(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 764 128**

(51) Int. CI.:

G09C 1/00 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.12.2016 E 16205920 (8)**

(97) Fecha y número de publicación de la concesión europea: **13.11.2019 EP 3340212**

(54) Título: **Dispositivo de lectura para leer una marca compuesta que comprende una función física no clonable para la lucha contra la falsificación**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.06.2020

(73) Titular/es:

MERCK PATENT GMBH (100.0%)
Frankfurter Strasse 250
64293 Darmstadt, DE

(72) Inventor/es:

ENDRESS, THOMAS;
SZABO, DANIEL y
WAHL, FABIAN

(74) Agente/Representante:

SÁNCHEZ SILVA, Jesús Eladio

DESCRIPCIÓN

Dispositivo de lectura para leer una marca compuesta que comprende una función física no clonable para la lucha contra la falsificación

Campo de la invención

La presente invención se refiere al campo de la protección contra la falsificación de productos. Específicamente, la invención está dirigida a un método de lectura con un dispositivo lector de una marca que comprende una función física no clonable, PUF, y un dispositivo lector correspondiente. En particular, sin limitación, tal dispositivo lector puede usarse en relación con o puede formar un componente de un sistema de seguridad de múltiples componentes, en particular de un sistema de protección contra la falsificación, que también se describe en la presente descripción como parte de una solución de seguridad global para protección contra la falsificación.

Antecedentes

En muchas industrias, la falsificación de productos es un problema sustancial que afecta significativamente no solo los ingresos de los fabricantes de productos originales, sino que incluso puede representar una grave amenaza para la salud e incluso la vida de los consumidores u operadores de productos falsificados, es decir, productos falsos. Tales categorías de productos relevantes para la seguridad incluyen, en particular, piezas para automóviles y aviones, componentes para la construcción de edificios u otra infraestructura, alimentos e incluso dispositivos médicos y farmacéuticos.

Con el fin de limitar la falsificación y abordar en particular tales preocupaciones de seguridad, la industria ha desarrollado una serie de diferentes medidas de protección. Las medidas de protección ampliamente utilizadas comprenden agregar un llamado elemento de seguridad a un producto, el elemento es bastante difícil de falsificar. Por ejemplo, los hologramas, las tintas ópticamente variables, los hilos de seguridad y las partículas magnéticas incrustadas son elementos de seguridad conocidos que son difíciles de reproducir por los falsificadores. Si bien algunos de estos elementos de seguridad son "visibles", es decir, pueden verse o de cualquier otra manera reconocerse fácilmente por un usuario del producto, otros elementos de seguridad son "encubiertos", es decir, están ocultos y solo pueden detectarse mediante el uso de dispositivos específicos, tales como fuentes de luz UV, espectrómetros, microscopios o detectores de campo magnético, o incluso equipos forenses más sofisticados. Los ejemplos de elementos de seguridad encubiertos son, en particular, impresiones con tinta luminiscente o tinta que solo es visible en la parte infrarroja del espectro electromagnético, pero no en su parte visible, composiciones de materiales específicos y pigmentos magnéticos.

Un grupo específico de elementos de seguridad, que se utilizan en particular en criptografía, se conoce como "Funciones físicas no clonables" (PUF). Las PUF a veces también se denominan como "Funciones físicas no clonables" o "Funciones físicas aleatorias". Una PUF es una entidad física que se incorpora en una estructura física y es fácil de evaluar, pero difícil de predecir, incluso para un atacante con acceso físico a la PUF. Las PUF dependen de la singularidad de su microestructura física, que típicamente incluye un componente aleatorio que ya está intrínsecamente presente en la entidad física o que se introduce o genera explícitamente en la entidad física durante su fabricación y que es sustancialmente incontrolable e impredecible. En consecuencia, incluso las PUF producidas por el mismo proceso de fabricación difieren al menos en su componente aleatorio y, por lo tanto, pueden distinguirse. Si bien en la mayoría de los casos, las PUF son elementos encubiertos, esto no es una limitación y las PUF visibles también son posibles.

Las PUF se conocen en particular en relación con su implementación en circuitos electrónicos integrados por medio de variaciones mínimas inevitables de las microestructuras producidas en un chip dentro de las tolerancias dadas relacionadas con el proceso, y específicamente cuando se usan para derivar claves criptográficas a partir de las mismas, por ejemplo, en chips para tarjetas inteligentes u otros chips relacionados con la seguridad. Un ejemplo de una explicación y aplicación de tales PUF relacionadas con los chips se describe en el artículo ″ Background on Physical Unclonable Functions (PUFs)", Virginia Tech, Departamento de Ingeniería Eléctrica e Informática, 2011, que está disponible en Internet en el hipervínculo http://rijn-dael.ece.vt.edu/puf/background.html.

Sin embargo, también se conocen otros tipos de PUF, tales como las distribuciones aleatorias de fibras en papel utilizadas como sustrato para la fabricación de billetes, en donde la distribución y orientación de las fibras puede detectarse por detectores específicos y utilizada como un elemento de seguridad del billete. Para evaluar una PUF, se utiliza el llamado esquema de autenticación de desafío-respuesta. El "desafío" es un estímulo físico aplicado a la PUF y la "respuesta" es su reacción al estímulo. La respuesta depende de la naturaleza incontrolable e impredecible de la microestructura física y, por lo tanto, puede usarse para autenticar la PUF y, por lo tanto, también un objeto físico del que forma parte la PUF. Un desafío específico y su respuesta correspondiente juntos forman un llamado "par desafío-respuesta" (CRP).

La criptografía asimétrica, a veces también denominada "criptografía de clave pública" o "criptografía de clave pública/privada" es una tecnología conocida basada en un sistema criptográfico que utiliza pares de claves, en donde

cada par de claves comprende una clave pública y una clave privada. Las claves públicas pueden difundirse ampliamente y, usualmente, incluso están disponibles públicamente, mientras que las claves privadas se mantienen en secreto y usualmente solo las conoce su propietario o titular. La criptografía asimétrica permite tanto (i) la autenticación, que es cuando la clave pública se utiliza para verificar que un titular de la clave privada asociada originó una información particular, por ejemplo, un mensaje o datos almacenados que contienen la información, al firmar digitalmente con su clave privada, como (ii) la protección de la información, por ejemplo, un mensaje o datos almacenados, mediante cifrado, de manera que solo el propietario/titular de la clave privada asociada pueda descifrar el mensaje cifrado con la clave pública por otra persona.

Recientemente, se ha desarrollado la tecnología de cadena de bloques, en donde una cadena de bloques es un libro de contabilidad público en forma de una base de datos distribuida que contiene una pluralidad de bloques de datos y que mantiene una lista de registros de datos en continuo crecimiento y está reforzada contra la manipulación y la revisión por medios criptográficos. Una aplicación destacada de la tecnología de cadena de bloques es la moneda virtual de Bitcoin utilizada para transacciones monetarias en Internet. El proyecto Ethereum proporciona, por ejemplo, otra plataforma de cadena de bloques conocida. En esencia, una cadena de bloques puede describirse como un protocolo descentralizado para registrar transacciones entre las partes, que captura y almacena de manera transparente cualquier modificación en su base de datos distribuida y las guarda "para siempre", es decir, mientras exista la cadena de bloques. Almacenar información en una cadena de bloques implica firmar digitalmente la información que va a almacenarse en un bloque de la cadena de bloques. Además, el mantenimiento de la cadena de bloques implica un proceso llamado "minería de cadena de bloques", en donde los llamados "mineros" que forman parte de la infraestructura de la cadena de bloques, verifican y sellan cada bloque, de manera que la información contenida en el mismo se guarde "para siempre" y el bloque ya no pueda modificarse.

El documento WO 2007/031908 describe un dispositivo, sistema y método para determinar la autenticidad de un artículo mediante el uso de dispositivos PUF que comprenden un patrón PUF que puede firmarse por una clave privada.

El documento EP 2 999 156 A1 describe un sistema de determinación de autenticidad del dispositivo y un método para usar información impresa, que puede verse desde el exterior de un dispositivo o componente, el dispositivo y el componente que tienen montado en el mismo un chip semiconductor que tiene una función PUF y una función de cifrado, e incluye datos auxiliares, para generar información secreta que es difícil de duplicar con el uso de la función PUF, e información secreta.

El documento EP 2 911 335 A1 describe un dispositivo para identificar productos genuinos y falsificados mediante el uso de pares de desafío-respuesta (CRP) basados en la función física no clonable (PUF), dicho dispositivo que comprende una o más antenas para emitir una serie de primeras señales electromagnéticas como un desafío válido y para recibir una serie de segundas señales electromagnéticas como respuestas del desafío válido, tanto el desafío como la respuesta forman un par desafío-respuesta para dicho desafío válido, en donde al menos una de las antenas es una antena de banda ancha, una unidad de radio definida por software (SDR) dispuesta para emitir dicha(s) primera(s) señal(es) electromagnética(s) como desafío(s) y dispuesta para recibir dicha(s) segunda(s) señal(es) electromagnética(s) como respuesta(s), una unidad de evaluación del par desafío-respuesta para analizar dicho(s) par(es) de desafío-respuesta y para proporcionar un resultado que reconozca si el desafío válido es genuino o falsificado.

Los materiales específicos relacionados con la seguridad y los elementos de seguridad, algunos de los cuales se relacionan con formas específicas de PUF, se describen en cada uno de los siguientes:

PAWAN KUMAR Y OTROS: "Future prospects of luminescent nanomaterial based security inks: from synthesis to anti-counterfeiting applications", NANOS-CALE, vol. 8, núm. 30, 1 de enero de 2016 (01-01-2016), páginas 14297-14340;

O. IVANOVA Y OTROS: " Unclonable security features for additiveD4 manufacturing", ADDITIVE MANUFACTURING, vol. 1-4, 1 de octubre de 2014 (2014-10-01), páginas 24-31;

WONG CHAU-WAI Y OTROS: "Counterfeit detection using paper PUF and mobile cameras", 2015 IEEE INTERNATIONAL WORKSHOP ON INFORMATION FO-RENSICS AND SECURITY (WIFS), IEEE, 16 de noviembre de 2015 (2015-11-16), páginas 1-6;

MIAO WANG Y OTROS: "Nanomaterial-based barcode", NANOSCALE, vol. 7, 25 de mayo de 2016 (25/05/2016), páginas 11240-11247;

BORA YOON Y OTROS: "Recent functional material based approaches to prevent and detect counterfeiting", JOURNAL OF MATERIALS CHEMISTRY C, vol. 1, núm. 13, 21 de enero de 2013 (2013-01-21), páginas 2388-2403;

DANIELA PAUNESCU Y OTROS: "Particles with an identity: Tracking and tracing in commodity products", POWDER TECHNOLOGY, vol. 291, 29 de diciembre de 2015 (2015-12-29), páginas 344-350;

FEI JIE Y OTROS: "Drug-laden 3D biodegradable label using QR code for anti-counterfeiting of drugs", MATERIALS SCIENCE AND ENGINEERING C, ELSEVIER SCIENCE S. A, CH, vol. 63, 4 de marzo de 2016 (04/03/2016), páginas 657-662;

F. FAYAZPOUR Y OTROS: "Digitally Encoded Drug Tablets to Combat Counterfeiting", ADVANCED MATERIALS, vol. 19, núm. 22, 19 de noviembre de 2007 (2007-11-19), páginas 3854-3858;

GOOCH JAMES Y OTROS: "Taggant materials in forensic science: A review", TRAC TRENDS IN ANALYTICAL CHEMISTRY, ELSEVIER, AMSTERDAM, NL, vol. 83, 11 de agosto de 2016 (2016-08-11), páginas 49-54,

US 2013/127959 A1 titulado "Method and apparatus for fractal identification";

US 2015/183257 A1 titulado "Verification of pharmaceutical product packaging to prevent counterfeits, using hidden security features revealed with a laser pointer";

NERALAGATTA M. SANGEETHA Y OTROS: "3D assembly of upconverting NaYF4 nanocrystals by AFM nanoxerography: creation of anti-counterfeiting microtags", NANOSCALE, vol. 5, núm. 20, 1 de enero de 2013 (2013-01-01), página 9587;

CHEUN NGEN CHONG Y OTROS: "Anti-counterfeiting with a Random Pattern", EMERGING SECURITY INFORMATION, SYSTEMS AND TECHNOLOGIES, 2008. SECURWARE '08. SECOND INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, ESTADOS UNIDOS, 25 de agosto de 2008 (2008-08-25), páginas 146-153;

DR FRED JORDAN Y OTROS: "May/June 2012 PHARMACEUTICAL ENGINEERING Anti-Counterfeiting Technologies, "Identifying Counterfeit Medicines with Industry-Suitable Technologies", 30 de junio de 2012 (30-06-2012);

H Lou Y OTROS: "The familiar concept of the barcode for tracking may be coming to a chemical reaction near you in the form of coded microparticles", 1 de octubre de 2004 (2004-10-01),

PETER ZIJLSTRA Y OTROS: "Five-dimensional optical recording mediated by surface plasmons in gold nanorods", NATURE, MACMILLAN JOURNALS LTD., ETC.', vol. 459, 21 de mayo de 2009 (2009-05-21), páginas 410-413;

JISEOK LEE Y OTROS: "Universal process-inert encoding architecture for polymer microparticles", NATURE MATERIALS, vol. 13, núm. 5, 13 de abril de 2014 (13-04-2014), páginas 524-529;

YUHAI ZHANG Y OTROS: "Multicolor Barcoding in a Single Upconversion Crystal", JOURNAL OF THE AMERICAN CHEMICAL SOCIETY, vol. 136, núm. 13, 2 de abril de 2014 (02/04/2014), páginas 4893-4896;

JANGBAE KIM Y OTROS: "Anti-counterfeit nanoscale fingerprints based on randomly distributed nanowires", NANOTECHNOLOGY, 10P, BRISTOL, GB, vol. 25, núm. 15, 20 de marzo de 2014 (2014-03-20), página 155303;

JULIEN ANDRES Y OTROS: "A New Anti-Counterfeiting Feature Relying on Invisible Luminescent Full Color Images Printed with Lanthanide-Based Inks", ADVANCED FUNCTIONAL MATERIALS, WILEY - VCH VERLAG GMBH & CO. KGAA, DE, vol. 24, no. 32, 27 de agosto de 2014 (2014-08-27), páginas 5029-5036;

RADZIWON MICHAL Y OTROS: "Anti-counterfeit Solution from Organic Semiconductor", PROCEDIA ENGINEERING, ELSEVIER, AMSTERDAM, NL, vol. 69, 25 de marzo de 2014 (2014-03-25), páginas 1405-1409.

Resumen de la invención

La presente invención aborda el problema de proporcionar una manera de leer de manera efectiva una marca de un objeto físico, tal como un producto, para permitir una verificación de la autenticidad del objeto, en donde la marca sirve para proteger el objeto contra la falsificación y la manipulación y comprende una PUF.

Una solución a este problema se proporciona mediante la enseñanza de las reivindicaciones independientes adjuntas. Las enseñanzas de las reivindicaciones dependientes proporcionan diversas modalidades preferidas de la presente invención.

Además, se presenta en la presente descripción una solución de seguridad completa, que incluye diversos aparatos y métodos como diferentes aspectos que pueden formar parte de una solución de seguridad global para proteger de manera eficaz los objetos físicos contra la falsificación y la manipulación.

