comunicación. Describimos dos ejemplos más detalladamente a continuación.

Delegación de clave simétrica a terceros
Consideremos el ejemplo de la Figura 8. Como ejemplo particular, (R, B) podría ser un par de "unión de enlace", denominado simplemente "par de enlace", como en el protocolo GTD básico. De este modo, se generan uno o varios pares de enlace durante la configuración, por ejemplo, en la fabricación del dispositivo, y almacenados por la parte configuradora, como el fabricante del dispositivo. Por una disposición fuera de banda, un tercero de confianza es de manera segura delegado uno o varios pares de enlace de este dispositivo en particular y puede comunicarse de forma segura con el dispositivo, haciendo referencia/suministrando las identidades de enlace.

El protocolo GTD iterado podría lograrse de manera análoga para permitir que un grupo de confianza delegue más confianza en las partes que pueden comunicarse de forma segura con el dispositivo.

Alternativamente, se puede usar una clave simétrica K elegida como se describe en conexión con la Figura 6, y el par (X, K) puede usarse de la misma manera que (R, B) anterior para permitir que terceros de confianza configuren un canal seguro a un dispositivo.

Infraestructura de Clave Pública
Consideremos una vez más la estructura ejemplificada en la Figura 6. Ahora, supongamos que K es una clave criptográfica asimétrica, por ejemplo, una clave privada. Las siguientes operaciones podrían llevarse a cabo en una ubicación segura particular, por ejemplo, en el fabricante del dispositivo durante la fabricación:

Se puede generar una clave de desencriptado de dispositivo privado K junto con un certificado de clave de encriptado público firmado por la clave de firma privada del dispositivo. Esta última clave también tiene un certificado de clave pública correspondiente firmado por una parte de confianza, tal como una Autoridad de Certificación (CA) de una Infraestructura de Clave Pública (PKI), y disponible para una parte relevante a la que acceder, véase [8]. La clave K se introduce en el circuito electrónico para producir la correspondiente X, que puede almacenarse en el dispositivo. Posteriormente, la clave privada K puede ser completamente borrada en el dominio del fabricante del dispositivo para evitar cualquier uso no autorizado. El certificado de claves de encriptado público se puede colocar en un repositorio de certificados disponible públicamente. Cualquier persona con acceso a la clave pública puede realizar posteriormente el encriptado de datos pertenecientes a este dispositivo. La clave privada de desencriptado sólo existe durante un breve instante en el circuito electrónico.

La situación es completamente análoga para las firmas digitales, reemplazando "desencriptado" por "firma" y "encriptado" por "verificación" en el párrafo anterior, como es conocido por cualquier persona familiarizada con el tema.

Un procedimiento similar se aplica a las realizaciones descritas con relación a las Figuras 9-12. Allí, ya está disponible una clave privada o generada dentro del circuito electrónico y la clave pública correspondiente se revela fuera del circuito. Por lo tanto, el fabricante del dispositivo o el usuario puede certificar/solicitar la certificación de esta clave pública y, a continuación, un tercero puede utilizar el certificado para habilitar las operaciones de seguridad deseadas.

Las realizaciones descritas anteriormente son dadas meramente como ejemplos, y debe entenderse que la presente invención está limitada únicamente por las reivindicaciones adjuntas.

REFERENCIAS BIBLIOGRÁFICAS

[1] European Patent Application 0 753 816 A1, publicada el 15 de enero de 1997.
[2] U.S. Patent Nº 6,141,756 emitida el 31 de octubre de 2000.
[3] Digital Signature Cards Range - Secure smart cards for doing electronic business, GEMPLUS, impreso el 27 de octubre de 2003 de http://www.gemplus.com/products/dig_sign_cards_range.
[4] How PKI can reduce the risks associated with e-business transactions, by Cannady and Stockton, IBM, 1º de febrero de 2001.
[5] The mechanisms of data security, impreso el 2 de septiembre de 2003 de http://www.cardsnowindia.com/news/security1.htm.
[6] Security in an open world, Skillteam, impreso el 2 de septiembre de 2003 de http://www.common.lu.
[7] HMAC, Keyed-Hashing for Message Authentication, RFC 2104 by IETF.
[8] Handbook of Applied Cryptography, Menezes, van Oorschot, and Vanstone, Capítulos 1, 9 y 12, CRC Press.
[9] U.S. Patent Nº 4,748,668 emitida el 31 de mayo de 1988.

REIVINDICACIONES

1. Circuito electrónico a prueba de manipulación indebida para su implementación en un dispositivo, incluyendo el circuito un secreto almacenado no accesible a través de una interfaz de circuito externo y medios para recibir sobre una interfaz de circuito datos de activación, en respuesta a los cuales el circuito realiza un procesamiento criptográfico, **caracterizado por que** dicho circuito electrónico a prueba de manipulación indebida comprende:

- medios (15) para recibir datos de seguridad específicos de dispositivo de configuración para generar, basándose en dicho secreto almacenado (12), dichos datos de activación como una representación criptográfica de dichos datos de seguridad específicos de dispositivo de configuración durante la configuración de dicho dispositivo;
- medios para emitir dicha representación criptográfica sobre una interfaz de circuito externo durante la configuración;
- medios (13) para volver a generar internamente dichos datos de seguridad específicos de dispositivo durante el uso del dispositivo realizando procesamiento criptográfico al menos parcialmente en respuesta a dicho secreto almacenado (12) siempre que los datos de activación aplicados sobre dicha interfaz correspondan a dicha representación criptográfica, estando dichos datos de seguridad específicos de dispositivo re-generados internamente confinados dentro de dicho circuito electrónico durante el uso de dicho dispositivo; y
- medios (14) para realizar una operación relacionada con la seguridad en respuesta a dichos datos de seguridad específicos de dispositivo internamente confinados.

2. El circuito electrónico de acuerdo con la reivindicación 1, en el que dicho dispositivo es un dispositivo de red y dicha operación está relacionada con al menos uno de: confidencialidad de datos, integridad de datos, autenticación, autorización y no repudio en la comunicación en red.

3. El circuito electrónico de acuerdo con la reivindicación 1, en el que dicho dispositivo está configurado para producir contenido digital y dicha operación relacionada con la seguridad está configurada para marcar dicho contenido digital basado en dichos datos de seguridad específicos de dispositivo.

4. El circuito electrónico de acuerdo con la reivindicación 3, en el que dicha operación está configurada para generar una huella digital específica del dispositivo integrada en dicho contenido digital.

5. El circuito electrónico de acuerdo con la reivindicación 1, en el que dicha etapa de re-generación sólo se realiza si dichos datos de activación se aplican continuamente sobre dicha interfaz.

6. El circuito electrónico de acuerdo con la reivindicación 1, en el que dichos medios para generar internamente dichos datos de seguridad específicos de dispositivo comprenden medios para generar una clave privada al menos en parte basada en dicho secreto almacenado, y dichos datos de activación son generados como una representación criptográfica de dicha clave privada durante la configuración de dicho dispositivo.

7. El circuito electrónico de acuerdo con la reivindicación 1, que comprende además medios (16) para hacer, durante la configuración de dicho dispositivo, dichos datos de seguridad específicos de dispositivo disponibles sobre una interfaz de circuito externo, siempre que se introduzca un código de acceso de dispositivo predeterminado en el circuito electrónico.

8. El circuito electrónico de acuerdo con la reivindicación 1, que comprende además medios para inhabilitar el acceso interno a por lo menos uno de dichos secretos almacenados y a dichos datos de seguridad específicos de dispositivo, a menos que se introduzca un código de acceso de dispositivo predeterminado en el circuito electrónico.

9. El circuito electrónico de acuerdo con la reivindicación 7 u 8, que comprende además:

- medios (18) para la autenticación de un fabricante de dicho dispositivo;
- medios (16) para proporcionar, durante la fabricación del dispositivo, dicho código de acceso del dispositivo a dicho fabricante del dispositivo en respuesta a una autenticación satisfactoria.

10. El circuito electrónico de acuerdo con la reivindicación 1, en el que dichos medios para realizar una operación relacionada con la seguridad, basada en dichos datos de seguridad específicos de dispositivo, comprenden:

- medios (13) para realizar un procesamiento criptográfico adicional basado en dichos datos de seguridad específicos de dispositivo y otros datos de entrada externos para generar datos de seguridad adicionales; y
- medios (14) para realizar dicha operación relacionada con la seguridad en respuesta a dichos datos de seguridad adicionales.

11. El circuito electrónico de acuerdo con la reivindicación 10, en el que dichos datos de seguridad específicos de

dispositivo representan una clave privada y dichos datos de entrada externos adicionales representan un encriptado de dichos datos de seguridad específicos de dispositivo adicionales mediante la clave pública correspondiente.

12. Circuito electrónico según la reivindicación 11, en el que dichos datos de seguridad adicionales representan una clave de desencriptado de contenido simétrico emitida por un proveedor de contenido, y dichos datos de seguridad específicos de dispositivo representan una clave privada de un fabricante de dispositivos.

13. Circuito electrónico según la reivindicación 1, en el que dichos medios para volver a generar datos de seguridad específicos de dispositivo están configurados para generar una clave criptográfica simétrica en respuesta a una simiente aplicada sobre una interfaz de circuito externo.

14. El circuito electrónico de acuerdo con la reivindicación 1, en el que dichos medios para volver a generar datos de seguridad específicos de dispositivo están configurados para generar una clave privada al menos parcialmente basada en dicho secreto almacenado, y dichos medios para realizar una operación relacionada con la seguridad comprenden medios para realizar operaciones de criptografía asimétrica basadas en dicha clave privada internamente confinada.

15. El circuito electrónico de acuerdo con la reivindicación 14, que comprende además medios para generar una clave pública correspondiente a dicha clave privada durante la configuración de dicho dispositivo, y medios para emitir dicha clave pública sobre una interfaz de circuito externo.

16. El circuito electrónico de acuerdo con la reivindicación 14, que comprende además:

- medios (14-3) para realizar la generación de claves compartidas para generar una nueva clave compartida basada en dicha clave privada generada y una clave pública de un interlocutor de comunicación previsto; y
- medios (14-2) para realizar el procesamiento criptográfico basado en dicha nueva clave compartida.