Un primer aspecto de la solución de seguridad proporcionada en la presente descripción se dirige a una marca de seguridad compuesta para un objeto físico, en particular una marca de seguridad compuesta contra la falsificación. La

marca de seguridad compuesta comprende una función física no clonable, PUF, y una representación de una firma digital o de un puntero que indica una localización donde puede accederse a dicha firma digital. La firma digital firma digitalmente un valor resumen resultante de la aplicación de una función resumen criptográfica predeterminada a los datos que representan una respuesta generada por la PUF en reacción a un desafío de un esquema de autenticación de desafío-respuesta predeterminado.

El término "objeto físico", como se usa en la presente descripción, se refiere a cualquier tipo de objeto físico, en particular a cualquier tipo de objeto hecho por el hombre o producto natural, tal como un vegetal o una pieza de materia prima natural. Además, como se usa en la presente descripción, el término "objeto físico" también puede referirse a una persona o un animal al que puede aplicarse una marca de seguridad compuesta. Un objeto físico puede comprender en sí mismo múltiples partes, por ejemplo, un bien consumible y un empaque del mismo.

El término "marca de seguridad compuesta", como se usa en la presente descripción, se refiere a una entidad física que comprende al menos dos marcas individuales diferentes ya que sus componentes, (por lo tanto, "compuesto"), se adaptan para aplicarse o crearse en o estar en un objeto físico, y permanece accesible después que se aplique a o se cree en o esté en el físico para evaluarlo. En la marca de seguridad compuesta de acuerdo con el primer aspecto anterior de la solución de seguridad, un primer componente es una PUF y un segundo componente es una representación de una firma digital o de un puntero que indica una localización donde puede accederse a dicha firma digital. En particular, los dos o más componentes de la marca de seguridad compuesta pueden localizarse en o estar dentro de un mismo sustrato o parte del objeto físico. Alternativamente, un subconjunto de los componentes o todos ellos pueden localizarse en o estar dentro de sustratos separados u otras partes del objeto físico.

El término "firma digital", como se usa en la presente descripción, se refiere a un conjunto de uno o más valores digitales que confirman la identidad de un remitente u emisor de datos digitales y la integridad de los últimos. Para crear una firma digital, se genera un valor resumen a partir de los datos que van a protegerse por medio de la aplicación de una función resumen criptográfica adecuada. Este valor resumen se cifra con una clave privada (a veces también llamada "clave segura") de un sistema criptográfico asimétrico, por ejemplo, basado en el conocido sistema criptográfico RSA, en donde la clave privada típicamente es conocida solo por el remitente/emisor. Usualmente, la firma digital comprende los propios datos digitales, así como también el valor resumen derivado de estos por el remitente/emisor. Un destinatario puede aplicar la misma función resumen criptográfica a los datos digitales recibidos, usar la clave pública correspondiente a dicha clave privada para descifrar el valor resumen comprendido en la firma digital y comparar el valor resumen descifrado de la firma digital con el valor resumen generado mediante la aplicación de la función resumen criptográfica a los datos digitales recibidos. Si ambos valores resumen coinciden, esto indica que la información digital no se ha modificado y, por lo tanto, su integridad no se ha visto comprometida. Además, la autenticidad del remitente/emisor de los datos digitales se confirma por medio del sistema criptográfico asimétrico, que garantiza que el cifrado mediante el uso de la clave pública solo funcione, si la información cifrada se cifró con la clave privada que va a asociarse matemáticamente con esa clave pública.

El término "función resumen criptográfica", como se usa en la presente descripción, se refiere a un tipo especial de función resumen, es decir, una función o algoritmo matemático que asigna datos de tamaño arbitrario a una cadena de bits de un tamaño fijo (un valor resumen), que se diseña para que sea también una función unidireccional, es decir, una función que sea fácil de calcular en cada entrada, pero difícil de invertir dada la imagen de una entrada aleatoria. Preferentemente, la función resumen criptográfica es una denominada función resumen resistente a colisiones, es decir, una función resumen que se diseña de manera que sea difícil encontrar dos conjuntos de datos diferentes d1 y d2, de manera que resumen (d1) = resumen (d2). Los ejemplos destacados de tales funciones resumen son las funciones resumen de la familia SHA, por ejemplo, la función SHA-3 o las funciones resumen de la familia BLAKE, por ejemplo, la función BLAKE2. En particular, pueden usarse las llamadas "funciones resumen criptográficas comprobadamente seguras". Estas son funciones resumen para las cuales puede demostrarse matemáticamente un cierto nivel de seguridad suficiente. En la presente solución de seguridad, la seguridad de la función resumen criptográfica se mejora aún más por el hecho de que la lectura de una marca que comprende una PUF, particularmente de una marca de seguridad compuesta, como se describe en la presente descripción, tiene lugar en una localización y hora en particular, donde el objeto físico que lleva la marca está realmente presente en tal localización y tiempo. Esto puede usarse o bien para aumentar el nivel absoluto de seguridad que puede lograrse o para permitir el uso de funciones resumen criptográficas que funcionan con conjuntos de datos más pequeños, por ejemplo, cadenas de datos más cortas como entradas y/o salidas, mientras todavía se proporciona un nivel dado de seguridad requerida.

Un "puntero que indica una localización donde puede accederse a dicha firma digital", como se usa en la presente descripción, puede ser en particular un puntero a una base de datos local o remota o a una dirección de servidor o dirección de Internet, por ejemplo, un hipervínculo o similar, en el que puede accederse a la firma digital, por ejemplo, descargarse. El puntero puede implementarse particularmente mediante el uso de un transmisor RFID o un código de barras simple o multidimensional, tal como un código QR o un código DATAMATRIX.

La marca de seguridad compuesta de acuerdo con el primer aspecto de la presente solución de seguridad puede usarse por una primera parte, por ejemplo, un emisor de un objeto físico en forma de un producto, para proteger cualquier objeto físico al que pertenezcan los componentes de la marca, es decir puede aplicarse al menos una PUF respectiva y la firma digital correspondiente de su respuesta. En particular, la marca se aplica preferentemente al

objeto físico de tal manera que no pueda separarse nuevamente del objeto sin destruir la marca o al menos partes de la misma.

Ya por naturaleza, la PUF es "no clonable" y por lo tanto proporciona un primer nivel de seguridad, es decir, como un medio para confirmar la autenticidad de la marca y, por lo tanto, del objeto físico. Sin embargo, este primer nivel de seguridad se mejora aún más a un segundo nivel de seguridad más alto mediante la combinación de la PUF con la firma digital que firma criptográficamente un valor resumen derivado de una respuesta de la PUF a un desafío de un esquema predeterminado de desafío-respuesta perteneciente a la PUF. De esta manera, en analogía a una firma digital para documentos electrónicos, se crea una firma digital para objetos físicos para proteger tales objetos, particularmente contra la falsificación. Con el fin de verificar la autenticidad del objeto físico, respectivamente, su origen, una segunda parte que recibe el objeto físico a la PUF de la marca del objeto físico aplica un desafío de acuerdo con este esquema de desafío-respuesta y se aplica la misma función resumen criptográfica para generar un valor resumen respectivo a partir de datos que representan la respuesta recibida de la PUF. El valor resumen contenido en la firma digital puede derivarse mediante el descifrado de la firma digital mediante el uso de su clave pública relacionada y luego pueden compararse los dos valores resumen. Si coinciden, esto indica que el objeto físico es auténtico y que la marca de seguridad compuesta no se ha manipulado. De cualquier otra manera, es decir, si no coinciden, esto indica que podría haber ocurrido algún tipo de fraude desde que el emisor aplicó la marca de seguridad compuesta al objeto físico.

En consecuencia, la marca de seguridad compuesta proporciona un nivel adicional de seguridad y, por lo tanto, una manera mejorada de proteger un objeto físico contra la falsificación y la manipulación. Además, como la respuesta de la PUF a un desafío de acuerdo con el esquema desafío-respuesta produce datos digitales, por ejemplo, una cadena de datos, la marca de seguridad compuesta puede usarse para proteger cualquier objeto físico al que pueda aplicarse tal marca, incluso si el objeto en sí no proporciona ningún dato digital.

A continuación, se describen las modalidades preferidas de la marca de seguridad compuesta, que pueden combinarse arbitrariamente entre sí o con otros aspectos de la solución descrita en la presente descripción, a menos que tal combinación se excluya explícitamente, sea inconsistente o técnicamente imposible.

De acuerdo con una primera modalidad preferida, la PUF comprende un colorante de conversión ascendente (UCD), preferentemente una pluralidad de diferentes colorantes de conversión. Un UCD es un colorante que muestra el efecto de la conversión ascendente de fotones (UC), que es un proceso en el que la absorción secuencial de dos o más fotones conduce a la emisión de luz a una longitud de onda más corta que la longitud de onda de excitación. Es una emisión de tipo anti-Stokes. Un ejemplo típico para tal proceso es la conversión de luz infrarroja a luz visible fluorescente. Los materiales mediante los cuales puede tener lugar la conversión ascendente a menudo contienen iones de elementos de bloque d y bloque f del sistema periódico. Los ejemplos de estos iones son Ln3+, Ti2+, Ni2+, Mo3+, Re4+, Os4+, etc. Tales materiales comprenden típicamente una porción relativamente baja de ensanchamiento espectral vibriónico y, por lo tanto, muestran fluorescencia en bandas muy estrechas del espectro electromagnético. Mediante el uso de una variedad de combinaciones diferentes, es decir, mezclas, de varias sustancias de conversión ascendente, es posible generar una gran cantidad de espectros individuales distinguibles.

Por ejemplo, suponiendo una resolución espectral de 20 nm dentro de la región espectral de 400 nm a 800 nm, ya hay 2^{20} posibilidades diferentes, si la detección se limita a la pregunta binaria de si el espectro muestra o no un pico dentro de los respectivos intervalos de 20 nm. En otras palabras, puede asignarse un valor binario de "0" o "1" a cada intervalo, uno de estos valores indica la presencia de un pico en ese intervalo y el otro valor indica la ausencia de tal pico. En consecuencia, puede formarse una cadena digital a partir de los 20 valores binarios asignados a los 20 intervalos en los que se divide dicha región espectral y, por lo tanto, 2^{20}, es decir, aproximadamente 10^6 combinaciones diferentes pueden representarse por tal cadena. Si, en cambio, se usa un intervalo de solo 10 nm, los números aumentaron a 2^{40}, es decir, aproximadamente 10^{11} combinaciones diferentes. Si, además, en cada intervalo se hace una distinción adicional en el caso de cada pico, por ejemplo, si el pico respectivo está más cerca de un pico "completo" o solo de un pico "medio" (ver Figura 4 (b)), entonces en el caso de 40 intervalos, el número de combinaciones incluso se incrementa a 3^{40}, es decir, aproximadamente 10^{18} combinaciones. En consecuencia, es prácticamente imposible crear una mezcla de UCD de tal manera que muestre el mismo espectro que la mezcla original que se busca clonar.

De esta manera, los UCD pueden usarse para crear una PUF. Una ventaja de usar UCD para las PUF es que pueden aplicarse a casi cualquier objeto físico, por ejemplo, como un componente de un recubrimiento o un material del que se fabrican el objeto físico o partes del mismo. Además, los UCD son típicamente elementos encubiertos y no pueden reconocerse fácilmente sin un equipo sofisticado. Esto puede usarse para aumentar aún más el nivel de seguridad alcanzable.

De acuerdo con otra modalidad preferida, la PUF comprende un patrón físico no clonable o una estructura configurada para generar un patrón virtual en respuesta al desafío. En una variante de esta modalidad, el patrón puede comprender una gran cantidad de partículas microscópicas cuya localización y/u orientación representan un patrón físico incontrolable e impredecible que puede detectarse, pero no clonarse por medios prácticos. En otra variante preferida, dicha estructura configurada para generar un patrón virtual comprende una microestructura que se configura para crear un patrón moteado óptico cuando se ilumina con luz de una fuente de luz adecuada. En particular, la

microestructura puede comprender una pluralidad de los denominados puntos cuánticos, es decir, partículas semiconductoras muy pequeñas, que tienen solo un tamaño de varios nanómetros, de manera que sus propiedades ópticas y electrónicas difieren de las partículas más grandes y que emiten luz de longitudes de onda específicas si se les aplica electricidad o luz (es decir, como un desafío). El tamaño, la forma y el material de los puntos cuánticos, que pueden controlarse durante la fabricación, determinan estas longitudes de onda y, por lo tanto, puede crearse una gran variedad de diferentes espectros de emisión como respuestas de un esquema de desafío-respuesta relacionado. En otra variante preferida, la microestructura puede comprender una pluralidad de materiales cuánticos en forma de barra (barras cuánticas), que ofrecen un mecanismo de conversión de color similar y una gama de colores extendida como puntos cuánticos esféricos. La única ventaja de las barras cuánticas es la emisión de luz polarizada. Por supuesto, también son posibles combinaciones de las variantes anteriores de microestructuras.

El término "luz" como se usa en la presente descripción, se refiere a radiación electromagnética y puede incluir, sin limitación, radiación en la parte visible del espectro electromagnético. Por ejemplo, la luz también puede comprender radiación ultravioleta o infrarroja o además de radiación visible. Un patrón "moteado" es un patrón de intensidad producido por la interferencia mutua de un conjunto de muchos frentes de onda electromagnéticos de una longitud de onda igual o similar, por ejemplo, en el espectro visible, pero diferentes fases y, usualmente, también diferentes amplitudes. La intensidad de las ondas resultantes de la interferencia varía aleatoriamente, al menos en la dimensión espacial. Típicamente, se usa radiación monocromática y suficientemente coherente, tal como la emisión láser, para generar tales patrones de moteado.

En particular, la microestructura puede ser una microestructura integral, tal como una superficie de un objeto físico que muestra una rugosidad óptica suficiente, o puede comprender una pluralidad de partes separadas, por ejemplo, partículas microscópicas en una distribución aleatoria dentro de un cuerpo (que es al menos parcialmente transparente a la radiación) o en una superficie de un objeto físico.

Similar a los UCD, una ventaja de usar tales microestructuras de generación de moteado para las PUF es que pueden aplicarse a casi cualquier objeto físico, ya sea en su superficie o incluso incrustarse dentro del objeto, si este último es lo suficientemente transparente a la luz necesaria para generar el patrón moteado. Debido a que tales microestructuras típicamente tienen dimensiones características en el orden de las longitudes de onda de la luz, pueden hacerse muy pequeñas y, por lo tanto, también son elementos típicamente encubiertos que no pueden reconocerse fácilmente sin un equipo sofisticado. Esto nuevamente aumenta el nivel de seguridad alcanzable.

De acuerdo con una modalidad preferida adicional, la PUF comprende al menos uno de los siguientes: (i) una imagen en la que la información oculta se incrusta esteganográficamente; (ii) una imagen que se imprime con una tinta que contiene uno o más tipos de colorantes de conversión ascendente, UCD; (iii) un holograma que contiene información oculta codificada en fase o codificada en frecuencia. En particular, además de los elementos de seguridad encubiertos mencionadas anteriormente, que aumentan el nivel de seguridad que puede lograrse, la imagen respectivamente del holograma puede comprender o representar además un elemento visible, por ejemplo, un código de barras unidimensional o multidimensional, como un Código QR o código DATAMATRIX, para presentar más información. Por ejemplo, tal código a continuación puede superponerse a la imagen o al holograma que contiene el elemento encubierto o la imagen puede imprimirse con tinta que contiene una mezcla de UCD. Esto permite implementaciones de PUF muy eficientes en cuanto al espacio que comprenden aspectos de seguridad cubiertos y elementos de seguridad encubiertos u otra información, tal como la firma digital de la marca de seguridad compuesta o los códigos del producto, las identidades del fabricante, la información del sitio de producción, etc.

De acuerdo con una modalidad preferida adicional, la representación de la firma digital y/o el puntero se implementa mediante uno o más de los siguientes: (i) una cadena alfanumérica; (ii) una representación gráfica o de imagen; (iii) un código de barras unidimensional o multidimensional; (iv) un dispositivo, por ejemplo, un chip inalámbrico de corto alcance, tal como un chip RFID, que transmite una señal que lleva la representación de la firma digital o el puntero. En particular, esta modalidad puede combinarse con la modalidad inmediatamente anterior. Además, la firma digital y/o puntero pueden representarse por solo una parte de dicha cadena, representación gráfica de imagen, código de barras o señal, respectivamente, cada uno de los cuales puede representar además información adicional que puede o no estar relacionada con la seguridad.

De acuerdo con una modalidad preferida adicional, la marca de seguridad compuesta comprende dicho puntero y dicho puntero indica un enrutamiento a un servidor desde el que puede recuperarse la firma digital. En particular, esto permite una administración central de las firmas digitales de múltiples objetos físicos en un entorno de servidor. Además, esto permite un monitoreo y control centralizado del uso de las firmas digitales administradas que pueden usarse de muchas maneras, por ejemplo, para la detección temprana de intentos de fraude o la optimización de la cadena de suministro. Específicamente, puede usarse una infraestructura de centro de confianza para tal supervisión y control centralizados. Opcionalmente, el puntero también puede contener o señalar información con respecto a un tipo de producto, número de serie u otra información relacionada con el objeto físico que va a marcarse con una marca de seguridad compuesta.

De acuerdo con una modalidad preferida adicional, en donde la PUF comprende un UCD, dichos datos que representan una respuesta generada por la PUF en reacción a un desafío de un esquema de autenticación de desafío-

respuesta predeterminado para dicho UCD representa un código de barras espectral que tiene un intervalo continuo o cuantificado de valores espectrales permitidos para un subconjunto discreto seleccionado de longitudes de onda, y/o una vida útil característica de un efecto de luminiscencia que ocurre en la respuesta. Esto permite, en particular, determinar y escalar el número de bits u otras unidades de información que pueden codificarse mediante el uso del UCD de la PUF. Si, por ejemplo, en cada intervalo del espectro el valor espectral correspondiente se cuantifica en uno de los cuatro niveles espectrales, ese intervalo del espectro puede usarse para codificar dos bits de información representados por la PUF. Agregar además una cuantización de la vida útil característica del efecto de luminiscencia en ese intervalo espectral, puede usarse para agregar más bits de información. Una cuantización puede ser preferible sobre un intervalo continuo de valores espectrales permitidos, ya que puede aumentar la robustez contra las distorsiones de la respuesta generada por la PUF.

De acuerdo con una modalidad preferida adicional, en donde la PUF comprende un patrón físico no clonable o una estructura configurada para generar un patrón virtual en respuesta al desafío, dichos datos que representan una respuesta generada por la PUF en reacción a un desafío de un esquema de autenticación de respuesta-desafío predeterminado para dicho patrón físico no clonable o la estructura configurada para generar un patrón virtual representa al menos un aspecto o porción reconocida de dicho patrón físico o dicho patrón virtual, respectivamente. En particular, dicho aspecto reconocido podría relacionarse con una medida estadística aplicada al patrón físico o patrón virtual, tal como una distancia promedio entre nodos individuales del patrón, una varianza relacionada o desviación estándar, o cualquier otro momento estadístico. Alternativamente, de acuerdo con otra variante, dicho patrón puede escanearse, por ejemplo, en forma de matriz, y por lo tanto convertirse en una cadena de bits, por ejemplo, mediante el uso de un umbral de discriminación y que representa los puntos de matriz que muestran una intensidad de luz por encima del umbral en un "1" y todos los puntos de matriz que tienen una intensidad de luz por debajo del umbral como "0", o viceversa. De esta manera, los patrones pueden convertirse eficientemente en datos que representan una respuesta generada por la PUF en reacción al desafío correspondiente.

De acuerdo con una modalidad preferida adicional, la marca de seguridad compuesta comprende al menos un componente resultante de un proceso de fabricación aditiva y la PUF está contenida o forma parte de ese componente. En particular, el proceso de fabricación aditiva puede denominarse proceso de impresión 3D. Preferentemente, la PUF se proporciona ya en la materia prima, a partir de la cual se hace el componente mediante el uso del proceso de fabricación aditiva. De esta manera, la PUF puede introducirse en el componente sin necesidad de modificaciones en los datos de fabricación en función de los cuales se realiza el proceso de fabricación aditiva. Además, la extremadamente alta flexibilidad y complejidad proporcionadas por los métodos de fabricación aditiva permiten una variedad prácticamente infinita de PUF diferentes y su disposición en o dentro del objeto físico a marcar. Esto, nuevamente, puede usarse para aumentar aún más el nivel de seguridad que puede lograrse con la marca de seguridad compuesta.

Un segundo aspecto de la solución proporcionada en la presente descripción se dirige a un objeto físico, en particular un producto, que comprende una marca de seguridad compuesta de acuerdo con el primer aspecto de la solución, preferentemente de acuerdo con una cualquiera o más de sus modalidades o variantes descritas en la presente descripción.

Específicamente, de acuerdo con las modalidades preferidas, el objeto físico es un producto que comprende uno o más artículos para consumo o uso y un empaque del mismo, y la PUF de la marca de seguridad compuesta se dispone o se contiene dentro de al menos uno de los artículos para consumo o uso, mientras que la representación o el puntero de la firma digital se dispone en o dentro del empaque. Por lo tanto, en esta modalidad, la marca de seguridad compuesta se forma en dos sustratos diferentes. Esto puede ser ventajoso, especialmente en situaciones en las que no hay suficiente espacio en el propio producto para llevar tanto la PUF como la firma digital. En una variante, el producto es un producto farmacéutico que comprende, por ejemplo, una botella que contiene un producto farmacéutico líquido o un blíster que contiene tabletas como un artículo para el consumo y una caja de cartón que rodea la botella o blíster como un empaque. El PUF de la marca de seguridad compuesta es una etiqueta impresa colocada en la botella en donde la etiqueta se imprime con una tinta que contiene una mezcla secreta de diferentes UCD. La firma digital correspondiente a la PUF se imprime en el empaque en forma de código de barras bidimensional, por ejemplo, un código QR o un código DATAMATRIX.

De acuerdo con otras modalidades preferidas, el objeto físico comprende uno o más de los siguientes artículos para consumo (bienes consumibles) o uso: un compuesto o composición farmacéutica o cosmética; un dispositivo medico; un equipo de laboratorio; una pieza de repuesto o componente de un dispositivo o sistema; un pesticida o herbicida; un material de siembra; un revestimiento, tinta, pintura, colorante, pigmentos, barniz, sustancia impregnante, aditivo funcional; una materia prima para la fabricación aditiva de productos. En particular, todos estos elementos tienen en común que existe la necesidad de prevenir la falsificación para evitar el mal funcionamiento, las amenazas a la salud u otros riesgos.

Un tercer aspecto de la solución proporcionada en la presente descripción se dirige a un método para proporcionar un objeto físico, en particular un producto, con una marca de seguridad compuesta. El método comprende las siguientes etapas: (i) agregar una función física no clonable, PUF, a un objeto a marcar; (ii) aplicar un desafío de un esquema de autenticación de desafío-respuesta predeterminado a al menos uno de dichas PUF añadidas para activar una

respuesta de acuerdo con dicho esquema de autenticación en reacción a dicho desafío; detectar dicha respuesta; (iii) aplicar una función resumen criptográfica predeterminada a los datos que representan dicha respuesta para obtener un valor resumen; (iv) firmar dicho valor resumen con una firma digital; y (v) agregar una representación de la firma digital o un puntero que indique dónde puede accederse por la firma digital al objeto a marcar. En consecuencia, se proporciona una marca de seguridad compuesta al objeto físico, que comprende dicha PUF y su firma digital correspondiente o un puntero al mismo. Preferentemente, la PUF es una PUF como se describió anteriormente como un componente de una marca de seguridad compuesta de acuerdo con el primer aspecto de la presente solución de seguridad, respectivamente sus modalidades y variantes preferidas. La marca de seguridad compuesta producida por el método corresponde, por lo tanto, en particular a la marca de seguridad compuesta de acuerdo con el primer aspecto de la presente solución de seguridad. Preferentemente, el método comprende además generar un par de claves pública/privada de un sistema criptográfico asimétrico y usar la clave privada para crear dicha firma digital de dicho valor resumen y hacer que dicha clave pública correspondiente esté disponible, directa o indirectamente, para un destinatario del objeto que lleva la marca de seguridad compuesta.

Opcionalmente, la marca de seguridad compuesta puede comprender más de una PUF, particularmente como se describió anteriormente, y más de una firma digital derivada de una PUF o un puntero al mismo de acuerdo con las etapas (ii) a (v), como se describió anteriormente. En consecuencia, en una modalidad correspondiente de un método, las firmas digitales adicionales pueden derivarse ya sea mediante la aplicación de en la etapa (ii) diferentes desafíos correspondientes a diferentes esquemas de desafío-respuesta a la misma PUF, si es compatible con este último, o agregando en la etapa (i) dos o más PUF al objeto a marcar y realizar la etapa (ii) para cada uno de estas PUF. En ambas variantes, las etapas (iii) a (v) siguen para cada una de las respuestas, en donde para la etapa (v) el puntero puede apuntar al conjunto correspondiente de firmas digitales generadas. De esta manera, el nivel de seguridad alcanzable puede incrementarse aún más.

De acuerdo con una modalidad relacionada preferida adicional, la etapa de agregar una o más PUF a un objeto a marcar comprende uno o más de los siguientes: (a) agregar una o más PUF a un material de recubrimiento para obtener un material de recubrimiento mejorado con la PUF y aplicar, por ejemplo, mediante pulverización, recubrimiento, infiltración, impresión o pintura, el material de revestimiento mejorado con la PUF a un objeto físico a marcar; (b) agregar una o más PUF, preferentemente por medio de uno o más procesos químicos o de mezcla, a una materia prima o un material intermedio, tal como una tinta o un color, antes o durante la producción de un objeto físico a marcar; (c) agregar una o más PUF a una materia prima o agente de fusión de un proceso de fabricación aditiva, por ejemplo, proceso de impresión 3D, para producir un objeto físico a marcar o al menos una parte de tal objeto. En particular, se pueden agregar una o más PUF a la materia prima o al agente de fusión antes o durante el proceso de fabricación aditiva. Esto permite una fácil integración de una o más PUF en el propio objeto. Además, el nivel de seguridad puede incrementarse aún más, debido a que a medida que una o más PUF se convierten en un componente integral del objeto, una eliminación, en particular una eliminación no destructiva, de la una o más PUF del objeto, puede evitarse ser de manera efectiva.

Un cuarto aspecto de la solución proporcionada en la presente descripción se dirige a un aparato para proporcionar un objeto físico, en particular un producto, con una marca de seguridad compuesta, en donde el aparato se adapta para realizar el método de acuerdo con el tercer aspecto de la solución, preferentemente de acuerdo con cualquiera o más de sus modalidades o variantes descritas en la presente descripción. En consecuencia, la descripción y las ventajas del tercer aspecto de la solución se aplican mutatis mutandis al aparato de acuerdo con este cuarto aspecto.

Un quinto aspecto de la solución descrita en la presente descripción se dirige a un método de lectura con un dispositivo lector de una marca que comprende una función física no clonable, PUF. El método comprende las siguientes etapas: (i) una etapa de estimulación, en donde se crea un desafío físico de acuerdo con un esquema de autenticación de desafío-respuesta predeterminado correspondiente a la PUF y se aplica a una PUF; (ii) una etapa de detección, en donde se detecta una respuesta generada por la PUF de acuerdo con el esquema de autenticación de desafío-respuesta en reacción al desafío y se genera una señal digital que representa la respuesta; (iii) una etapa de procesamiento, en donde la señal digital se procesa para generar un valor resumen de la respuesta mediante la aplicación de una función resumen criptográfica predeterminada a la señal digital, y (iv) una etapa de salida, en donde se emiten los datos que representan el valor resumen generado como resultado de la primera lectura.

El método comprende además una etapa de adquisición, en donde se lee una marca de seguridad compuesta que comprende una PUF y una primera firma digital correspondiente o un puntero que indica una fuente donde puede accederse a tal primera firma digital, y dicha primera firma digital se adquiere de la marca o la fuente indicada por el puntero, respectivamente. Además, en la etapa de salida (i) una representación de la primera firma digital adquirida, y/o (ii) una salida coincidente que indica si, de acuerdo con al menos un criterio de coincidencia predeterminado, se emite un valor resumen proporcionado y firmado por la primera firma digital adquirida que coincide con el valor resumen generado a partir de la respuesta al desafío. De esta manera, el método proporciona una verificación de la autenticidad de la marca, respectivamente, del objeto físico que lleva la marca al permitir una comparación, por ejemplo, por el usuario, entre la primera firma digital comprendida en la marca, por un lado, y una representación correspondiente de la información contenida en la respuesta de la PUF de la marca por otro lado. Además, de acuerdo con la segunda alternativa (ii), tal comparación, es decir, que se corresponda, ya está disponible como parte del método en sí, lo que aumenta aún más la fiabilidad y la facilidad de uso de este método. En particular, la marca de

seguridad compuesta puede ser una marca como se describe en la presente descripción en relación con el primer aspecto de la presente solución de seguridad, por ejemplo, de acuerdo con una o más de sus modalidades preferidas y variantes descritas en la presente descripción.

La etapa de adquisición comprende además adquirir a partir de la marca de seguridad compuesta una segunda firma digital o un puntero que indica una fuente donde puede accederse a una segunda firma digital particular perteneciente a la marca. Además, la etapa de salida comprende además emitir una representación de la segunda firma digital adquirida como un segundo resultado de lectura. En particular, la marca de seguridad compuesta puede ser una marca como se describe en la presente descripción en relación con el primer aspecto de la presente solución de seguridad, por ejemplo, de acuerdo con las modalidades preferidas y variantes de la misma como se describe en la presente descripción, donde un objeto que se marca por la marca es un producto que comprende uno o más artículos de consumo o uso y un empaque de los mismos. La etapa de adquisición, por lo tanto, también permite que el dispositivo lector adquiera, además de la respuesta, información adicional comprendida en la marca, que puede ser particularmente información de la cadena de suministro. Por un lado, esto puede usarse tanto para (i) examinar la marca/objeto en vista de si ha sido falsificado o manipulado o no, y (ii) leer y enviar la información adicional, tal como la cadena de suministro u otra información logística. Además, sin embargo, la combinación de ambos usos (i) y (ii) puede usarse para aumentar aún más el aspecto de seguridad de la presente solución de seguridad, debido a que dicha información adicional, como la información de la cadena de suministro, puede usarse para identificar localizaciones o personas de manera retroactiva involucradas en la cadena de suministro, donde podría haber ocurrido un posible fraude, así como también posibles fechas o plazos relacionados. En consecuencia, un dispositivo lector adaptado para realizar el método de esta modalidad es un dispositivo de doble uso o incluso multiusos, que aumenta la facilidad de uso y reduce el número de dispositivos diferentes necesarios para leer la marca de seguridad compuesta completa.