17. El circuito electrónico de acuerdo con la reivindicación 1, en el que dichos medios para volver a generar son operables para generar dichos datos de seguridad específicos de dispositivo como una cadena de k claves de enlace B_1, …, B_k en respuesta a las correspondientes identidades de enlace R_1, ..., R_k de acuerdo con la siguiente fórmula:

$$\mathbf{B_i = f(B_{i-1}, R_i) \text{ para } i=1, \ldots, k,}$$

Donde B_0 representa el secreto almacenado, y f es una función criptográfica unidireccional.

18. Un dispositivo (100) implementado con un circuito electrónico (10) a prueba de manipulación que tiene medios (12) para almacenar de manera no manipulable un secreto no accesible a través de una interfaz de circuito externo, y medios para recibir sobre una interfaz de circuito datos de activación en respuesta al cual el circuito realiza el procesamiento criptográfico, **caracterizado por que** el dispositivo (100) comprende:

- medios (15) para recibir datos de seguridad específicos de dispositivo de configuración para generar, basándose en dicho secreto almacenado (12), dichos datos de activación como una representación criptográfica de dichos datos de seguridad específicos de dispositivo de configuración durante la configuración de dicho dispositivo;
- medios para emitir dicha representación criptográfica sobre una interfaz de circuito externo durante la configuración;
- medios (13) para volver a generar internamente dichos datos de seguridad específicos de dispositivo durante el uso del dispositivo realizando un procesamiento criptográfico al menos parcialmente en respuesta a dicho secreto almacenado (12) siempre que dichos datos de activación aplicados sobre dicha interfaz correspondan a dicho enlace criptográfico, Estando dichos datos de seguridad específicos de dispositivo re-generados internamente confinados dentro de dicho circuito electrónico durante el uso de dicho dispositivo; y
- medios (14) para realizar una operación relacionada con la seguridad en respuesta a dichos datos de seguridad específicos de dispositivo internamente confinados.

19. El dispositivo de acuerdo con la reivindicación 18, en el que dicho dispositivo es un dispositivo de red y dicha operación está relacionada con al menos uno de: confidencialidad de datos, integridad de datos, autenticación, autorización y no repudio en comunicación en red.

20. El dispositivo de acuerdo con la reivindicación 18, en el que dicho dispositivo está configurado para producir contenido digital y dicha operación relacionada con la seguridad está configurada para marcar dicho contenido digital basado en dichos datos de seguridad específicos de dispositivo.

21. Un método para gestionar datos de seguridad para un dispositivo (100) en el que está instalado un circuito electrónico (10) a prueba de manipulación que tiene medios (12) para almacenar un secreto no accesible a través de

una interfaz de circuito externo, medios para recibir más de un datos de activación de interfaz de circuito y medios (13) para realizar operaciones criptográficas, **caracterizado por que** comprende las etapas de:

- almacenar, en un entorno controlado durante la fabricación del circuito electrónico a prueba de manipulación, un número aleatorio y secreto en dicho circuito electrónico de tal manera que el número secreto no esté disponible fuera de dicho circuito electrónico;
- realizar, durante la fabricación de circuitos, un procesamiento criptográfico basado al menos parcialmente en dicho número secreto almacenado para generar datos de activación como una representación criptográfica de datos de seguridad específicos de dispositivo recibidos;
- emitir dicha representación criptográfica sobre una interfaz de circuito externo durante la fabricación del circuito (10) a prueba de manipulación indebida;
- regenerar internamente en el circuito electrónico (10) a prueba de manipulaciones dichos datos específicos del dispositivo durante el uso del dispositivo realizando un procesamiento criptográfico al menos en respuesta a dicho secreto (12), siempre que los datos de activación aplicados sobre dicha interfaz correspondan a dicha representación criptográfica, estando dichos datos de seguridad específicos de dispositivo re-generados internamente confinados dentro de dicho circuito electrónico a prueba de manipulación indebida (10); e
- implementar, durante la fabricación del circuito del circuito electrónico a prueba de manipulación indebida (10), una operación relacionada con la seguridad en dicho circuito electrónico, estando configurada dicha operación relacionada con la seguridad para recibir al menos dichos datos de seguridad específicos de dispositivo internamente confinados como entrada durante el uso del dispositivo.

22. El método de acuerdo con la reivindicación 21, en el que dicho dispositivo (100) es un dispositivo de red y dicha operación está relacionada con al menos uno de: confidencialidad de datos, integridad de datos, autenticación, autorización y no repudio en comunicación en red.

23. Procedimiento según la reivindicación 21, en el que dicho dispositivo (100) está configurado para producir contenido digital y dicha operación relacionada con la seguridad (14) está configurada para marcar dicho contenido digital basado en dichos datos de seguridad específicos de dispositivo.

24. El método de acuerdo con la reivindicación 21, que comprende además las etapas de:

- ingresar, en un entorno controlado durante la configuración del dispositivo, dichos datos de activación como datos de entrada en dicho circuito electrónico con el fin de obtener datos de seguridad específicos de dispositivo de la funcionalidad criptográfica del circuito electrónico;
- ingresar, en un entorno controlado durante la configuración del dispositivo, un código de acceso de dispositivo predeterminado al circuito electrónico (10) para acceder a los datos de seguridad específicos de dispositivo a través de una interfaz de circuito externo (17); y
- registrar, en un entorno controlado durante la configuración del dispositivo, dichos datos de seguridad específicos de dispositivo y dichos datos de entrada.

25. El método según la reivindicación 21, que comprende además las etapas de:

- generar, en un entorno controlado durante la configuración del dispositivo, datos de seguridad específicos de dispositivo;
- ingresar, en un entorno controlado durante la configuración del dispositivo, dichos datos de seguridad específicos de dispositivo generados en dicho circuito electrónico con el fin de obtener dichos datos de activación como una representación de resultado de la funcionalidad criptográfica del circuito electrónico; y
- registrar, en un entorno controlado durante la configuración del dispositivo, dicha representación de resultados y los datos de seguridad específicos de dispositivo previamente generados.

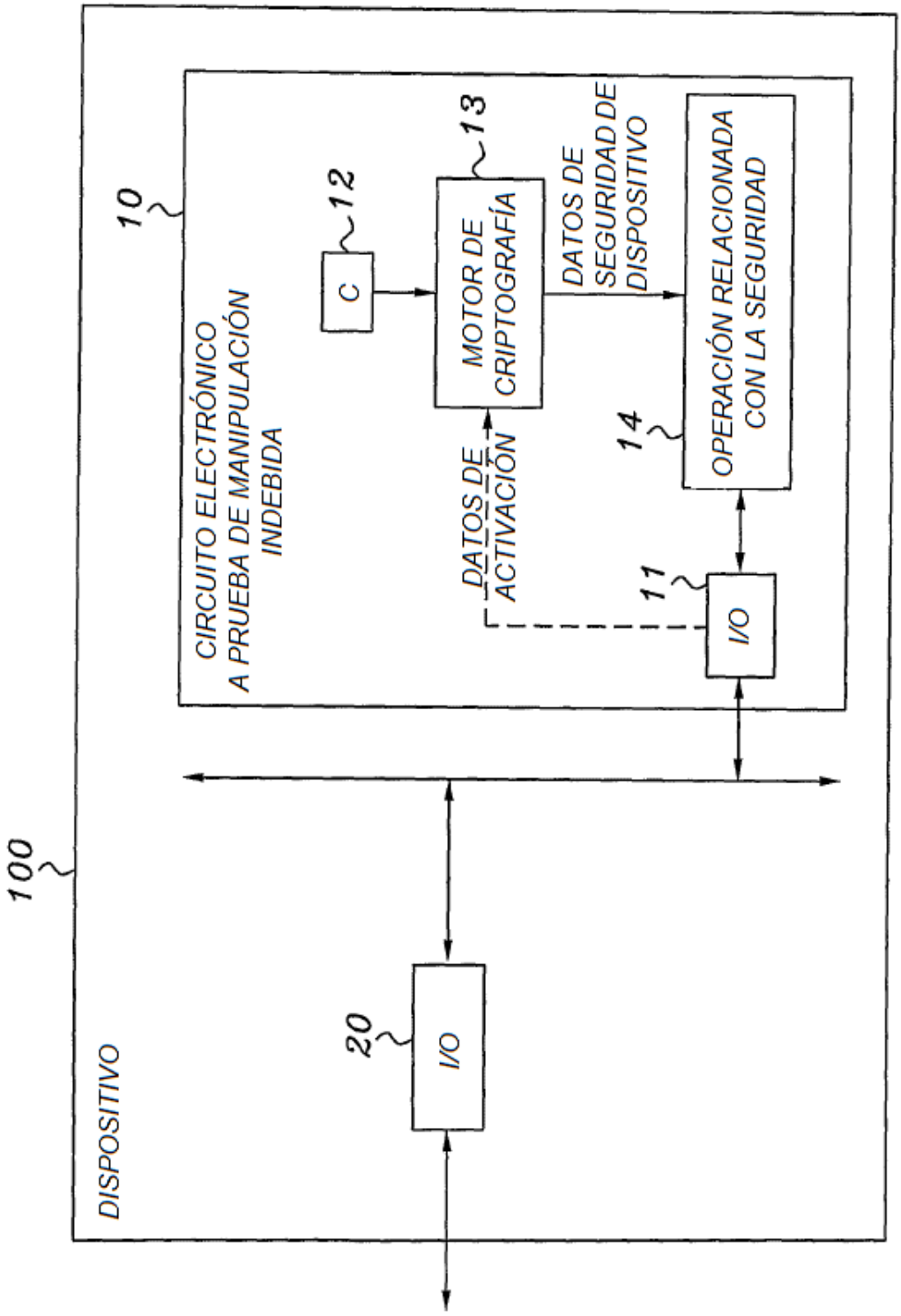
100
DISPOSITIVO
20
I/O
10
CIRCUITO ELECTRÓNICO A PRUEBA DE MANIPULACIÓN INDEBIDA
C
12
MOTOR DE CRIPTOGRAFÍA
13
DATOS DE SEGURIDAD DE DISPOSITIVO
OPERACIÓN RELACIONADA CON LA SEGURIDAD
14
DATOS DE ACTIVACIÓN
11
I/O