El término "estimulación", como se usa en la presente descripción, se refiere a crear y aplicar a una PUF un desafío físico de acuerdo con un esquema de autenticación predeterminado de desafío-respuesta correspondiente a la PUF. Específicamente, una estimulación puede comprender la emisión de radiación electromagnética como un desafío que desencadena una respuesta de acuerdo con el esquema de autenticación de desafío-respuesta, cuando se aplica a una PUF que es sensible a esta radiación particular, por ejemplo, si la PUF es un UCD en el que un efecto anti-Stokes que genera la respuesta puede activarse por dicha radiación. En consecuencia, un "estimulador", como se usa en la presente descripción, es un componente del dispositivo lector que se adapta para crear tal estimulación y aplicarla a una PUF.

El término "detección de una respuesta generada por una PUF", como se usa en la presente descripción, se refiere a detectar físicamente una respuesta generada por una PUF en reacción a un desafío de acuerdo con un esquema de autenticación de desafío-respuesta correspondiente y generar una señal digital que representa la respuesta, por ejemplo, por los datos respectivos que se transportan por la señal digital. En consecuencia, un "detector PUF", como se usa en la presente descripción, es un componente del dispositivo lector que se adapta para realizar la etapa de detección. En particular, el detector PUF puede comprender un receptor para la radiación electromagnética emitida por la PUF en respuesta al desafío que le aplica un estimulador.

Para aplicar la función resumen criptográfica predeterminada a la señal digital, la función resumen puede actuar particularmente sobre la señal digital completa, por ejemplo, una representación de datos de la señal digital completa, o solo en una parte distintiva de la misma, tal como por ejemplo (i) una porción de carga útil (o un subconjunto distintivo de la misma) de una señal digital que se representa de acuerdo con un protocolo de comunicación que define una porción de sobrecarga y una porción de carga útil de la señal, o (i) una porción de dicha señal que cae en un marco de tiempo específico, por ejemplo, dentro de un período de tiempo definido después del inicio de la detección seguido de la aplicación del desafío a una PUF.

En consecuencia, el método de lectura de acuerdo con este aspecto de la solución puede usarse ventajosamente para "leer" las marcas que comprenden una PUF correspondiente y proporcionar el resultado de "lectura" como datos de salida que pueden usarse para verificar si la marca o el objeto físico que lleva la marca ha sido falsificado o manipulado. En particular, el método puede usarse para "leer" una marca de seguridad compuesta de acuerdo con el primer aspecto de la solución, por ejemplo, de acuerdo con una o más de sus modalidades o variantes descritas en la presente descripción. Por lo tanto, el método de lectura puede formar parte de una solución general que proporciona un nivel adicional de seguridad y, por lo tanto, una forma mejorada de proteger un objeto físico contra la falsificación y la manipulación.

De acuerdo con una modalidad preferida, la señal digital se genera en la etapa de procesamiento de tal manera que representa al menos una propiedad distintiva específica de PUF de la respuesta que es, al menos sustancialmente, invariable bajo variaciones de las condiciones ambientales en las que se detecta la respuesta. A manera de ejemplo, tales condiciones ambientales variables podrían ser condiciones de luz, temperatura, presión de aire u otros parámetros o propiedades del entorno al que la PUF típicamente se expone durante su detección por el dispositivo lector. Una ventaja de esta modalidad es una mayor robustez del método de lectura y del dispositivo lector utilizado por lo tanto con respecto a su capacidad de leer correctamente las marcas que comprenden una PUF correspondiente.

Esto permite una distinción aún más confiable entre las marcas falsificadas o manipuladas y los objetos físicos que llevan tales marcas, por un lado, y por el otro lado, las marcas/objetos que no se han falsificados o manipulados.

De acuerdo con una modalidad preferida adicional, detectar la respuesta en la etapa de detección comprende detectar al menos una propiedad de radiación electromagnética emitida por la PUF como respuesta en reacción al desafío y generar la señal digital de manera que represente esta respuesta. Esto permite, en particular, una lectura inalámbrica sin contacto de una marca que contiene la PUF. Tal método de lectura y un dispositivo de lectura respectivo pueden usarse particularmente de manera ventajosa para detectar respuestas de PUF que son muy pequeñas o están incrustadas debajo de una superficie de una marca/objeto o donde la marca o el objeto físico que lleva la marca es muy sensible a impactos mecánicos o químicos que típicamente acompañarían a un método de lectura basado en el contacto.

Específicamente, de acuerdo con una modalidad adicional y relacionada, detectar la respuesta en la etapa de detección comprende detectar una vida útil característica de un efecto de luminiscencia que ocurre en la respuesta como una propiedad de la radiación electromagnética emitida por la PUF. En consecuencia, la etapa de detección puede comprender particularmente detectar la radiación luminiscente en diferentes puntos posteriores en el tiempo después de una estimulación de una PUF correspondiente para derivar de la radiación detectada una medida para una vida útil característica, tal como un medio tiempo u otras medidas de un tiempo de descomposición, por ejemplo. Dado que tales vidas útiles características de los efectos de luminiscencia son principalmente específicos del material, son invariables bajo una gran variedad de parámetros ambientales diferentes y, por lo tanto, son particularmente adecuados para caracterizar la respuesta de una PUF correspondiente que muestra tal efecto como una propiedad distintiva.

De acuerdo con otra modalidad preferida relacionada, detectar la respuesta en la etapa de detección comprende detectar un espectro de la radiación emitida como una propiedad de la radiación electromagnética emitida por la PUF. Además, el procesamiento de la señal digital en la etapa de procesamiento comprende determinar a partir de la señal digital uno o más de los siguientes: (i) la posición (es decir, longitud de onda o frecuencia o un parámetro relacionado) de uno o más rasgos característicos (por ejemplo, picos, huecos o mínimos dentro del espectro); (ii) una o más medidas estadísticas que caracterizan el espectro (por ejemplo, media, mediana, varianza, desviación estándar u otros momentos o medidas estadísticas); (iii) uno o más valores espectrales cuantificados del espectro (por ejemplo, de las intensidades detectadas dentro de un espectro de intensidad de la radiación); (iv) un código de barras espectral que representa un intervalo continuo o cuantificado de valores espectrales permitidos que ocurren en el espectro, por ejemplo, para un subconjunto discreto seleccionado de longitudes de onda. Además, cada una de estas variantes puede proporcionar una mayor robustez del método frente a las condiciones ambientales variables en las que se detecta la respuesta.

De acuerdo con otras modalidades preferidas, el segundo resultado de lectura comprende una o más de la siguiente información: (i) información de localización perteneciente a una localización donde el dispositivo lector adquirió la segunda firma digital; (ii) información de autenticación de un usuario del dispositivo lector; (iii) información de hora y/o fecha que indica el momento en el que el dispositivo lector adquirió la segunda firma digital; (iv) una identificación del producto, número de serie y/o número de lote de un objeto que va a marcarse por la marca; (v) una fecha de vencimiento de un objeto que va a marcarse por la marca.

De acuerdo con una modalidad preferida adicional, la etapa de salida comprende además emitir al menos una parte, preferentemente la totalidad, de un resultado de lectura en forma de un código de barras unidimensional o multidimensional. Esto permite el uso de escáneres de códigos de barras fácilmente disponibles para el procesamiento posterior de la salida proporcionada por la etapa de salida, que puede ser particularmente ventajoso, donde el dispositivo lector se integra o interactúa con una línea de producción automatizada u otra línea de procesamiento, donde sus salidas necesitan ser procesadas por algoritmos procesados por la línea en lugar de por un usuario humano.

De acuerdo con una modalidad preferida adicional, el método comprende además una etapa de autenticación, en donde un usuario se autentica antes de permitirle operar adicionalmente el dispositivo lector en caso de una autenticación exitosa. Esto puede usarse ventajosamente para aumentar aún más la seguridad de la solución al evitar que usuarios no autorizados interactúen con éxito con el dispositivo lector y, por lo tanto, se involucren en la cadena de seguridad proporcionada por la presente solución de seguridad. Además, esto puede usarse para adquirir información sobre la identidad de usuario u otra información relacionada con el usuario, que puede usarse para aumentar la transparencia del flujo de objetos físicos que van a marcarse por la marca, particularmente productos, a lo largo de una cadena de suministro. En caso de problemas de seguridad, esta información puede usarse luego para rastrear posibles amenazas a la seguridad proporcionada por la solución general e identificar localizaciones o personas que podrían estar relacionadas con tales amenazas.

De acuerdo con una modalidad preferida adicional, el método comprende además una etapa de comunicación, en donde un resultado de lectura se comunica por un enlace de comunicación a un lado contrario. En particular, la etapa de comunicación podría adaptarse para enviar y recibir datos a través de un enlace de comunicación por cable, inalámbrico u óptico, tal como por ejemplo y sin limitación un enlace de comunicación basado en LAN inalámbrica, Bluetooth, red celular o una línea telefónica clásica. Tal enlace de comunicación puede usarse para una variedad de

propósitos diferentes, que incluye el envío de información adquirida, por ejemplo, la salida proporcionada en la etapa de salida, a un lado contrario, que podría ser, por ejemplo, una instancia de seguridad central, tal como un centro de confianza que comprende un servidor de seguridad central, que podría formar un componente de la solución de seguridad actual.

Además, de acuerdo con otra modalidad, la etapa de comunicación comprende además capturar y enviar la información relacionada con la seguridad a un lado contrario predeterminado a través del enlace de comunicación. Dicho lado contrario podría ser, por ejemplo, el centro de confianza mencionado en la modalidad inmediatamente anterior. En particular, tal envío de información relacionada con la seguridad puede ocurrir de manera aleatoria, o puede activarse específicamente de acuerdo con un esquema de activación predeterminado o de manera remota, por ejemplo, por el lado contrario. Esto permite un monitoreo remoto del estado de seguridad del dispositivo lector y/o de los eventos relacionados con la seguridad en los que está involucrado el dispositivo lector. Tal evento relacionado con la seguridad podría ser, por ejemplo, la detección de una marca/objeto que se ha falsificado o manipulado, de acuerdo con la salida generada en la etapa de salida u otra información relacionada con la seguridad proporcionada por el dispositivo lector.

Específicamente, de acuerdo con las modalidades preferidas relacionadas, la información relacionada con la seguridad comprende uno o más de los siguientes: (i) información de localización que caracteriza una localización actual o pasada del dispositivo lector; (ii) datos de usuario que caracterizan o identifican a un usuario del dispositivo lector; (iii) datos de red que caracterizan el enlace de comunicación; (iv) información que caracteriza un intento o acto real detectado por al menos un sensor del dispositivo lector o una reacción correspondiente del dispositivo lector (por ejemplo, como se describió anteriormente); (v) información de autenticación generada por un dispositivo de autenticación proporcionado en el dispositivo lector, preferentemente por el dispositivo de autenticación descrito anteriormente.

De acuerdo con una modalidad adicional, el método comprende además una etapa de monitorización de información, en donde se detecta un evento de seguridad en la información contenida en una señal recibida desde el lado contrario a través del enlace de comunicación. Esta etapa permite, en particular, una transición del dispositivo lector a un modo seguro o incluso su desactivación, en caso de que un lado contrario autorizado, por ejemplo, un centro de seguridad central, envíe información que contenga dicho evento de seguridad al dispositivo lector, para evitar cualquier impacto negativo que el dispositivo lector pueda tener en el sistema de seguridad general. Tal impacto negativo podría resultar, por ejemplo, si cualquier acto comprometedor tal como una intrusión no autorizada o una modificación de microprogramas/software en el dispositivo lector o un uso por parte de una persona no autorizada o en una localización no autorizada se ha comunicado o detectado por el lado contrario.

De acuerdo con una modalidad preferida adicional, el método comprende además una etapa de monitorización de acceso, en donde uno o más de los siguientes se detectan mediante uno o más sensores como un evento de seguridad: (i) un intento o acto real de intrusión física en el dispositivo lector, tal como una abertura de su alojamiento; (ii) un intento o acto real de acceder local o remotamente a una funcionalidad de control interno del dispositivo lector, por ejemplo, sus microprogramas, sistema operativo o una aplicación, en donde tal acceso no está disponible para un usuario del dispositivo en el curso de su operación normal. Específicamente, tal intento de acceso podría estar dirigido a asumir el control de la funcionalidad del dispositivo lector o modificar el mismo. En consecuencia, esta modalidad puede usarse ventajosamente para aumentar aún más el aspecto de seguridad de la presente solución de seguridad, y particularmente para proteger tanto el dispositivo lector como la solución completa presentada en la presente descripción contra intrusiones y manipulaciones no autorizadas.

De acuerdo con una modalidad preferida relacionada adicional, el método comprende además una etapa de defensa de seguridad, en donde una o más de las siguientes medidas de seguridad se realizan en reacción a la detección de un evento de seguridad: (i) bloquear el dispositivo lector para limitar o prevenir su uso posterior; (ii) autodestruir al menos una parte funcional del dispositivo lector o destruir los datos almacenados en el mismo para evitar su uso o acceso por parte de un usuario; (iii) enviar un mensaje de error. En particular, las medidas de seguridad pueden considerarse medidas específicas para convertir el dispositivo lector en un modo seguro o para desactivarlo, como se describió anteriormente.

De acuerdo con una modalidad preferida adicional, la etapa de salida comprende firmar digitalmente datos que contienen el valor resumen generado y emitir la firma digital resultante como el primer resultado de lectura. De esta manera, el método puede usarse particularmente para generar inicialmente una firma digital de una respuesta generada por una PUF en reacción a un desafío de un esquema de autenticación predeterminado desafío-respuesta, por ejemplo, durante un proceso de fabricación o puesta en servicio de productos que van a protegerse por una marca de seguridad compuesta, como se describe en la presente descripción. En particular, la firma digital generada puede incorporarse además de la PUF en dicha marca de seguridad compuesta. Preferentemente, el método, por ejemplo, la etapa de salida, comprende además generar un par de claves pública/privada de un sistema criptográfico asimétrico y usar la clave privada para crear dicha firma digital de dicho valor resumen y hacer que dicha clave pública correspondiente esté disponible, directa o indirectamente, a un destinatario del objeto que lleva la marca de seguridad compuesta.

De acuerdo con una modalidad preferida adicional, el método comprende además una etapa de almacenamiento, en donde un resultado de lectura que se emite en la etapa de salida se almacena en un bloque de una cadena de bloques. Esto permite un almacenamiento seguro y confiable de los resultados de lectura con una integridad de datos muy alta, de manera que es esencialmente imposible manipular o borrar o de cualquier otra manera reducir o perder tales datos, por ejemplo, debido a la eliminación involuntaria o deliberada o debido a la corrupción de datos. Por lo tanto, el historial completo de lectura permanece disponible. Además, puede accederse a la información almacenada donde sea que esté disponible el acceso a la cadena de bloques. Esto permite un almacenamiento y acceso seguro y distribuido a los resultados de lectura almacenados, por ejemplo, para fines de verificación de integridad, tal como verificar si un proveedor de un producto que va a marcarse con una marca de seguridad compuesta, como se describe en la presente descripción, era de hecho el emisor del producto, o no. En base a esta modalidad, el mundo físico, al que pertenecen los objetos marcados y las propias marcas, puede conectarse al poder de la tecnología de cadena de bloques. Por lo tanto, puede lograrse un alto grado de capacidad de seguimiento del origen y la cadena de suministro de objetos físicos, tales como productos.