Fig. 1

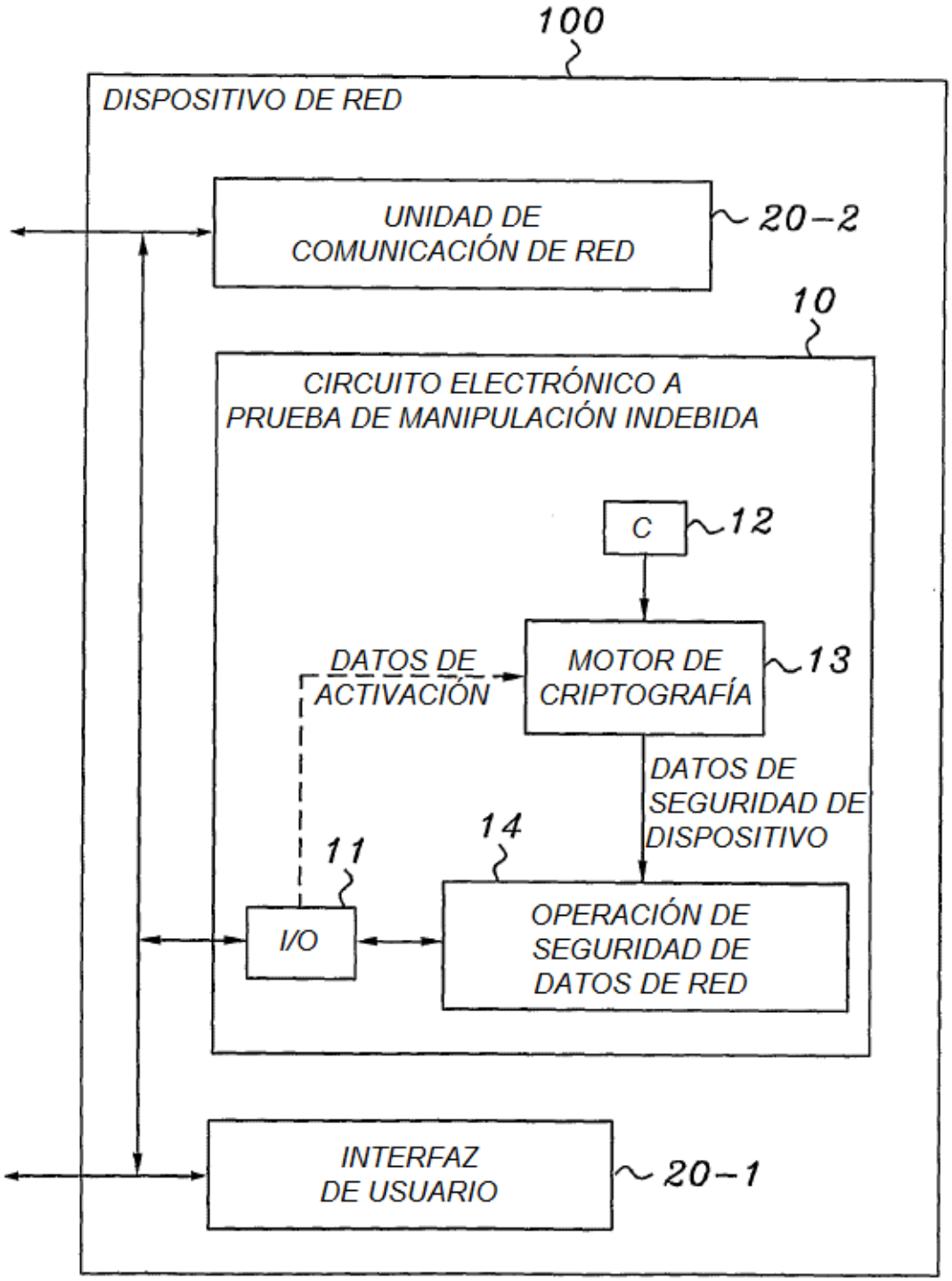
100
DISPOSITIVO DE RED
UNIDAD DE COMUNICACIÓN DE RED
20-2
10
CIRCUITO ELECTRÓNICO A PRUEBA DE MANIPULACIÓN INDEBIDA
C
12
DATOS DE ACTIVACIÓN
MOTOR DE CRIPTOGRAFÍA
13
DATOS DE SEGURIDAD DE DISPOSITIVO
11
14
I/O
OPERACIÓN DE SEGURIDAD DE DATOS DE RED
INTERFAZ DE USUARIO
20-1

Fig. 2

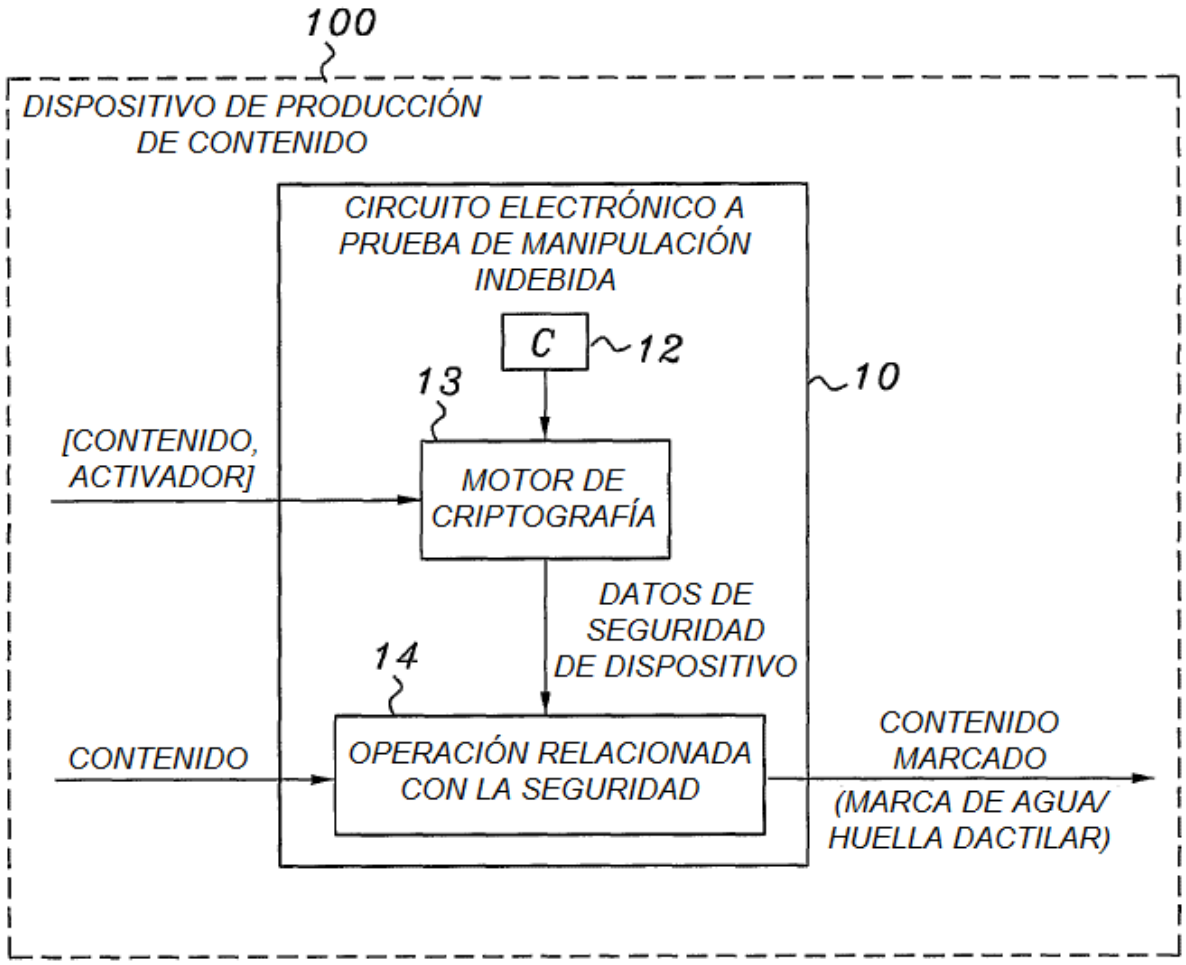
100
DISPOSITIVO DE PRODUCCIÓN DE CONTENIDO
CIRCUITO ELECTRÓNICO A PRUEBA DE MANIPULACIÓN INDEBIDA
C
12
10
13
[CONTENIDO, ACTIVADOR]
MOTOR DE CRIPTOGRAFÍA
DATOS DE SEGURIDAD DE DISPOSITIVO
14
CONTENIDO
OPERACIÓN RELACIONADA CON LA SEGURIDAD
CONTENIDO MARCADO
(MARCA DE AGUA/ HUELLA DACTILAR)

Fig. 3

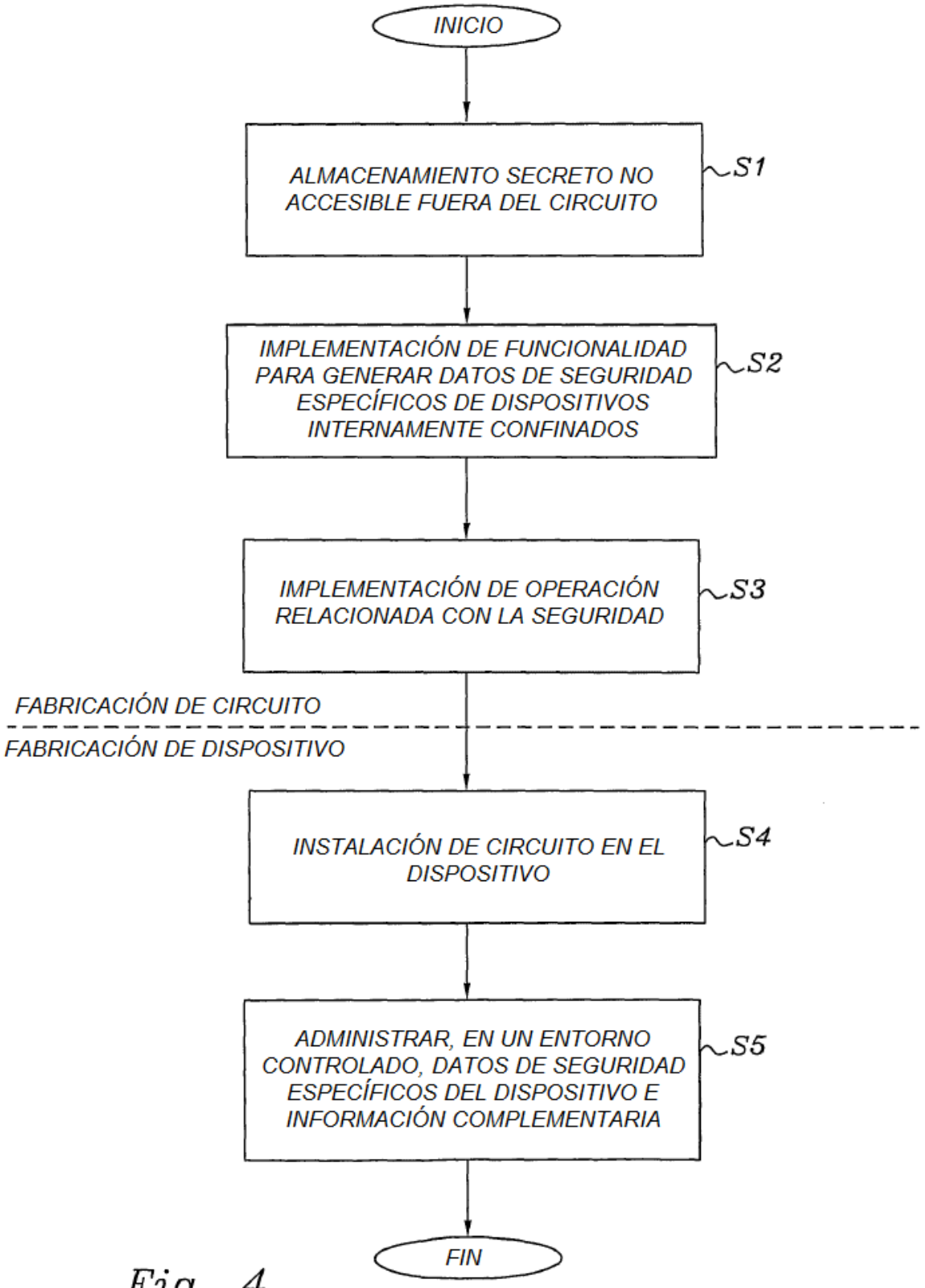
INICIO
ALMACENAMIENTO SECRETO NO ACCESIBLE FUERA DEL CIRCUITO
S1
IMPLEMENTACIÓN DE FUNCIONALIDAD PARA GENERAR DATOS DE SEGURIDAD ESPECÍFICOS DE DISPOSITIVOS INTERNAMENTE CONFINADOS
S2
IMPLEMENTACIÓN DE OPERACIÓN RELACIONADA CON LA SEGURIDAD
S3
FABRICACIÓN DE CIRCUITO
FABRICACIÓN DE DISPOSITIVO
INSTALACIÓN DE CIRCUITO EN EL DISPOSITIVO
S4
ADMINISTRAR, EN UN ENTORNO CONTROLADO, DATOS DE SEGURIDAD ESPECÍFICOS DEL DISPOSITIVO E INFORMACIÓN COMPLEMENTARIA
S5
FIN

Fig. 4

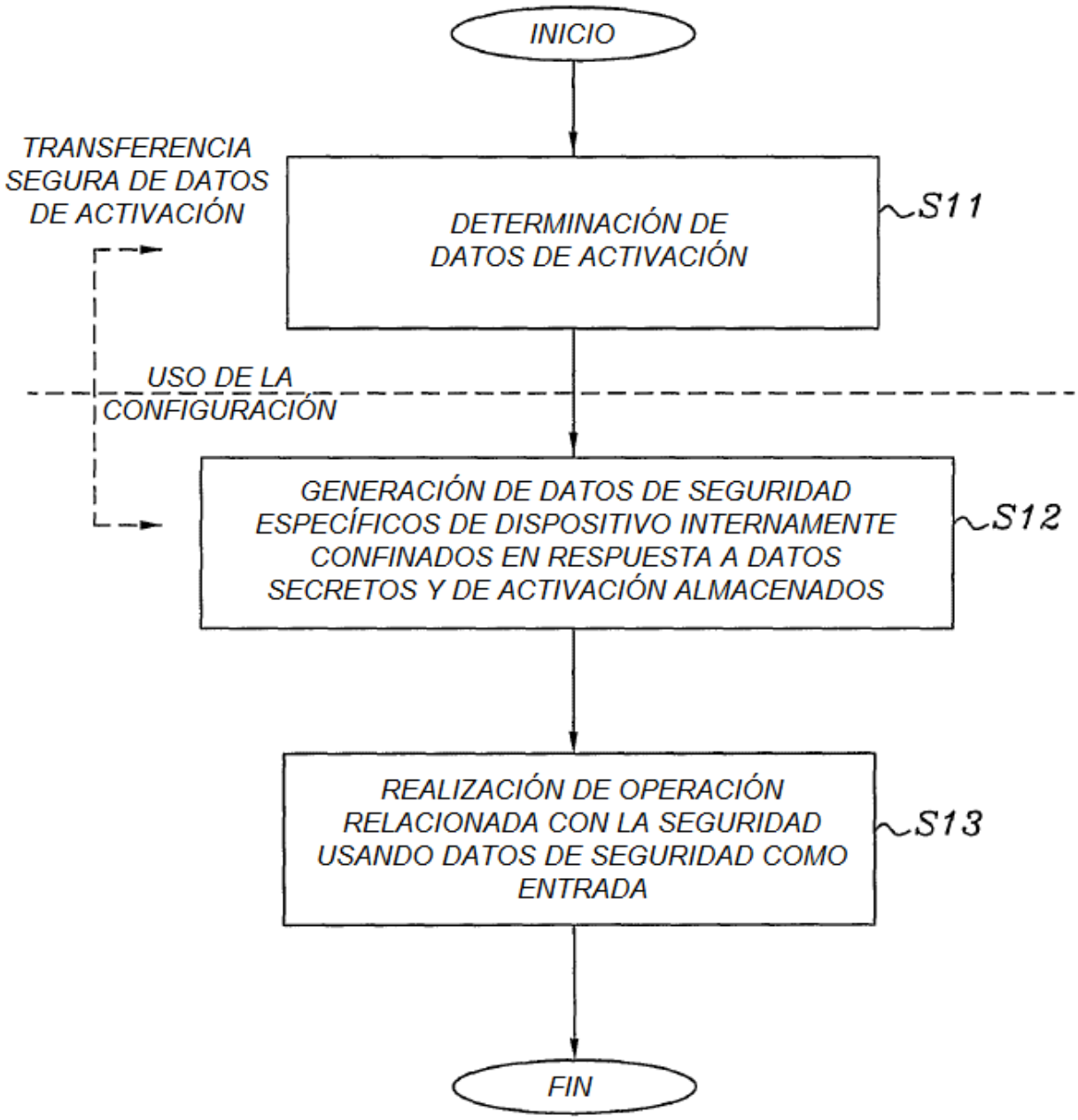
INICIO
TRANSFERENCIA SEGURA DE DATOS DE ACTIVACIÓN
DETERMINACIÓN DE DATOS DE ACTIVACIÓN
S11
USO DE LA CONFIGURACIÓN
GENERACIÓN DE DATOS DE SEGURIDAD ESPECÍFICOS DE DISPOSITIVO INTERNAMENTE CONFINADOS EN RESPUESTA A DATOS SECRETOS Y DE ACTIVACIÓN ALMACENADOS
S12
REALIZACIÓN DE OPERACIÓN RELACIONADA CON LA SEGURIDAD USANDO DATOS DE SEGURIDAD COMO ENTRADA
S13
FIN

Fig. 5

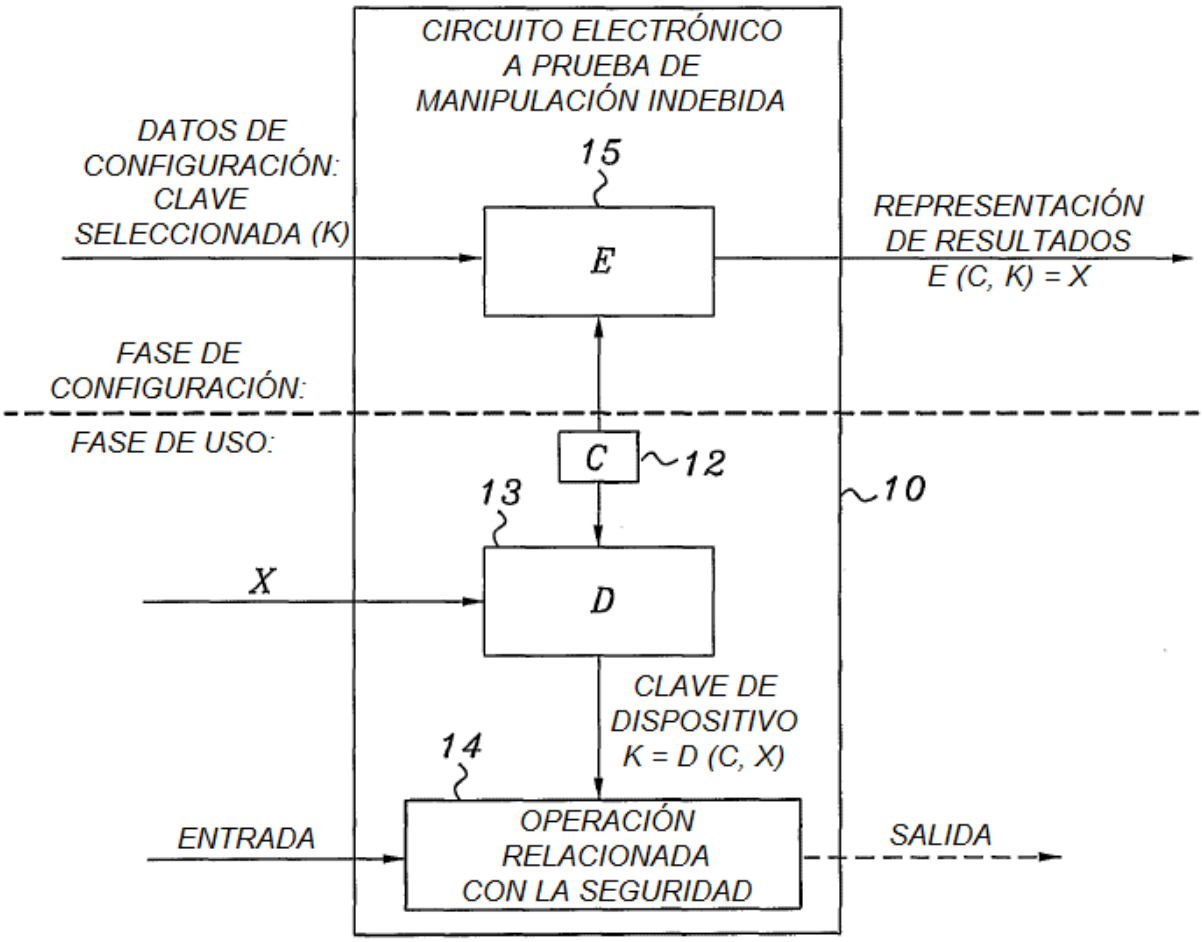
CIRCUITO ELECTRÓNICO
A PRUEBA DE
MANIPULACIÓN INDEBIDA
DATOS DE
CONFIGURACIÓN:
CLAVE
SELECCIONADA (K)
15
E
REPRESENTACIÓN
DE RESULTADOS
E (C, K) = X
FASE DE
CONFIGURACIÓN:
FASE DE USO:
C
12
10
13
X
D
CLAVE DE
DISPOSITIVO
K = D (C, X)
14
ENTRADA
OPERACIÓN
RELACIONADA
CON LA SEGURIDAD
SALIDA