De acuerdo con una modalidad preferida relacionada adicional, la etapa de almacenamiento comprende: (i) almacenar un primer resultado de lectura que comprende los datos que representan el valor resumen generado en la etapa de procesamiento en un bloque de una primera cadena de bloques; y (ii) almacenar el segundo resultado de lectura obtenido en la etapa de adquisición (como se describió anteriormente), en un bloque de una segunda cadena de bloques que se separa de la primera cadena de bloques. Esto permite almacenar y, por lo tanto, guardar los resultados de la primera y segunda lectura, es decir, los que se derivan de la lectura de la PUF y los que se leen de la segunda firma digital, en una cadena de bloques, lo que proporciona por lo tanto las ventajas descritas en relación con la modalidad inmediatamente anterior. El uso de cadenas de bloques diferentes para los dos resultados de lectura diferentes proporciona además la ventaja de admitir fácilmente una combinación de una (segunda) cadena de suministro existente para los resultados de la segunda lectura con una primera cadena de suministro adicional, para los resultados de la primera lectura relacionados con las respuestas de las PUF. En consecuencia, pueden habilitarse fácilmente diferentes derechos de acceso y la gestión de las cadenas de bloques puede estar en manos de diferentes autoridades. En particular, esta modalidad puede usarse para verificar si (i) el proveedor de un producto fue de hecho su emisor, y (ii) si la cadena de suministro fue como se esperaba o no.

De acuerdo con una modalidad preferida relacionada adicional, la etapa de almacenamiento comprende además: (i) cuando se almacena el primer resultado de lectura en un bloque de la primera cadena de bloques, que incluye un puntero de cadena de bloques cruzada, que asigna de manera lógica el bloque de la primera cadena de bloques a un bloque correspondiente de la segunda cadena de bloques en el bloque de la primera cadena de bloques; y (ii) cuando se almacena el resultado de la segunda lectura en un bloque de la segunda cadena de bloques, que incluye un puntero de cadena de bloques cruzada, que asigna de manera lógica el bloque de la segunda cadena de bloques a un bloque correspondiente de la primera cadena de bloques en el bloque de la segunda cadena de bloques. De esta manera, las dos cadenas de bloques pueden interconectarse mediante punteros de cadena de bloques cruzados que pueden usarse para aumentar aún más el nivel de seguridad alcanzable de la presente solución de seguridad. En particular, esto puede usarse para rastrear intentos de manipulación o falsificación de objetos marcados en diferentes puntos a lo largo de una cadena de suministro. Por ejemplo, esta modalidad permite rastrear una localización y/o un punto en el momento de tal intento o, en el caso de una autenticación obligatoria en el dispositivo lector, una identificación de un usuario que se involucra en tal intento.

Un sexto aspecto de la presente solución de seguridad se dirige a un dispositivo lector para leer una marca que comprende una función física no clonable, PUF, en donde el dispositivo lector se adapta para realizar el método del quinto aspecto de la presente solución de seguridad, preferentemente, de acuerdo con cualquiera o más de sus modalidades y variantes descritas en la presente descripción. Por lo tanto, lo que se describe en la presente descripción sobre el quinto aspecto de la presente solución de seguridad se aplica de manera similar al dispositivo lector de acuerdo con este sexto aspecto.

Específicamente, el dispositivo lector puede comprender como unidades funcionales (i) un estimulador que se configura para realizar la etapa de estimulación; (ii) un detector PUF que se configura para realizar la etapa de detección; (iii) un dispositivo de procesamiento configurado para realizar la etapa de procesamiento; y (iv) un generador de salida que se configura para realizar la etapa de salida.

De acuerdo con las modalidades preferidas, el dispositivo lector puede comprender además uno o más de los siguientes: (v) un dispositivo de adquisición configurado para realizar dicha etapa de adquisición; (vi) un dispositivo de autenticación configurado para realizar dicha etapa de autenticación; (vii) un dispositivo de comunicación configurado para realizar dicha etapa de comunicación; (viii) un dispositivo de monitoreo configurado para realizar dicha etapa de monitoreo de información; (ix) un dispositivo de seguridad que comprende al menos un sensor y se configura para realizar dicha etapa de monitoreo de acceso; (x) una disposición de defensa de seguridad configurada para realizar dicha etapa de defensa de seguridad; (xi) un dispositivo de almacenamiento de la cadena de bloques configurado para realizar dicha etapa de almacenamiento. Preferentemente, dos o más componentes (i) a (xi) pueden combinarse o integrarse en un componente multifuncional del dispositivo lector. Por ejemplo, todos los componentes que involucran un procesamiento de datos pueden combinarse o implementarse como una unidad integral de procesamiento multifuncional.

De acuerdo con las modalidades preferidas adicionales, el dispositivo lector se integra o forma de cualquier otra forma un componente de uno o más de los siguientes: un dispositivo portátil, por ejemplo, un producto o dispositivo de escaneo de código de barras; un equipo de producción, control de calidad o puesta en servicio; una línea de producción o control de calidad o puesta en servicio; un objeto volador, por ejemplo, un dron; un robot, por ejemplo, un robot agrícola; una máquina agrícola. Esto permite una integración de la funcionalidad del dispositivo lector en un sistema que tiene una funcionalidad adicional o más amplia, particularmente de manera automatizada o semiautomatizada. Por ejemplo, en el caso de una línea de control de calidad de producción o de puesta en servicio, el dispositivo lector puede integrarse en la línea de tal manera que lea automáticamente las marcas, en particular las marcas de seguridad compuestas, en los productos que se ejecutan a lo largo de la línea para realizar una captura inicial de los datos relacionados. Los datos capturados pueden almacenarse luego en una base de datos relacionada o compararse con los datos ya almacenados con el fin de verificar que la línea de producción o puesta en servicio produce, respectivamente, las comisiones del conjunto de productos previsto. De manera similar, en uno o más nodos de una cadena de suministro, tales como los centros logísticos, tales dispositivos lectores pueden integrarse en línea en los sistemas de identificación y transporte, por ejemplo, transportadores, para verificar automática o semiautomática (por ejemplo, en el caso de un dispositivo portátil) y verificar la autenticidad de los productos en base a sus marcas, antes de enviarlos al siguiente nodo de la cadena de suministro. Lo mismo se aplica a un nodo final, es decir, a un destinatario y/o usuario final de los productos.

Un séptimo aspecto de la presente solución de seguridad se dirige a un programa de ordenador que comprende instrucciones, que cuando se ejecuta en uno o más procesadores de un dispositivo lector de acuerdo con el sexto aspecto hace que el dispositivo lector realice el método de acuerdo con el quinto aspecto de la presente solución de seguridad.

El programa de ordenador puede implementarse particularmente en forma de un soporte de datos en el que se almacenan uno o más programas para realizar el método. Esto puede ser ventajoso, si el producto del programa de ordenador está destinado a comercializarse como un producto individual en un producto individual independiente de la plataforma del procesador en la que se ejecutarán uno o más programas. En otra implementación, el producto de programa de ordenador se proporciona como un archivo en una unidad de procesamiento de datos, particularmente en un servidor, y puede descargarse a través de una conexión de datos, por ejemplo, Internet o una conexión de datos dedicada, tal como una red de área local o propietaria.

Breve descripción de los dibujos

Otras ventajas, características y aplicaciones de la presente solución de seguridad se proporcionan en la siguiente descripción detallada y las figuras adjuntas, en donde:

La Figura 1 ilustra esquemáticamente varias marcas de seguridad compuestas de acuerdo con las modalidades preferidas de la presente solución de seguridad;

La Figura 2 ilustra esquemáticamente un objeto físico multiparte de acuerdo con una modalidad preferida de la presente solución de seguridad, el objeto que comprende un bien de consumo embotellado y un empaque relacionado, en donde el objeto se marca con una marca de seguridad compuesta de acuerdo con la presente solución de seguridad que comprende una PUF implementada en la botella y una firma digital correspondiente impresa en el empaque;

La Figura 3 ilustra esquemáticamente otro objeto físico multiparte de acuerdo con una modalidad preferida de la presente solución de seguridad, el objeto que comprende como bienes consumibles un conjunto de tabletas farmacéuticas dispuestas en blísteres y un empaque relacionado para los blísteres, en donde cada una de las tabletas contiene una PUF basada en UCD y el empaque comprende una impresión en el mismo que representa un conjunto de firmas digitales correspondientes a las PUF;

La Figura 4 ilustra varias maneras diferentes de derivar datos que representan una respuesta generada por una PUF basada en UCD en reacción a un desafío correspondiente de un esquema de autenticación de desafío-respuesta predeterminado, de acuerdo con las modalidades preferidas de la presente solución de seguridad;

La Figura 5 muestra un diagrama de flujo que ilustra un método básico para marcar un objeto físico con una marca de seguridad compuesta, de acuerdo con las modalidades preferidas de la presente solución de seguridad;

La Figura 6 ilustra esquemáticamente un aparato para realizar el método de la Figura 5, de acuerdo con una modalidad preferida de la presente solución de seguridad.

Las Figuras 7A y B muestran un diagrama de flujo que ilustra una primera modalidad de un método de lectura con un dispositivo lector de una marca que comprende una PUF, tal como una marca de seguridad compuesta de la Figura 1, de acuerdo con una modalidad preferida de la presente solución de seguridad;

Las Figuras 8A y 8B muestran un diagrama de flujo que ilustra una segunda modalidad de un método de lectura con un dispositivo lector de una marca que comprende una PUF, tal como una marca de seguridad compuesta de la Figura 1, de acuerdo con otra modalidad preferida de la presente solución de seguridad;

La Figura 9 ilustra esquemáticamente un dispositivo lector de acuerdo con una modalidad preferida de la presente solución de seguridad;

La Figura 10 es una descripción esquemática de una modalidad preferida de la presente solución de seguridad; y

La Figura 11 muestra esquemáticamente una evolución de un conjunto de dos cadenas de bloques interconectadas a lo largo de una cadena de suministro para un producto que va a marcarse con una marca de seguridad compuesta, de acuerdo con las modalidades preferidas de la presente solución de seguridad.

En las figuras, se usan signos de referencia idénticos para los mismos elementos o elementos mutuamente correspondientes de la solución descrita en la presente descripción.

Descripción detallada

A. Marca de seguridad compuesta

La Figura 1 muestra seis variaciones diferentes (a) - (f) de una marca de seguridad compuesta 1 para un objeto físico, especialmente un producto, de acuerdo con las modalidades preferidas de la presente solución de seguridad. Cada una de estas marcas de seguridad compuestas 1 comprende una PUF 2 y una representación de una firma digital 3 que firma digitalmente un valor resumen derivado de los datos que representan una respuesta recibida de la PUF en reacción a un desafío correspondiente a un esquema de autenticación predeterminado desafío-respuesta. En consecuencia, la PUF 2 y la firma digital 3 se relacionan y se corresponden entre sí. La firma digital 3 se creó con la ayuda de una clave privada de un par de clave pública/clave privada de un sistema criptográfico asimétrico. Puede leerse con la ayuda de la clave pública correspondiente del sistema criptográfico asimétrico para verificar la autenticidad de la firma digital y, por lo tanto, el objeto físico marcado con esta.

De acuerdo con su naturaleza, la PUF 2 puede considerarse única (por lo tanto, "no clonable") como lo es su respuesta al desafío. En consecuencia, debido a la naturaleza unidireccional resistente a colisiones de la función resumen criptográfica, también el valor resumen derivado de la respuesta es único y, por lo tanto, pertenece solo a esta PUF 2 exacta, ya que es prácticamente imposible tener valores resumen idénticos mediante la aplicación de dicha función resumen a las respuestas de diferentes PUF, y aún más, si las PUF también tienen que estar presentes al mismo tiempo en una misma localización (coincidencia espacial y de tiempo).

Por lo tanto, tal marca de seguridad compuesta 1 es extremadamente difícil, si no imposible, de falsificar y, por lo tanto, puede usarse para proteger objetos físicos, tales como productos y otros bienes, en particular contra la falsificación y la manipulación.

La Figura 1 (a) muestra una primera variante de dicha marca de seguridad compuesta 1, en donde la PUF 2 se implementa como un área en la superficie de la marca de seguridad compuesta 1 que contiene una mezcla de UCD ya en su material o que tiene una o más capas adicionales que contienen un material de recubrimiento o tinta que contiene una mezcla de UCD. La firma digital 3 se representa por un código de barras bidimensional, tal como un código QR.

La Figura 1 (b) muestra otra variante, en donde la PUF 2 se implementa como una microestructura en forma de una distribución aleatoria de un gran número (por ejemplo, 10^6 o más) de partículas microscópicas que reflejan la luz, que, cuando se ilumina con luz láser coherente de una longitud de onda específica como desafío, crea un patrón moteado característico por medio de interferencia. El patrón puede detectarse con un sensor óptico, tal como una cámara digital adecuada, para generar datos que representen la respuesta, por ejemplo, como un archivo de imagen digital.

La Figura 1 (c) muestra aún otra variante, en donde la PUF 2 se implementa mediante un holograma que contiene información oculta codificada en fase o codificada en frecuencia. Cuando se ilumina con una luz láser coherente de una longitud de onda específica como desafío, el holograma genera una imagen holográfica virtual de la que puede extraerse la información oculta como respuesta de acuerdo con un esquema de autenticación de desafío-respuesta con la ayuda de uno o más sensores ópticos y algoritmos de procesamiento de imágenes adecuados. En esta variante, la firma digital 3 se implementa de manera ilustrativa por medio de un chip RFID, que se configura para emitir una señal que representa la firma digital 3, cuando se activa.

La Figura 1 (d) muestra aún otra variante, en donde la PUF 2 se implementa por medio de una imagen que se imprime mediante el uso de tinta que contiene una mezcla de diferentes tipos de UCD. Opcionalmente, además, la información oculta puede incrustarse esteganográficamente en la imagen. Por ejemplo, podría haber variaciones de color específicas mínimas creadas artificialmente, que son invisibles para el ojo humano, pero que se utilizan para codificar tal información y pueden detectarse mediante el uso de sensores ópticos adecuados en combinación con los

algoritmos de análisis respectivos. En esta variante, la firma digital 3 se implementa de manera ilustrativa como una cadena numérica.

La Figura 1 (e) muestra aún otra variante, en donde tanto la PUF 2 como la firma digital 3 se implementan como una combinación integrada, por medio de una imagen de código de barras que se imprime mediante el uso de tinta que contiene una mezcla de diferentes tipos de UCD. El código de barras codifica la firma digital 3, mientras que el material de tinta representa la PUF 2. Esto permite una implementación extremadamente compacta de la marca de seguridad compuesta 1.

La Figura 1 (f) muestra aún otra variante, en donde, al igual que en la Figura 1 (e), tanto la PUF 2 como la firma digital 3 se implementan como una combinación integrada, por medio de una imagen de código de barras que se imprime mediante el uso de tinta que contiene una mezcla de diferentes tipos de UCD. Sin embargo, a diferencia de la Figura 1 (e), el código de barras no codifica la firma digital 3 en sí. En cambio, codifica un puntero 4 que indica dónde puede accederse a la firma digital real 3 desde un lugar que no es parte de la marca de seguridad compuesta 1 en sí. Preferentemente, este puntero 4 es una representación de una dirección de Internet, por ejemplo, de un servidor, desde donde se puede descargar o acceder a la firma digital 3. Nuevamente, esto permite una implementación extremadamente compleja de la marca de seguridad compuesta 1, y además permite una gestión central, almacenamiento y provisión de las respectivas firmas digitales 3 de múltiples marcas de seguridad compuestas 1, por ejemplo, las pertenecientes a una serie particular de productos de un fabricante determinado.