Fig. 6

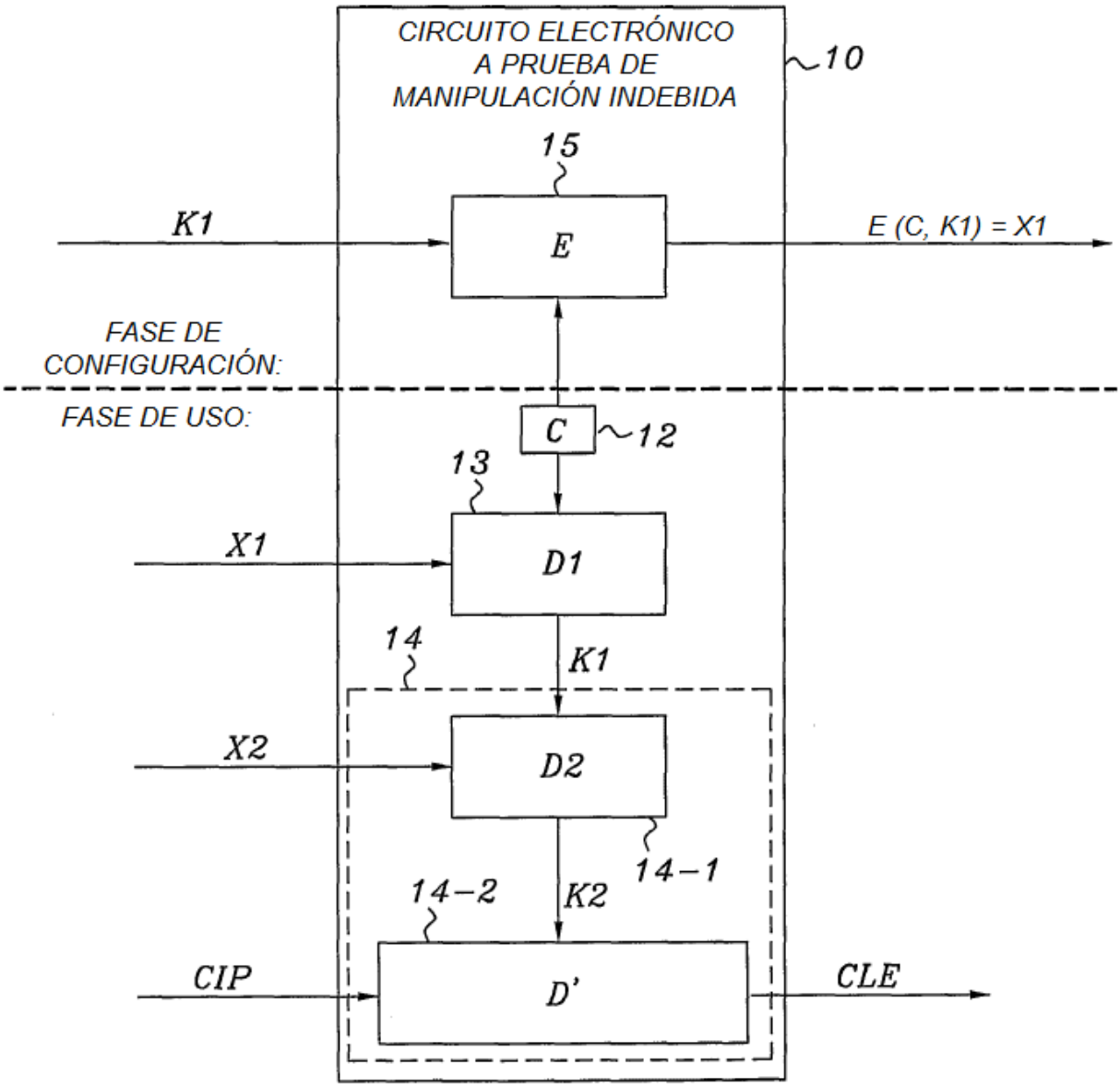
CIRCUITO ELECTRÓNICO
A PRUEBA DE
MANIPULACIÓN INDEBIDA
10
15
K1
E
E (C, K1) = X1
FASE DE
CONFIGURACIÓN:
FASE DE USO:
C
12
13
X1
D1
14
K1
X2
D2
14-1
14-2
K2
CIP
D'
CLE

Fig. 7

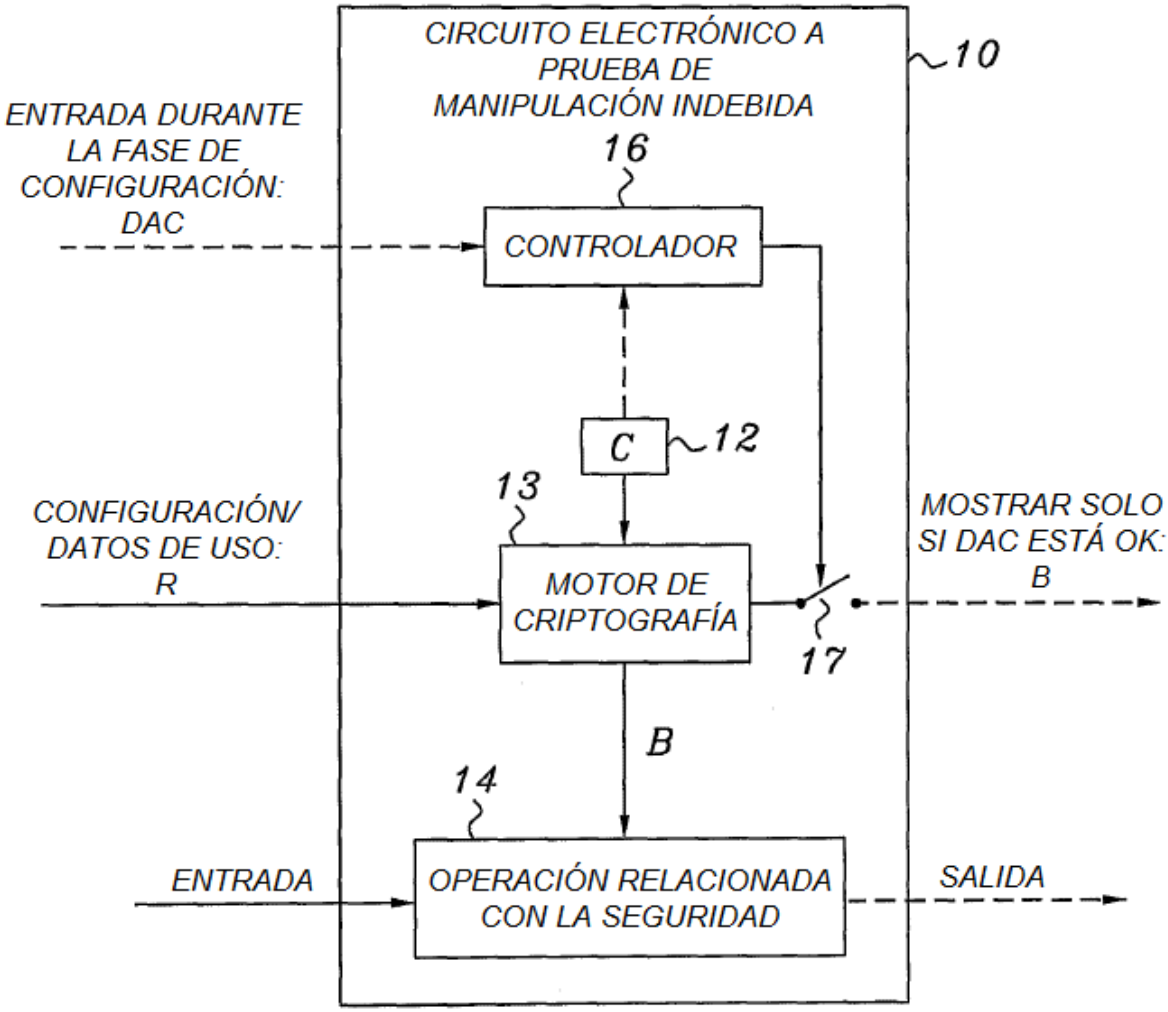
CIRCUITO ELECTRÓNICO A PRUEBA DE MANIPULACIÓN INDEBIDA
10
16
ENTRADA DURANTE LA FASE DE CONFIGURACIÓN: DAC
CONTROLADOR
C
12
13
CONFIGURACIÓN/ DATOS DE USO: R
MOTOR DE CRIPTOGRAFÍA
17
MOSTRAR SOLO SI DAC ESTÁ OK: B
B
14
ENTRADA
OPERACIÓN RELACIONADA CON LA SEGURIDAD
SALIDA

Fig. 8

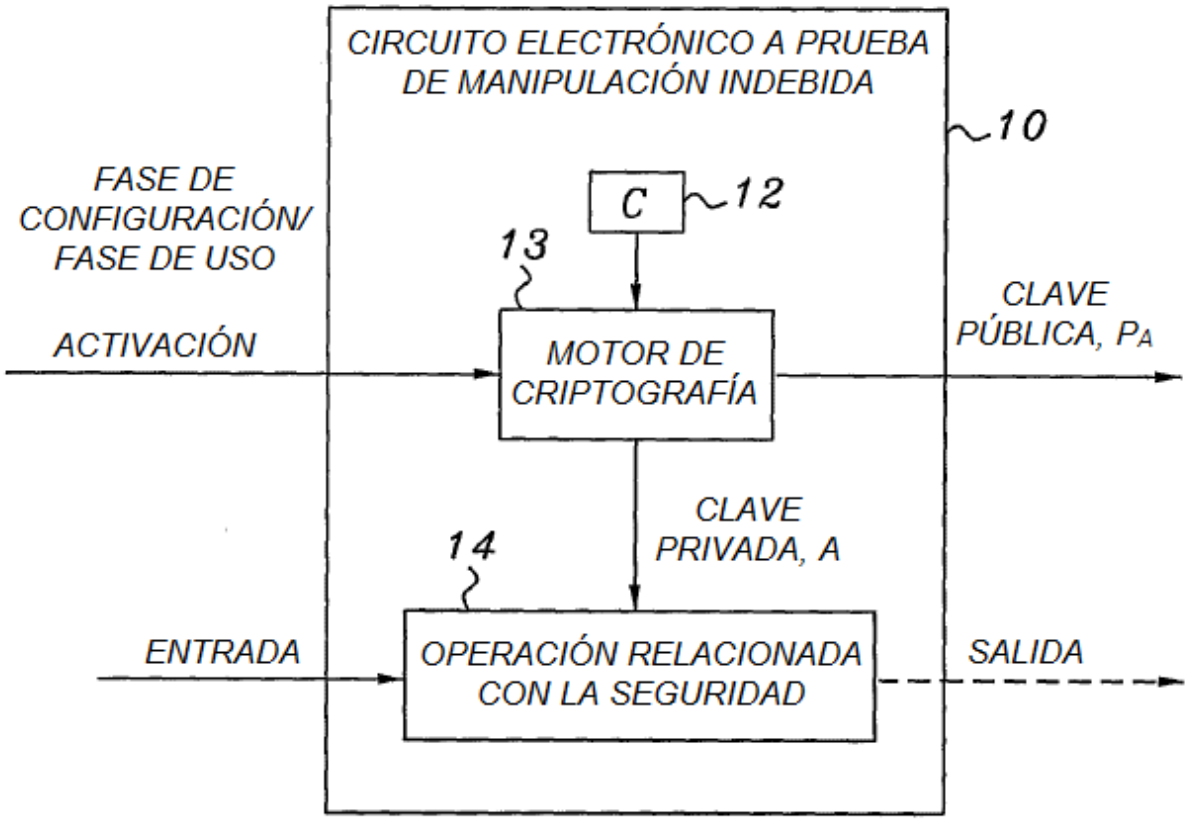
CIRCUITO ELECTRÓNICO A PRUEBA DE MANIPULACIÓN INDEBIDA
10
FASE DE CONFIGURACIÓN/ FASE DE USO
C
12
13
ACTIVACIÓN
MOTOR DE CRIPTOGRAFÍA
CLAVE PÚBLICA, PA
CLAVE PRIVADA, A
14
ENTRADA
OPERACIÓN RELACIONADA CON LA SEGURIDAD
SALIDA

Fig. 9

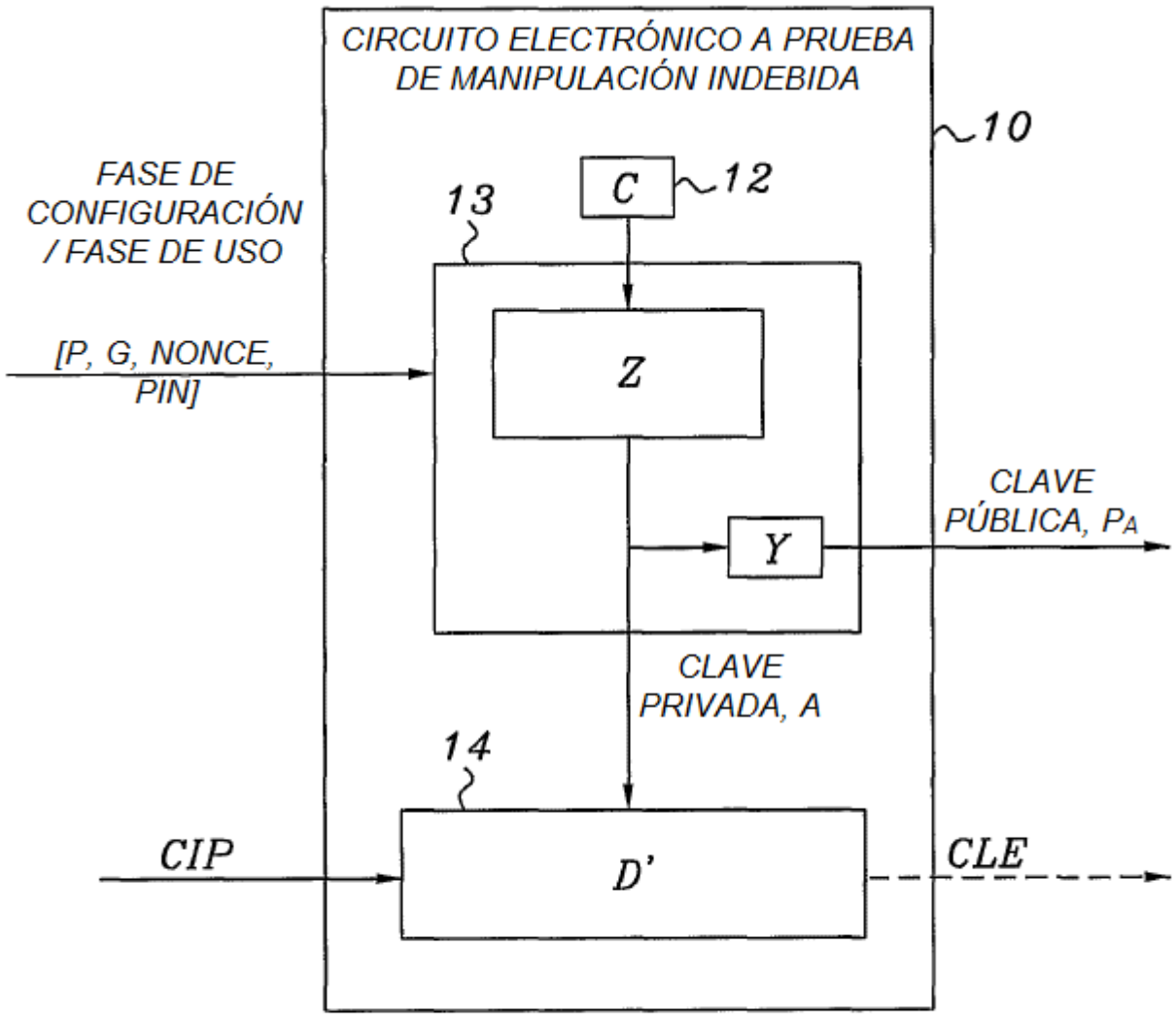
CIRCUITO ELECTRÓNICO A PRUEBA DE MANIPULACIÓN INDEBIDA
10
FASE DE CONFIGURACIÓN / FASE DE USO
13
C
12
[P, G, NONCE, PIN]
Z
Y
CLAVE PÚBLICA, PA
CLAVE PRIVADA, A
14
CIP
D'
CLE

Fig. 10

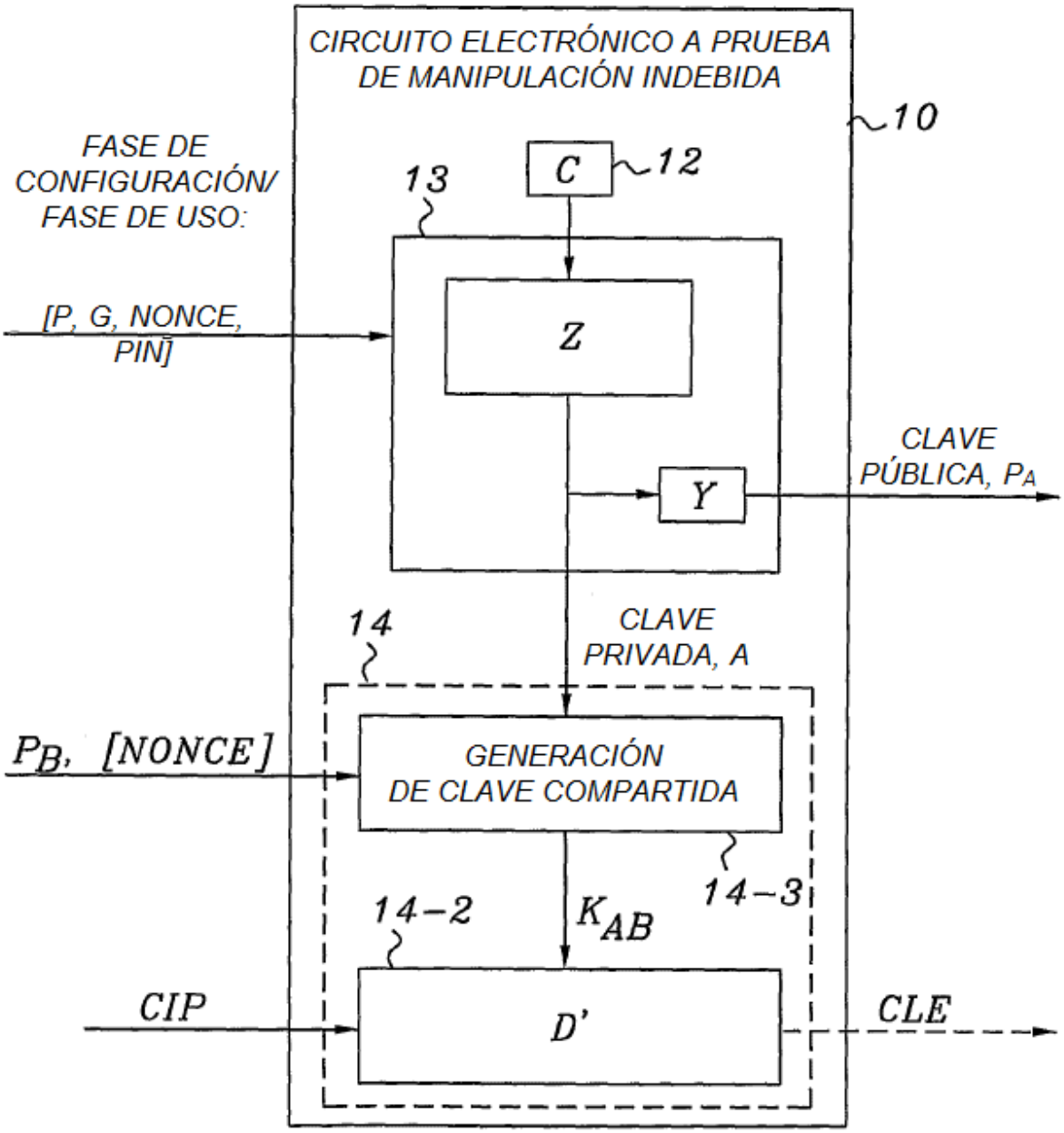
CIRCUITO ELECTRÓNICO A PRUEBA DE MANIPULACIÓN INDEBIDA
10
FASE DE CONFIGURACIÓN/ FASE DE USO:
13
C
12
[P, G, NONCE, PIN]
Z
Y
CLAVE PÚBLICA, PA
14
CLAVE PRIVADA, A
PB, [NONCE]
GENERACIÓN DE CLAVE COMPARTIDA
14-3
14-2
KAB
CIP
D'
CLE