La Figura 2 muestra un objeto físico multiparte de acuerdo con una modalidad preferida de la presente solución de seguridad. El objeto comprende un bien consumible 6, tal como un producto farmacéutico líquido, que está contenido en un recipiente, especialmente una botella 5 y un empaque relacionado 7. Una marca de seguridad compuesta 1 se divide en dos partes en diferentes sustratos. Como una primera parte de la marca de seguridad compuesta 1, se coloca una PUF 2 en la botella 5. El tipo de PUF 2 puede ser cualquier tipo de PUF como se describe en la presente descripción, en particular como se describe en relación con la Figura 1 anterior. La segunda parte de la marca de seguridad compuesta 1 comprende un código de barras que representa la firma digital 3 correspondiente a la PUF 2 y que está impresa en el empaque 7. Como la PUF 2 y la firma digital 3 se interconectan como se describió anteriormente, cualquier falsificación por medio de la sustitución del empaque 7 o la botella 5 puede detectarse por medio de la identificación de una discordancia entre el valor resumen que puede derivarse de la respuesta recibida en reacción a un desafío relacionado de acuerdo con el esquema de autenticación de desafío-respuesta predeterminado y el valor resumen que se contiene y protege criptográficamente por la firma digital 3.

La Figura 3 muestra otro objeto físico multiparte de acuerdo con una modalidad preferida adicional de la presente solución de seguridad. Aquí, los productos a proteger son tabletas farmacéuticas (píldoras) 8 que están contenidas en un conjunto de blísteres 9. Cada una de las tabletas contiene una mezcla de UCD de un tipo que no causa efectos perjudiciales en un mamífero, especialmente un cuerpo humano, cuando se ingiere. La mezcla de UCD puede ser la misma para todas las tabletas o, como alternativa, incluso individual por tableta o un subconjunto de las mismas. Como en la Figura 2, un empaque 7 forma una segunda parte del objeto físico a proteger y lleva la(s) firma(s) digital(es) 3 correspondiente(s) a una o más PUF 2 contenidas en las tabletas 8. De esta manera, cuando la PUF 2 es una parte inseparable integral del bien consumible en sí, el nivel de seguridad se puede mejorar aún más en comparación con una situación de acuerdo con la Figura 2, donde solo el contenedor 5 para el bien consumible lleva la PUF 2.

La Figura 4 ilustra varias formas diferentes (a) - (c) de derivar datos que representan una respuesta generada por una PUF 2 basada en UCD en reacción a un desafío correspondiente de un esquema de autenticación de desafío-respuesta predeterminado. En particular, el desafío puede comprender la irradiación de la PUF 2 por radiación electromagnética que tiene propiedades particulares, por ejemplo, un cierto intervalo o espectro de longitud de onda, tales como componentes espectrales particulares en la parte infrarroja o UV del espectro electromagnético.

La Figura 4 (a) muestra una primera variante, en donde un espectro $I(\lambda)$ de una intensidad I de la luz emitida por la PUF 2 en respuesta al desafío se detecta como una función de la longitud de onda λ. En particular, las longitudes de onda seleccionadas λ_1, λ_2, λ_3, ..., a la que ocurren los picos del espectro $I(\lambda)$, pueden identificarse por medio del análisis de espectro o incluso simplemente mediante el uso de umbrales de intensidad adecuados. A manera de ejemplo, y sin limitación, esta información puede representarse luego por una cadena de datos F, que en una forma simple solo representa los valores de las respectivas longitudes de onda λ_1, λ_2, λ_3, etc. En una versión mejorada, también se incluyen en F los valores de intensidad correspondientes I_1, I_2 e I_3, etc. para estas longitudes de onda, como se indica en el lado derecho de la Figura 4 (a). Alternativamente, o además, otras características del espectro $I(\lambda)$ pueden identificarse y representarse por F. La cadena de datos F puede ser en particular un número binario que consiste en una serie de bits. Además, la cadena de datos F puede interpretarse como un "código de barras espectral" que representa características genuinas del espectro $I(\lambda)$, en particular en su representación gráfica como se muestra en el lado derecho de la Figura 4(a). En esta variante, los valores de intensidad I son valores analógicos, es decir, pueden tener cualquier valor que pueda representarse por la cadena de datos F.

La Figura 4 (b) muestra otra variante, que es similar a la de la Figura 4 (a) con la excepción de que los valores de intensidad I están cuantificados y pueden tomar solo uno de los tres valores posibles, que en este ejemplo son valores normalizados "0", "1/2" y "1" de una unidad de intensidad adecuada. Esta variante puede usarse ventajosamente para

crear una forma particularmente robusta de representación del espectro por la cadena de datos F, debido a que la cuantificación de la cadena de datos resultante F es menos sensible a las variaciones en los valores detectados I causadas por imperfecciones de la propia medición. Las cadenas de datos F de las variantes mostradas en las Figuras 4(a) y 4(b) cada una forman implementaciones de un código de barras espectral.

La Figura 4 (c) muestra aún otra variante, en donde la intensidad I(t, λ) de luz luminiscente, preferentemente luz fluorescente, emitida por una PUF como respuesta al desafío se detecta en función del tiempo t y la longitud de onda λ. Se determina una vida útil característica T = T (λ), que puede corresponder, por ejemplo, al período de vida media $T_{1/2}$ de la luz luminiscente de la longitud de onda λ. Una cadena de datos F correspondiente puede formarse nuevamente como una representación de la respuesta. En particular, la cadena de datos F puede incluir los tiempos de vida característicos $T_i(\lambda)$ y las longitudes de onda relacionadas $\lambda_{i,}$, i =1, 2,... de un conjunto de diferentes longitudes de onda, que son preferentemente aquellas longitudes de onda donde se detectan los picos del espectro I (λ).

Si bien, en aras de una ilustración simple, los ejemplos anteriores se han descrito mediante el uso de una cadena de datos unidimensional F como una representación de la respuesta, también son posibles otras formas de representaciones de datos, en particular también formas multidimensionales, tales como las matrices.

B. Proporcionar un objeto físico con una marca de seguridad compuesta

Las Figuras 5 y 6 ilustran un método y un aparato ilustrativo para proporcionar un objeto físico con una marca de seguridad compuesta de acuerdo con la presente solución de seguridad.

Específicamente, la Figura 5 es un diagrama de flujo que ilustra un método básico para marcar un objeto físico con una marca de seguridad compuesta. La Figura 6 ilustra esquemáticamente un aparato 17 para realizar el método de la Figura 5, de acuerdo con una modalidad preferida que implica un proceso de fabricación aditiva (impresión 3D). El aparato 17 comprende una impresora 3-D 12, un escáner PUF 14, un dispositivo de procesamiento 15 y una impresora de código de barras 16. Además, el aparato 17 puede comprender además un contenedor 11 para una materia prima y medios (no dibujados) para mezclar UCD proporcionados desde un suministro 10 con una materia prima de impresión 3D. Opcionalmente, algunos o todos estos componentes 10 a 16 pueden integrarse en un mismo dispositivo.

En una primera etapa S5-1 del método, se agrega una PUF 2 (opcionalmente una pluralidad de PUF diferentes) a un objeto físico a marcar, que puede ser, por ejemplo y sin limitación, uno de los productos farmacéuticos ilustrados en las Figuras 3 y 4, o una pieza de repuesto, material de siembra, etc., como ya se describió en la sección de resumen anterior. En el caso del aparato 17 de la Figura 6, el objeto físico será típicamente un objeto sólido que puede imprimirse en 3-D. En este caso, la etapa S5-1 puede comprender la adición de uno o más tipos de UCD (preferentemente una mezcla secreta de UCD) al contenedor 11 que contiene una materia prima, por ejemplo, en forma de polvo, adecuada para la impresión en 3D. El UCD y la materia prima se mezclan, y luego la mezcla de material resultante se proporciona a la impresora 3-D 12 como un material de impresión 3-D. Con la ayuda de la impresora 3-D 12, un producto 13, tal como por ejemplo un dispositivo médico en forma de malla, se imprime de acuerdo con una especificación de diseño del producto entregado a la impresora 3-D 12 por medio de un archivo de diseño respectivo. Como los UCD se habían mezclado con la materia prima antes de la impresión, el producto resultante 13 incorpora estos UCD, que juntos forman una o más PUF 2.

En una etapa adicional S5-2, el producto 13 resultante de la etapa S5-1 se expone a un desafío C que se emite por el escáner PUF 14 en forma de radiación electromagnética de una longitud de onda, respectivamente, el intervalo de longitud de onda correspondiente al esquema de autenticación de desafío-esquema predeterminado perteneciente a las PUF 2 incorporadas en el producto 13. En una etapa adicional S5-3, que típicamente se produce de manera sustancialmente simultánea con la etapa S5-2, el escáner PUF 14 detecta una respuesta R emitida por la(s) PUF 2 que se incorporan en el producto 13 en reacción al desafío C. la respuesta se transforma luego en una cadena de datos F que la representa, por ejemplo, como se describió anteriormente en relación con la Figura 4. Particularmente, y sin limitación, la cadena de datos F puede ser una cadena binaria, como se ilustra. Si hay dos o más PUF 2, la cadena de datos F puede representar en particular las respuestas individuales de todas estas PUF 2, que opcionalmente también pueden interpretarse como una respuesta única combinada de una PUF combinada que comprende todos las PUF individuales.

En una etapa adicional S5-4, la cadena de datos F se proporciona al dispositivo de procesamiento 15 como una entrada, que aplica una función resumen criptográfica predeterminada H(...) a la cadena de datos F, para generar un valor resumen H = H(F) que representa la respuesta R. En otra etapa S5-5, con la ayuda del dispositivo de procesamiento 15, el valor resumen resultante H se firma digitalmente con una clave privada de un par de claves pública/privada de un sistema criptográfico asimétrico, tal como el esquema RSA bien conocido, con el fin de generar una firma digital 3 que comprenda el propio valor resumen H y una versión firmada digitalmente S [H(F)] del mismo.

En una etapa adicional S5-6a, mediante el uso de la impresora de código de barras 16, la firma digital 3 se imprime en una superficie del producto 13 en forma de código de barras bidimensional, por ejemplo, un código QR o un código DATAMATRIX. Como consecuencia, el producto terminado 13 ahora comprende tanto la(s) PUF 2 como la firma digital

correspondiente (3) y, por lo tanto, una marca de seguridad compuesta completa 1 de acuerdo con la presente solución de seguridad.

En una variante alternativa, se realiza una etapa adicional S5-6b en lugar de la etapa S5-6a. La etapa S5-6b es similar a la etapa S5-6a, con la excepción de que en lugar de la firma digital 3 en sí, solo se imprime un puntero 4 que indica dónde puede accederse a la firma digital 3, por ejemplo, en una base de datos o en un servidor de Internet en el producto 13. Antes, simultáneamente o después de la etapa S5-6b, se realiza una etapa adicional S5-7 en donde la firma digital 3 obtenida en la etapa S5-5 es almacenada por el dispositivo de procesamiento a través de un enlace de datos a la localización indicada por el puntero 4 para acceso posterior.

En ambas variantes S5-6a y S5-6b, puede agregarse una representación de la firma digital 3 respectivamente del puntero 4, en lugar o además de la impresión, en forma de una representación electrónica, por ejemplo, un chip RFID que se dispone para emitir una señal que lleve dicha representación al recibir una señal de activación respectiva (véase la Figura 1(c)).

C. Lectura de una marca que comprende una PUF

La lectura de una marca que comprende una PUF, en particular de una marca de seguridad compuesta de acuerdo con el primer aspecto de la presente solución de seguridad, por ejemplo, como se muestra y describe en relación con la Figura 1, se describe ahora en relación con las Figuras correspondientes 7A a 9.

Las Figuras 7A y 7B juntas muestran un diagrama de flujo (dividido en dos partes conectadas a través del conector "A") que ilustra una primera modalidad preferida de un método de lectura con un dispositivo lector de una marca que comprende una PUF, tal como una marca de seguridad compuesta de la Figura 1. El método comprende, opcionalmente, una primera fase que comprende las etapas S7-1 a S7-7, que sirven para mejorar la seguridad de un dispositivo lector que realiza el método.

La etapa S7-1 es una etapa de monitoreo de acceso, en donde se evalúan las salidas del sensor para detectar, como evento de seguridad, un intento o un acto real de intrusión física en el dispositivo lector, o un intento o acto real de acceso local o remoto de una funcionalidad de control interno, tal como un dispositivo de procesamiento o dispositivo de comunicación, del dispositivo lector. Si en una etapa adicional S7-2, se determina que en la etapa S7-1 se detectó un evento de seguridad (S7-2; sí), el método realiza una etapa de defensa de seguridad S7-5 como etapa final, en donde un mensaje de error que indica el evento de seguridad se emite en una interfaz de usuario y/o se envía a través de un enlace de comunicación a un lado contrario, tal como un centro de confianza predeterminado. Además, el dispositivo lector puede bloquearse y/o el dispositivo lector o al menos los datos almacenados en el mismo pueden autodestruirse para evitar el acceso no autorizado a los datos o cualquier funcionalidad del dispositivo lector. De cualquier otra manera (S7-2; no), el método pasa a una etapa de monitoreo de información S7-3.

En la etapa de monitoreo de información S7-3, se recibe una señal a través de un enlace de comunicación de una autoridad central de la solución de seguridad, tal como un centro de confianza que proporciona un servidor de seguridad, y se evalúa para detectar si un evento de seguridad se indica por la información contenida en la señal. Si en una etapa adicional S7-4, se determina que en la etapa S7-3 se indicó un evento de seguridad en la información (S7-4; sí), el método continúa y realiza la etapa de defensa de seguridad S7-5 como una etapa final. De cualquier otra manera (S7-4; no), el método pasa a una etapa de autenticación S7-5.

En la etapa de autenticación S7-5, un usuario del dispositivo lector se autentica, por ejemplo, a través de una interfaz de usuario adecuada, tal como un teclado para ingresar una contraseña o un sensor de huellas digitales, etc. Si en otra etapa S7-7, se determina que la autenticación de la etapa S7-6 falló (S7-7; no), el método vuelve a la etapa 7-1 o, alternativamente, a la etapa de autenticación S7-6 (no está dibujada). De cualquier otra manera (S7-7; sí), el método pasa a una segunda fase, en donde se lee la marca y se emite un resultado de lectura.

Esta segunda fase comprende una etapa de estimulación S7-8, en donde se crea un desafío físico de acuerdo con un esquema predeterminado de desafío-respuesta correspondiente a una PUF comprendida en la marca y se aplica a la PUF, que podría contener, por ejemplo, una mezcla de diferentes UCD.

Posterior o simultáneamente con la etapa de estimulación S7-8, se realiza una etapa de detección S7-9, en donde se detecta una respuesta generada por la PUF en reacción al desafío físico y de acuerdo con el esquema de autenticación de desafío-respuesta y se genera una señal digital que representa la respuesta y que podría, por ejemplo, tomar la forma o incluir un código de barras espectral, como se describió anteriormente.

En una etapa de procesamiento posterior S7-10, la señal digital se procesa para generar un valor resumen de la respuesta mediante la aplicación de una función resumen criptográfica predeterminada a la señal digital. Opcionalmente, la etapa de procesamiento puede comprender además firmar digitalmente dicho valor resumen para proporcionar una (primera) firma digital del mismo.

La etapa de procesamiento S7-10 es seguida por una etapa de salida S7-14a, en donde se emite un (primer) resultado de lectura, por ejemplo, en una interfaz de usuario del dispositivo lector o en un flujo de datos o archivo proporcionado en una interfaz electrónica u óptica del dispositivo lector. El (primer) resultado de lectura comprende los datos que representan el valor resumen generado en la etapa de procesamiento y/o una representación de dicha (primera) firma digital. En consecuencia, este método puede usarse para leer una marca que comprende una PUF, en particular una marca de seguridad compuesta, como se describe en la presente descripción (por ejemplo, en la Figura 1) y para emitir un resultado de lectura correspondiente que se basa en la respuesta generada por la PUF. Este resultado de lectura puede usarse para fines de autenticación en el campo (por ejemplo, en varios nodos a lo largo de una cadena de suministro de productos que va a marcarse), o incluso inicialmente en un sitio de fabricación o puesta en servicio, cuando se marca inicialmente un objeto físico, para verificar la marca y para capturar su respuesta para un uso posterior, por ejemplo, para almacenarla en una base de datos para fines de autenticación posteriores.

Las Figuras 8A y 8B juntas muestran un diagrama de flujo (dividido en dos partes conectadas a través del conector "B") que ilustra una segunda modalidad preferida de un método de lectura con un dispositivo lector de una marca que comprende una PUF, tal como una marca de seguridad compuesta de la Figura 1. Opcionalmente, este método puede comprender una primera fase similar que comprende las etapas S8-1 a S8-7 (que corresponden a las etapas S7-1 a S7-7 de la Figura 7A) para mejorar la seguridad de un dispositivo lector en sí. Además, el método comprende una etapa de estimulación S8-8, una etapa de detección S8-9 y una etapa de procesamiento S8-10, en donde estas etapas corresponden a y pueden ser en particular idénticas a las etapas S7-8 a S7-10 de las Figuras 7A y 7B.

El método comprende además una etapa de adquisición S8-11, en donde se adquiere una primera firma digital comprendida en la marca de seguridad compuesta y se accede a una segunda firma digital perteneciente a la marca. En particular, dicho acceso puede realizarse mediante la adquisición de la marca de seguridad compuesta de un puntero que indica una fuente donde puede accederse a la segunda firma digital, por ejemplo, desde un servidor remoto. La segunda firma digital se lee desde dicha fuente y se inicializa (desactiva) un indicador de coincidencia. La etapa de adquisición S8-11 puede realizarse antes, simultáneamente o después de la etapa de procesamiento S8-10.

En una etapa de coincidencia posterior S8-12, se compara el valor resumen firmado y comprendido en la primera firma digital adquirida y un valor resumen generado en la etapa de procesamiento S8-10. Si los dos valores resumen coinciden (S8-12; sí), se establece el indicador de coincidencia (etapa S8-13), de cualquier otra manera (S8-12; no) no se establece el indicador de coincidencia. Por supuesto, el uso de este indicador de coincidencia es solo una de las muchas implementaciones posibles diferentes para determinar y comunicar si los dos valores resumen coinciden o no.

El método comprende además una etapa de salida S8-14b, en donde se emiten diversos resultados de lectura, por ejemplo, en una interfaz de usuario del dispositivo lector o en un flujo de datos o archivo proporcionado en una interfaz electrónica u óptica del dispositivo lector. En particular, los resultados de lectura incluyen un (primer) resultado de lectura que comprende los datos que representan el valor resumen generado en la etapa de procesamiento y/o una representación de dicha (primera) firma digital. Otros resultados de lectura pueden comprender una representación de la primera firma digital adquirida, una representación, por ejemplo, como un código de barras, de la segunda firma digital leída, y/o una salida coincidente que indica (i) una coincidencia, si se establece el indicador de coincidencia, y (ii) de cualquier otra manera es una discordancia. En consecuencia, también este método puede usarse para leer una marca que comprende una PUF, particularmente una marca de seguridad compuesta, como se describe en la presente descripción (por ejemplo, en la Figura 1) y para emitir un resultado de lectura correspondiente que se basa en la respuesta generada por la PUF. Nuevamente, este resultado de lectura puede usarse particularmente para fines de autenticación en el campo (por ejemplo, en varios nodos a lo largo de una cadena de suministro de productos que van a marcarse).

El método comprende además una etapa de almacenamiento S8-15, que se realiza preferentemente de manera simultánea o después de la etapa de salida S8-14b. En la etapa de almacenamiento S8-15, el primer resultado de lectura que comprende los datos que representan el valor resumen generado en la etapa de procesamiento se almacena en un bloque de una primera cadena de bloques y el segundo resultado de lectura obtenido en la etapa de adquisición se almacena en un bloque de una segunda cadena de bloques separada. Además, los punteros de cadena de bloques cruzados relacionados que conectan las dos cadenas de bloques se almacenan en cada una de las dos cadenas de bloques para indicar los bloques en cada una de las cadenas de bloques, que se corresponden entre sí en este sentido, que contienen datos creados y almacenados en el mismo evento de lectura. En particular, la segunda cadena de bloques podría estar relacionada con la información de la cadena de suministro, tal como la hora, la localización y la identificación del usuario del evento de lectura actual. La primera cadena de bloques, por otro lado, se usa para rastrear la información de autenticación, en particular, ya sea que en el evento de lectura actual el objeto físico que lleva la marca haya sido autenticado o no con éxito como original (es decir, no falsificado o manipulado).

Además, el método puede comprender una etapa de comunicación S8-16, en donde la salida de datos en la etapa de salida, que incluye la salida coincidente, y opcionalmente también una marca de tiempo y/o una localización actual del evento de lectura, respectivamente, el dispositivo lector (cada uno de los cuales puede considerarse información relacionada con la seguridad) se envía a través de un enlace de comunicación a un servidor central predeterminado, que por ejemplo puede formar parte de un centro de confianza.

La Figura 9 ilustra esquemáticamente un dispositivo lector 20, de acuerdo con una modalidad preferida de la presente invención. En particular, el dispositivo lector puede adaptarse para realizar el método de las Figuras 7A y 7B y/o las Figuras 8A y 8B. A manera de ejemplo, y sin limitación, el dispositivo lector 20 puede formar un componente o usarse en relación con una línea de fabricación o puesta en servicio, que se ilustra en la Figura 9 por medio de un transportador 31 en el que los objetos físicos 32, es decir los productos, cada uno que lleva una marca de seguridad compuesta como se describe en la presente descripción (por ejemplo, en la Figura 1), se transportan hacia y desde el dispositivo lector 20.

El dispositivo lector 20 puede comprender varios componentes diferentes 21 a 30, que se interconectan comunicativamente por un bus de datos 33 o cualquier otra tecnología de comunicación adecuada. En particular, el dispositivo lector 20 comprende un estimulador 21 adaptado para generar y aplicar a una marca de seguridad compuesta 1 en el producto 32 que pasa por el transportador 31 una estimulación de acuerdo con un esquema de autenticación de desafío-respuesta predeterminado, y un detector PUF correspondiente 22 adaptado para detectar la respuesta emitida por la PUF de la marca en reacción a la estimulación. Por ejemplo, si la PUF comprende una mezcla de diferentes UCD, el estimulador 21 puede adaptarse para admitir una radiación electromagnética adecuada con el fin de estimular los UCD en la PUF para reemitir la radiación electromagnética que es característica de la PUF específica de la marca. En consecuencia, en tal caso, el detector de PUF se adapta para detectar tal radiación reemitida y analizarla espectralmente para derivar una señal digital, por ejemplo, en forma de código de barras espectral, que representa la respuesta y que puede procesarse adicionalmente.

Además, el dispositivo lector 20 puede comprender un dispositivo de adquisición 23 que se adapta para adquirir una primera firma digital comprendida en la marca de seguridad compuesta. En particular, el dispositivo de adquisición 23 puede adaptarse para realizar una etapa similar a la etapa S8-11 de la Figura 8B.

Además, el dispositivo lector 20 puede comprender un dispositivo de comunicación 24 que se adapta para comunicarse con un lado contrario 34, por ejemplo, un servidor de seguridad central de un centro de confianza, a través de un enlace de comunicación. En particular, el enlace de comunicación puede implementarse como un enlace inalámbrico, en cuyo caso el dispositivo de comunicación típicamente comprendería o estaría conectado a una antena 24a, o el enlace puede implementarse por medio del cable, tal como un cable eléctrico u óptico, como un enlace de comunicación no inalámbrico 24b. Particularmente, el dispositivo lector 20 puede configurarse para enviar los resultados de lectura que se emitirán en la etapa de salida (como en la etapa 8-14b de la Figura 8B, por ejemplo) a través del enlace de comunicación para informar al lado contrario 34 de los resultados de la lectura y/u otra información, tal como información relacionada con la seguridad (por ejemplo, la ocurrencia de un evento de seguridad en el dispositivo lector 20).

Para aumentar aún más la seguridad, el dispositivo lector 20 también puede comprender un dispositivo de autenticación 25 que se adapta para autenticar a un usuario del dispositivo lector 20, antes de permitir el acceso a este y/o su uso posterior (tal como en las etapas S8-6 y S8-7 de la Figura 8A).

El dispositivo lector 20 puede comprender además un dispositivo de seguridad 26 que comprende uno o más sensores para detectar un evento de seguridad, tal como un intento o acto real de intrusión física en el dispositivo lector 20, o un intento o acto real de acceso local o remoto sin autorización a una funcionalidad de control interno del dispositivo lector 20. Preferentemente, el dispositivo de seguridad 26 interactúa con o comprende además una disposición de defensa de seguridad 27 para proteger el dispositivo lector 20 en caso de que se detecte un evento de seguridad. En particular, la disposición de defensa de seguridad 27 puede adaptarse para realizar una etapa similar a la etapa S7-5 de la Figura 7A o a la etapa S8-5 de la Figura 8A. Por ejemplo, la disposición de defensa de seguridad 27 puede configurarse para bloquear una interfaz de usuario del dispositivo lector 20 en caso de que se detecte un evento de seguridad o para activar una autodestrucción de un chip de seguridad contenido en el dispositivo lector 20, para proteger los datos almacenados en el mismo, que incluye, por ejemplo, una clave criptográfica privada u otros datos relevantes para la seguridad, tales como los datos de autenticación. Además, o en lugar del dispositivo de seguridad 26, el dispositivo lector 20 puede comprender un dispositivo de monitoreo 28, que se configura para detectar un evento de seguridad indicado en la información contenida en una señal recibida desde el lado contrario 34 sobre dicho enlace de comunicación. Por ejemplo, en caso de que tal lado contrario 34, por ejemplo, un centro de confianza, aprenda acerca de un intento más amplio de atacar la seguridad e integridad de los dispositivos lectores 20 que se distribuyen en el campo, por ejemplo, a lo largo de una cadena de suministro dada, dicha señal puede usarse para desencadenar de manera proactiva un bloqueo (al menos temporalmente) de cualquier uso adicional de los dispositivos lectores 20 en el campo para evitar la manipulación de los dispositivos lectores 20 por tales ataques.

Además, el dispositivo lector 20 comprende un dispositivo de procesamiento 29 que está particularmente adaptado, por ejemplo, por un programa de software respectivo que se ejecuta en este, para procesar la señal digital generada por el detector PUF para generar un valor resumen de la respuesta de la PUF mediante la aplicación de una función resumen criptográfica predeterminada a la señal digital (véanse las etapas S7-10 de la Figura 7B y las etapas S8-10 de la Figura 8B). En algunas implementaciones, el dispositivo de procesamiento 29 puede implementar adicionalmente una funcionalidad adicional del dispositivo lector 20 que implica el procesamiento o control de datos. En consecuencia, la totalidad o parte de cualquier funcionalidad de procesamiento de los otros componentes 21 a 28 y 30 del dispositivo

lector 20 puede incorporarse en el dispositivo de procesamiento 29 en lugar de implementarse en componentes separados.

El dispositivo lector también puede comprender un dispositivo de almacenamiento de cadena de bloques que se adapta para almacenar datos en una o más cadenas de bloques, a las que el dispositivo lector 20 puede conectarse a través de dicho enlace de comunicación. En particular, dichos datos pueden corresponder a los resultados de lectura generados cuando el dispositivo lector se usa para leer una marca que comprende una PUF. Si bien el dispositivo de almacenamiento de la cadena de bloques puede implementarse como un componente o módulo separado del dispositivo lector 20, preferentemente se incluye en el dispositivo de procesamiento 29, como en la Figura 9.

Un generador de salida 30 forma un componente adicional del dispositivo lector 20. Se configura para generar, por ejemplo, en una interfaz de usuario o en una interfaz eléctrica u óptica, datos que representan el valor resumen generado como primer resultado de lectura, una representación de firmas digitales adquiridas, tales como la primera firma digital y la segunda firma digital descritas anteriormente (cf. etapa S8-14b de la Figura 8B) y, opcionalmente, una salida coincidente que indica si los valores resumen resultantes de la etapa de procesamiento (cf. etapa S8-10 de la Figura 8B) y la etapa de adquisición (cf. etapa S8-11 de la Figura 8B) coincidencia (cf. etapa S8-12 de la Figura 8B).

D. Solución de seguridad general

Las Figuras 10 y 11 ilustran aspectos preferidos adicionales de la solución de seguridad global que se basa en el uso de marcas que comprenden una PUF y en uno o más dispositivos lectores, como se describió anteriormente. En particular, la Figura 10 muestra una visión general esquemática de una modalidad básica de un sistema de seguridad 14 basada en la presente solución de seguridad que permite verificar, a un destinatario B que participa en una cadena de suministro, si un producto que va a marcarse por una marca de seguridad compuesta 1 (por ejemplo, según la Figura 1) es original y de hecho fue proporcionado por el supuesto fabricante original A posicionado aguas arriba en la cadena de suministro.

Para este fin, el fabricante A se equipa con un aparato para aplicar una marca de seguridad compuesta 1 a los productos 32 que se van a enviar posteriormente a lo largo de la cadena de suministro. Por ejemplo, tal aparato puede ser un aparato similar al aparato que se muestra en la Figura 6. Alternativamente, el fabricante A puede equiparse con un dispositivo lector 20, tal como el que se muestra en la Figura 9, y usar un aparato separado para aplicar una marca de seguridad compuesta correspondiente 1 que lleva información leída por el dispositivo lector 20, que incluye una (primera) firma digital que comprende un valor resumen que va a derivarse de la lectura de la PUF en la marca de seguridad compuesta 1. En consecuencia, el aparato 17, respectivamente 20, se configura para realizar el método correspondiente de la Figura 5, respectivamente, de las Figuras 7A y 7B. Además, el aparato 17 o 20 se equipa para generar un par de claves pública/privada de un sistema criptográfico asimétrico, almacenar la clave privada (clave segura, SK) en un espacio de almacenamiento seguro del aparato 17 respectivamente 20 y reenviar la clave pública (PUK) junto con la primera firma digital y, opcionalmente, la información relacionada con la seguridad adicional, tal como la hora y/o localización de la generación de la primera firma digital, a un servidor de seguridad central 34 localizado en un centro de confianza que se contempla por un tercero de confianza. En consecuencia, el centro de confianza desempeña el papel de una autoridad de registro, donde se registran y almacenan las claves públicas particulares de uno o más aparatos 17 y dispositivos lectores 20. Preferentemente, cualquier comunicación hacia y desde el centro de confianza se protege mediante cifrado, en particular para evitar "ataques por intermediarios".

Para aumentar el nivel de seguridad disponible, la clave pública se puede proporcionar a una autoridad de certificación de una infraestructura de clave pública (PKI), particularmente a un servidor de autoridad de certificación relacionado 42, donde la clave pública está certificada e incluida en un certificado criptográfico que se pone a disposición del fabricante A y una autoridad de validación (servidor) 41. Ahora, cualquier nodo adicional en la cadena de suministro que esté equipado con un dispositivo lector 20 como se describe en la presente descripción, tal como el destinatario B, puede solicitar el certificado a la autoridad de validación 41 para usarlo para examinar el producto marcado presuntamente originario del fabricante A por su autenticidad. Con ese fin, el dispositivo lector 20 en el destinatario B ejecuta el método de las Figuras 8A y 8B y, de esta manera, detecta la PUF en la marca de seguridad compuesta 1 del producto 32 y lee la primera firma digital contenida en el mismo, que incluye el valor resumen que se compara con el valor resumen derivado de la respuesta detectada de la PUF. Si ambos valores resumen coinciden, esto confirma que el fabricante A fue de hecho el emisor del producto 32, de cualquier otra manera, el producto o su marca se han falsificados o manipulados de cualquier otra manera.