Fig. 11

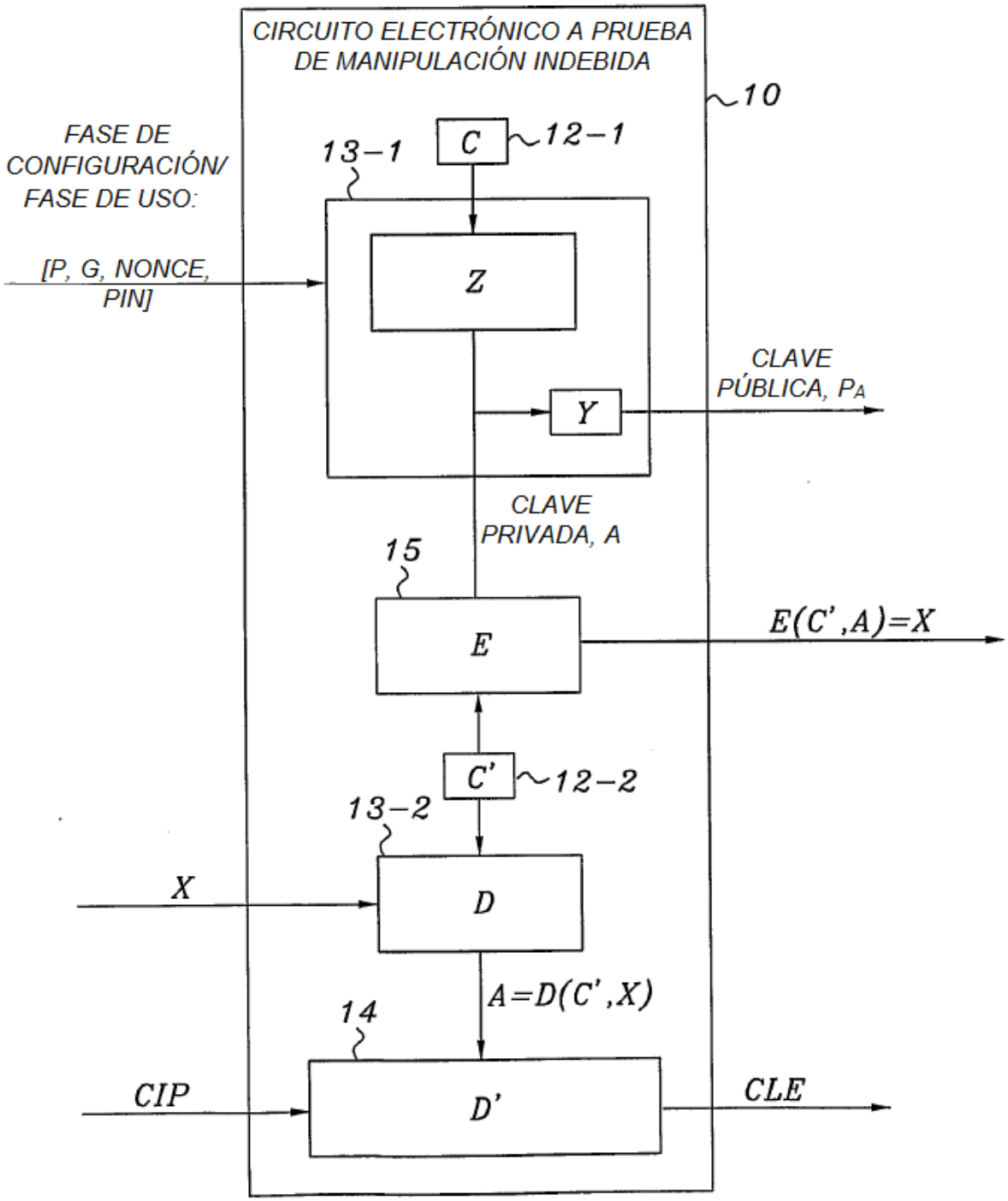
CIRCUITO ELECTRÓNICO A PRUEBA DE MANIPULACIÓN INDEBIDA
10
FASE DE CONFIGURACIÓN/ FASE DE USO:
[P, G, NONCE, PIN]
13–1
C
12–1
Z
Y
CLAVE PÚBLICA, PA
CLAVE PRIVADA, A
15
E
E(C',A)=X
C'
12–2
13–2
X
D
A=D(C',X)
14
CIP
D'
CLE

Fig. 12

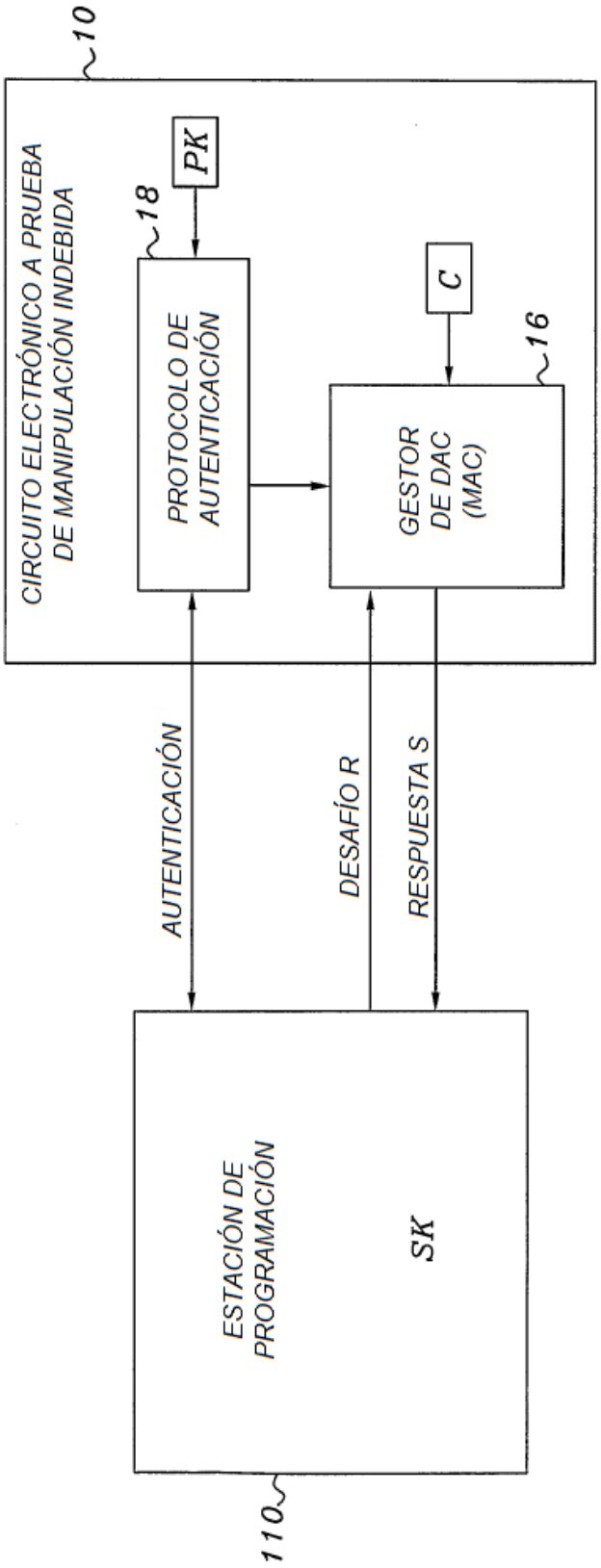
10
CIRCUITO ELECTRÓNICO A PRUEBA DE MANIPULACIÓN INDEBIDA
18
PK
PROTOCOLO DE AUTENTICACIÓN
C
16
GESTOR DE DAC (MAC)
AUTENTICACIÓN
DESAFÍO R
RESPUESTA S
ESTACIÓN DE PROGRAMACIÓN
SK
110

Fig. 13

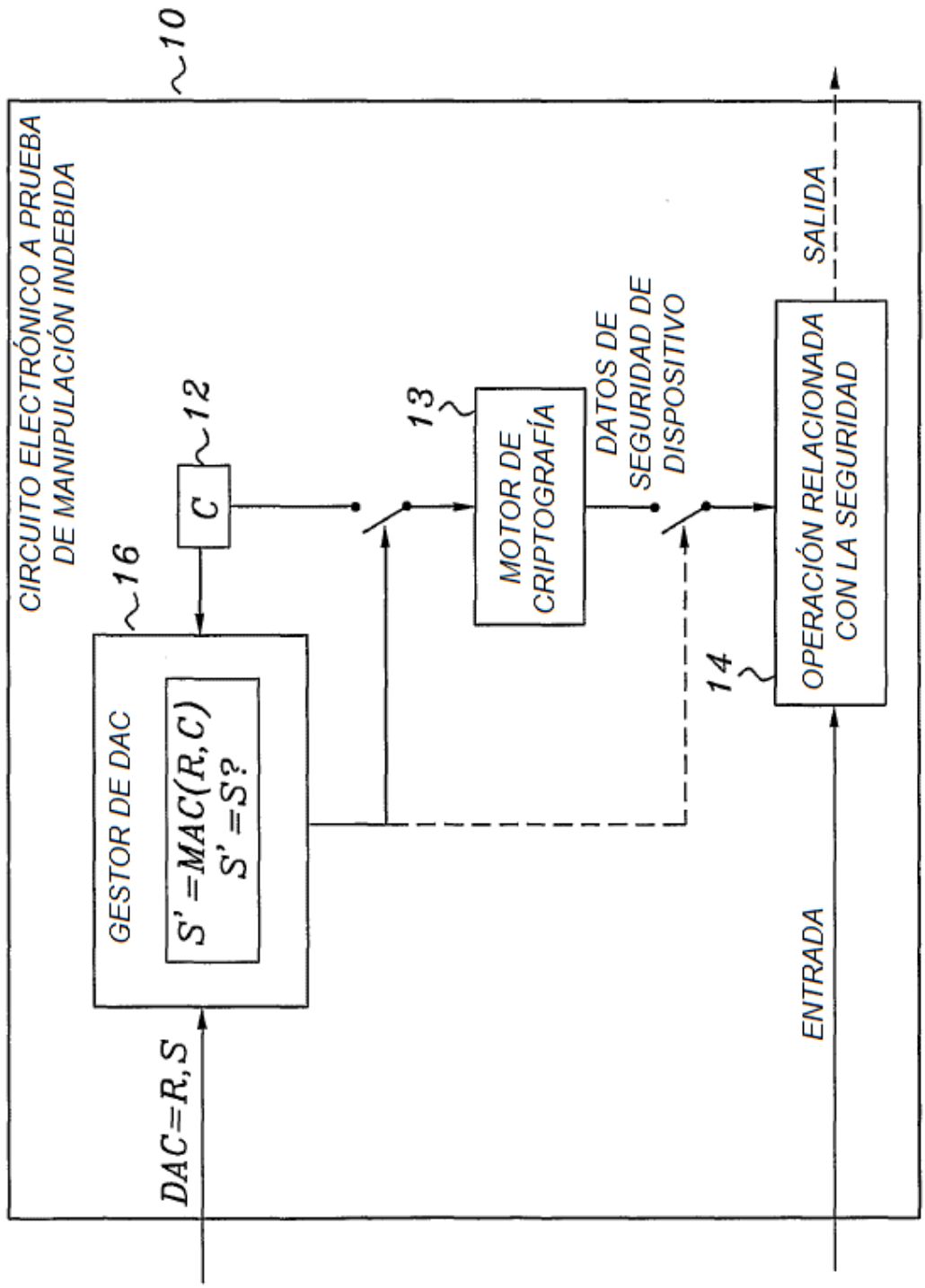
CIRCUITO ELECTRÓNICO A PRUEBA DE MANIPULACIÓN INDEBIDA
10
GESTOR DE DAC
16
S' =MAC(R,C)
S' =S?
C
12
13
MOTOR DE CRIPTOGRAFÍA
DATOS DE SEGURIDAD DE DISPOSITIVO
14
OPERACIÓN RELACIONADA CON LA SEGURIDAD
SALIDA
ENTRADA
DAC=R,S

Fig. 14

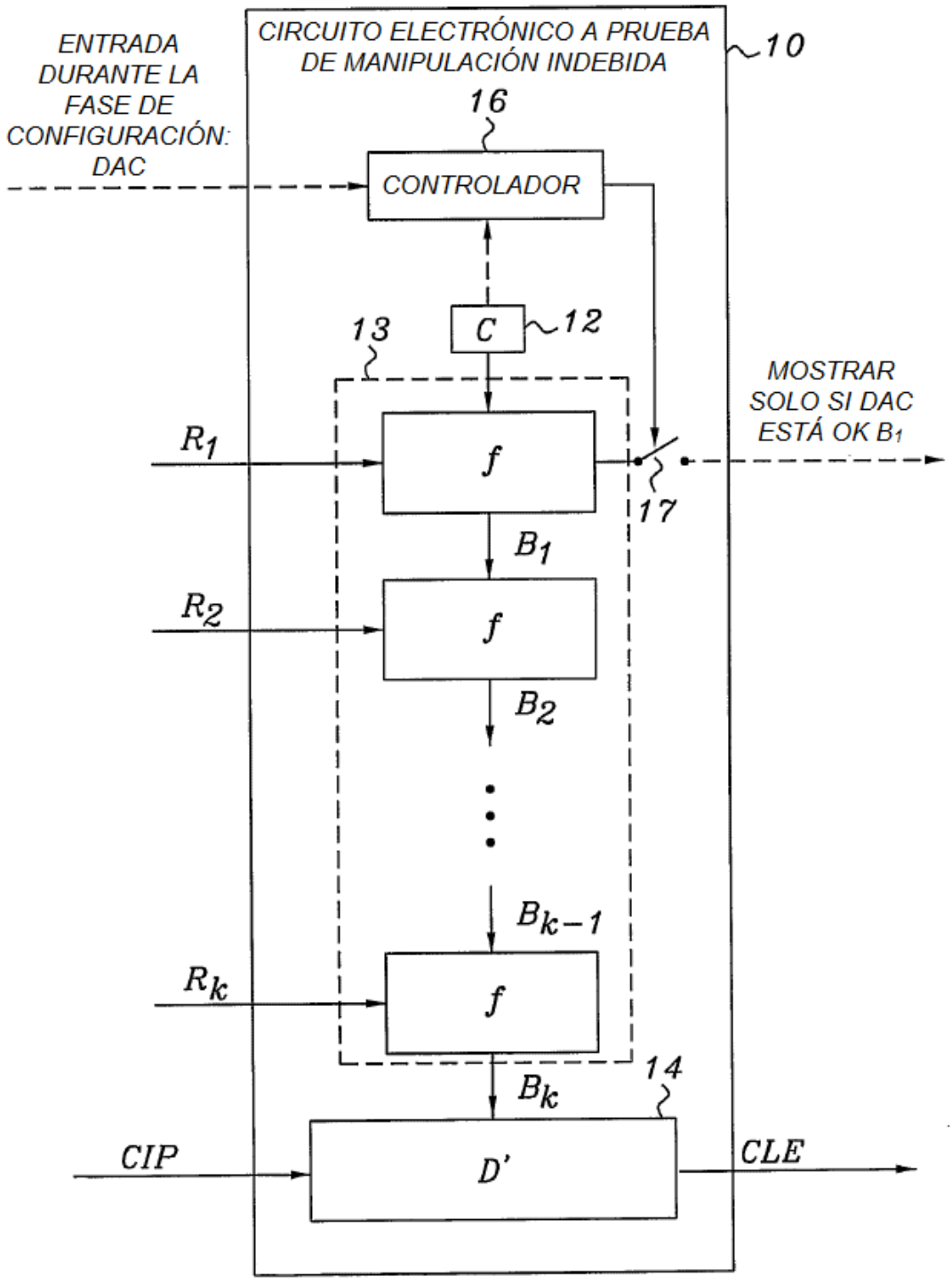
ENTRADA DURANTE LA FASE DE CONFIGURACIÓN: DAC
CIRCUITO ELECTRÓNICO A PRUEBA DE MANIPULACIÓN INDEBIDA
10
16
CONTROLADOR
C
12
13
MOSTRAR SOLO SI DAC ESTÁ OK B1
R1
f
17
B1
R2
f
B2
Bk−1
Rk
f
14
Bk
CIP
D'
CLE

Fig. 15

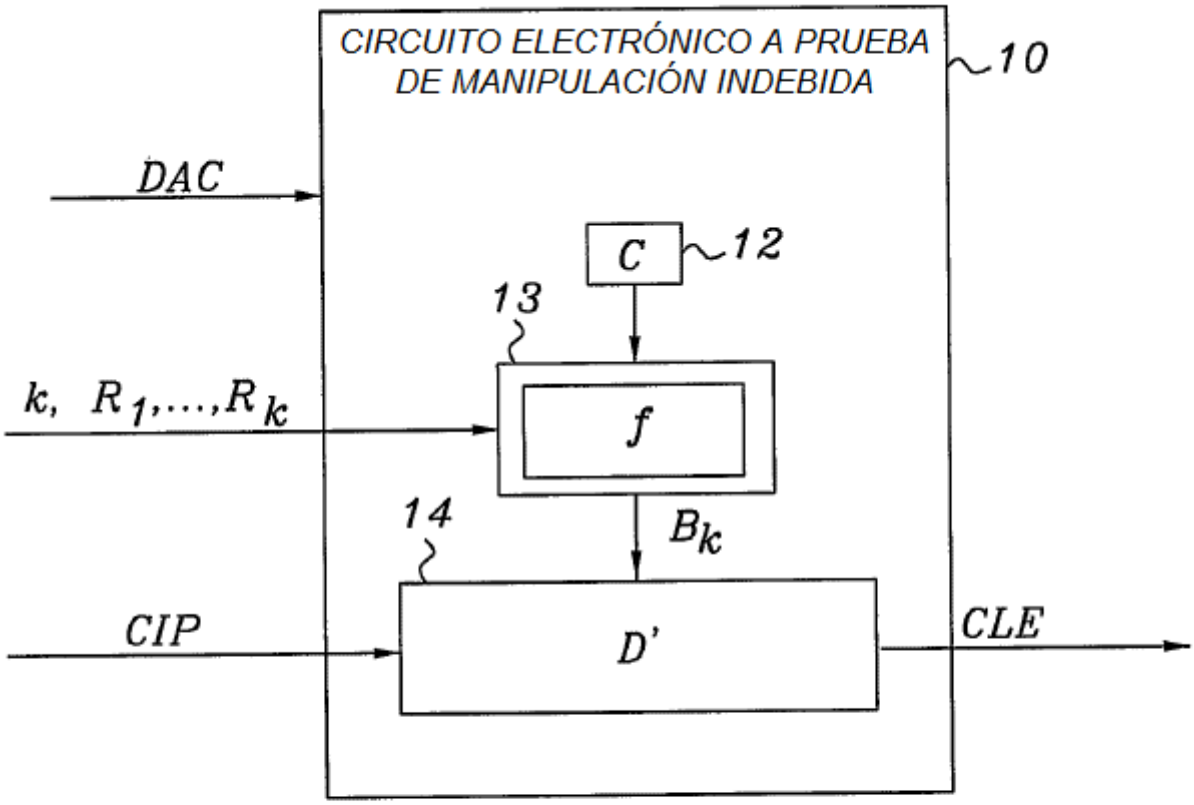
CIRCUITO ELECTRÓNICO A PRUEBA DE MANIPULACIÓN INDEBIDA
10
DAC
C
12
13
k, R1,...,Rk
f
14
Bk
CIP
D'
CLE

Fig. 16