El resultado de esta comparación, es decir, el resultado coincidente y, opcionalmente, la información adicional relacionada con la seguridad, como la hora y la localización del examen y/o la identidad de un usuario del dispositivo lector 20 que realiza el examen, o se reenvía y almacena en el servidor de seguridad central 34 del centro de confianza. Esto permite un monitoreo central de la cadena de suministro e identificación temprana de cualquier problema de falsificación o manipulación que ocurra a lo largo de la cadena de suministro. El servidor de seguridad central 34 puede configurarse además para generar o consolidar y poner a disposición a través de una interfaz de datos API el rastreo y el seguimiento de datos que reflejan el procesamiento del producto 32 a lo largo de la cadena de suministro en base a los resultados coincidentes y la información relacionada con la seguridad proporcionada por cualquier dispositivo lector 20 que participa en la cadena de suministro.

La Figura 11 se refiere a una modalidad preferida adicional de la presente solución de seguridad, particularmente de un sistema de seguridad 40, en donde la tecnología de cadena de bloques se usa para almacenar de manera segura y poner a disposición los datos de autenticación que se generan a lo largo de la cadena de suministro. Específicamente, la Figura 11 ilustra esquemáticamente una evolución de un conjunto de dos cadenas de bloques interconectadas en paralelo a una cadena de suministro para un producto 32 que va a marcarse con una marca de seguridad compuesta 1, de acuerdo con las modalidades preferidas de la presente solución de seguridad. Particularmente, las modalidades de la Figura 10 y la Figura 11 pueden combinarse dentro de una única solución.

La solución de la Figura 11 comprende una primera cadena de bloques BC-PUF que se configura para almacenar y poner a disposición de manera segura la información de autenticación, en particular los valores resumen derivados de la detección de PUF contenidos en las marcas compuestas de seguridad 1 de los productos relacionados 32, como se describe en la presente descripción. Además, se proporciona una segunda cadena de bloques BC-SCM, que se configura para almacenar de manera segura y poner a disposición la información de la cadena de suministro, tales como los números de serie de los productos 32, las fechas y las localizaciones de las lecturas de las marcas de seguridad compuestas 1 de los productos 32 etc. En particular, tales datos de la cadena de suministro pueden almacenarse en la segunda cadena de bloques BC-SCM en forma de, o además de, los valores resumen relacionados que se generan a partir de dichos datos mediante la aplicación de una función resumen adecuada. Las dos cadenas de bloques BC-PUF y BC-SCM, que ambas se configuran para rastrear el movimiento de los productos 32 a lo largo de la cadena de suministro, tienen sus bloques relacionados, es decir, los bloques que contienen datos pertenecientes al mismo punto de control a lo largo de la cadena de suministro, unidos por punteros de cadena de bloques cruzados, lo que proporciona por lo tanto referencias desde y hacia los bloques correspondientes.

En un primer nodo de la cadena de suministro, que es propiedad de un fabricante A de un producto 32, este producto 32 se marca con una marca de seguridad compuesta 1, como se describe en la presente descripción, por ejemplo, del tipo que se muestra en la Figura 1. De nuevo, un aparato 17 o un dispositivo lector 20, como se describió anteriormente con referencia a la Figura 6, respectivamente, la Figura 9, puede usarse para este propósito. En el curso de este proceso de marcado, el aparato 17 detecta la marca de seguridad compuesta 1 respectivamente 20 y se generan unos valores resumen respectivos. Opcionalmente, este valor resumen se confirma comparándolo con un valor resumen correspondiente proporcionado por la primera firma digital también contenida en la marca de seguridad compuesta 1, y luego se almacena en un primer bloque de la cadena de bloques BC-PUF como un resumen PUF inicial valor como parte de una primera transacción almacenada #1 originada por el fabricante A.

La marca de seguridad compuesta 1 del producto 32 comprende además una segunda firma digital que incluye un segundo valor resumen derivado de los datos relacionados con la cadena de suministro pertenecientes al fabricante A. Este segundo valor resumen se lee de la marca de seguridad compuesta 1, mediante el uso del aparato 17 respectivamente, el dispositivo lector 20, y almacenado en un primer bloque de la segunda cadena de suministro BC-SCM como parte de una primera transacción #1 originada por el fabricante A, opcionalmente junto con otros datos relacionados con la cadena de suministro. Ambos de estos dos primeros bloques contienen datos correspondientes a la etapa inicial de la cadena de suministro que pertenece al fabricante A y, en consecuencia, en cada uno de los dos bloques se agrega un puntero de cadena cruzada al bloque correspondiente en la otra cadena de bloques, para permitir referencias cruzadas.

En la siguiente etapa a lo largo de la cadena de suministro, el producto 32 alcanza un segundo nodo intermedio C, que podría ser, por ejemplo, propiedad de una empresa de logística responsable del transporte adicional del producto a lo largo de la cadena de suministro. El nodo C se equipa con otro dispositivo lector 20 y, por lo tanto, realiza un examen del producto 32 ejecutando el método de las Figuras 8A y 8B en dicho dispositivo lector 20 en relación con la marca de seguridad compuesta 1 del producto 32. Si este examen confirma que el fabricante A es el emisor del producto 32, una transacción respectiva #2 que confirma el examen positivo se almacena en un segundo bloque de la primera cadena de bloques BC-PUF. De cualquier otra manera, dicha transacción almacenada #2 indica un resultado negativo del examen, lo que indica un fraude en relación con el producto 32, respectivamente, su marca de seguridad compuesta 1. Además, el generador de salida 30 puede emitir un mensaje de alarma o error, por ejemplo, en una interfaz de usuario, del dispositivo lector 20, o puede enviarse un mensaje de alarma/error al centro de confianza central 34 a través del enlace de comunicación 24a o 24b para indicar dicho resultado negativo.

El segundo bloque se entrecruza con el bloque anterior, es decir, el primer bloque de dicha cadena de bloques mediante la adición del resumen de bloque de dicho bloque anterior. Esta entrada en la primera cadena de bloques BC-PUF confirma que el producto 32 se examinó en el nodo C con el resultado respectivo. El valor inicial de resumen PUF permanece disponible a través del entrecruzamiento con el primer bloque. De manera similar, como en el nodo anterior, la información de la cadena de suministro se genera a partir de la segunda firma digital de la marca de seguridad compuesta 1 y otros datos relacionados con el nodo y se almacenan en la segunda cadena de bloques BC-SCM como una transacción #2. También en esta segunda cadena de suministro BC-SCM, el segundo bloque se entrecruza al primer bloque anterior mediante el almacenamiento de un resumen de bloque de dicho bloque anterior en el segundo bloque. Nuevamente, se agrega un puntero de la cadena de bloques cruzado en cada uno de los segundos bloques para permitir la referencia cruzada entre ellos.

En la siguiente etapa a lo largo de la cadena de suministro, el producto 32 alcanza un tercer nodo intermedio d, que podría ser, por ejemplo, una estación logística remota que no se equipa con un dispositivo lector 20 sino que en su lugar solo tiene un escáner convencional que solo es capaz de leer la segunda firma digital comprendida en la marca de seguridad compuesta 1 del producto 32. A diferencia de los nodos anteriores, en el nodo d solo los datos relacionados con la cadena de suministro se escriben en un tercer bloque de la segunda cadena de suministro BC-SCM como una transacción #3, de manera similar al nodo C. Sin embargo, no se almacenan datos en la primera cadena de suministro BC-PUF, ya que el escáner no es capaz de leer la PUF de la marca de seguridad compuesta 1 y generar los datos relacionados.

Finalmente, en una cuarta etapa a lo largo de la cadena de suministro, el producto 32 llega al nodo B, que podría ser, por ejemplo, un destino final o un minorista local del producto 32. En este nodo B, se realiza un procedimiento similar mediante el uso de otro dispositivo lector 20, como en el nodo C anterior y, en consecuencia, se agregan entradas similares a los bloques adicionales respectivos de ambas cadenas de bloques PC-PUF y BC-SCM.

Las dos cadenas de bloques sirven como un libro público seguro de todas de dichas transacciones que se han producido y se han almacenado desde el inicio de dichas cadenas de bloques. Además, las cadenas de bloques proporcionan un nivel de integridad extremadamente alto, ya que no pueden manipularse (en la práctica) y, por lo tanto, su uso mejora aún más la seguridad de la solución de seguridad global presentada en la presente descripción. En particular, los datos almacenados en las dos cadenas de bloques pueden usarse para examinar si el fabricante A fue en realidad el emisor del producto 32 y si la cadena de suministro fue la esperada. Este examen puede realizarse en cada nodo A, C, B a lo largo de la cadena de suministro que se equipa con un dispositivo lector 20 y, por lo tanto, puede examinar la marca de seguridad compuesta 1 del producto 32 y acceder a los datos almacenados en las dos cadenas de bloques.

Si bien se ha descrito al menos una modalidad ilustrativa de la presente solución de seguridad, hay que señalar que existe un gran número de variaciones a la misma. Además, se aprecia que las modalidades ilustrativas descritas solo ilustran ejemplos no limitantes de cómo se puede implementar la presente solución de seguridad y que no se pretende limitar el alcance, la aplicación o la configuración de los aparatos y métodos descritos en la presente descripción. Por el contrario, la descripción anterior proporcionará al experto en la técnica construcciones para implementar al menos una modalidad ilustrativa de la solución, en donde debe entenderse que pueden realizarse diversos cambios de funcionalidad y el dispositivo de los elementos de la modalidad ilustrativa, sin desviarse del objetivo definido por las reivindicaciones adjuntas y sus equivalentes legales.

Lista de signos de referencia

1	Marca de seguridad compuesta
2	Función física no clonable, PUF
3	Firma digital correspondiente a la PUF
4	Puntero que indica dónde puede accederse a la firma digital
5	Botella que contiene bien consumible
6	Bien consumible, en particular sustancia farmacéutica líquida
7	Empaque
8	Comprimido farmacéutico, píldora
9	Blíster
10	Suministro de mezcla de diferentes UCD
11	Contenedor con materia prima para impresión 3-D
12	Dispositivo de fabricación aditiva, impresora 3-D
13	Objeto/producto físico impreso en 3D
14	Escáner PUF
15	Dispositivo de procesamiento
16	Impresora de código de barras
17	Aparato para proporcionar una marca de seguridad compuesta a un objeto
20	Dispositivo lector
21	Estimulador
22	Detector PUF
23	Dispositivo de adquisición
24	Dispositivo de comunicación
24a	Antena
24b	Enlace de comunicación no inalámbrico
25	Dispositivo de autenticación
26	Dispositivo de seguridad
27	Acuerdo de defensa de seguridad
28	Dispositivo de monitoreo
29	Dispositivo de procesamiento
30	Generador de salida
31	Transportador de una línea de producción

32 Objetos físicos marcados (productos)
33 Bus
34 Servidor de seguridad central, centro de confianza
40 Sistema de seguridad
41 Servidor de la Autoridad de Validación
42 Servidor de la Autoridad de Certificación
C Desafío de acuerdo con el esquema de autenticación de desafío-respuesta
R Respuesta de acuerdo con el esquema de autenticación de desafío-respuesta
F Datos (cadena) que representan la respuesta por PUF al desafío
H(F) Función resumen criptográfica aplicada a F, que produce un valor resumen H= H(F)
S[H(F)] Firma digital del valor resumen H
λ, longitud de onda
λi Longitud de onda, a la cual se produce un pico de intensidad de luz I en la respuesta R
I Intensidad de luz
Ii Intensidad de luz en la longitud de onda λi

REIVINDICACIONES

1. Un método para leer con un dispositivo lector una marca de seguridad compuesta que comprende una función física no clonable, PUF, y una primera firma digital correspondiente o un puntero que indica una fuente donde puede accederse a dicha primera firma digital, el método que comprende las siguientes etapas:
una etapa de estimulación, en donde se crea un desafío físico de acuerdo con un esquema de autenticación de desafío-respuesta predeterminado correspondiente a la PUF y se aplica a una PUF;
una etapa de detección, en donde se detecta una respuesta generada por la PUF de acuerdo con el esquema de autenticación de desafío-respuesta en reacción al desafío y se genera una señal digital que representa la respuesta;
una etapa de procesamiento, en donde la señal digital se procesa para generar un valor resumen de la respuesta mediante la aplicación de una función resumen criptográfica predeterminada a la señal digital; una etapa de salida, en donde se emiten los datos que representan el valor resumen generado como un primer resultado de lectura; y
caracterizado porque comprende además una etapa de adquisición, en donde la marca de seguridad compuesta se lee para adquirir dicha primera firma digital de la marca de seguridad compuesta o la fuente indicada por el puntero, respectivamente;
en donde en la etapa de salida una representación de la primera firma digital adquirida y/o una salida coincidente que indica si, de acuerdo con al menos un criterio de coincidencia predeterminado, se genera un valor resumen proporcionado y firmado por la primera firma digital adquirida coincide con el valor resumen generado a partir de la respuesta al desafío; en donde la etapa de adquisición comprende además adquirir de la marca de seguridad compuesta una segunda firma digital o un puntero que indica una fuente donde puede accederse a una segunda firma digital particular perteneciente a la marca; y
en donde la etapa de salida comprende además emitir una representación de la segunda firma digital adquirida como un segundo resultado de lectura.

2. El método de acuerdo con la reivindicación 1, en donde en la etapa de procesamiento de la señal digital se genera de tal manera que representa al menos una propiedad distintiva específica de la PUF de la respuesta que es, al menos sustancialmente, invariable bajo variaciones de las condiciones ambientales en las que se detecta la respuesta.

3. El método de una o más de las reivindicaciones anteriores, en donde detectar la respuesta en la etapa de detección comprende detectar al menos una propiedad de radiación electromagnética emitida por la PUF como respuesta en reacción al desafío y la señal digital se genera de manera que represente esta respuesta.

4. El método de acuerdo con la reivindicación 3, en donde detectar la respuesta en la etapa de detección comprende detectar una vida útil característica de un efecto de luminiscencia que se produce en la respuesta como una propiedad de la radiación electromagnética emitida por la PUF.

5. El método de acuerdo con la reivindicación 3 o 4, en donde:
detectar la respuesta en la etapa de detección comprende detectar un espectro de la radiación emitida como una propiedad de la radiación electromagnética emitida por la PUF;
y procesar la señal digital en la etapa de procesamiento comprende determinar a partir de la señal digital uno o más de los siguientes:
- la posición de uno o más rasgos característicos dentro del espectro;
- una o más medidas estadísticas que caracterizan el espectro;
- uno o más valores espectrales cuantificados del espectro;
- un código de barras espectral que representa un intervalo continuo o uno cuantificado de valores espectrales permitidos que ocurren en el espectro.

6. El método de una o más de las reivindicaciones anteriores, en donde la etapa de salida comprende además emitir al menos una parte de un resultado de lectura en forma de un código de barras unidimensional o multidimensional.

7. El método de una o más de las reivindicaciones anteriores, que comprende además una etapa de autenticación, en donde un usuario se autentica antes de permitirle operar aún más el dispositivo lector en caso de una autenticación exitosa.

8. El método de una o más de las reivindicaciones anteriores, que comprende además una etapa de comunicación, en donde un resultado de lectura se comunica a través de un enlace de comunicación a un lado contrario.

9. El método de acuerdo con la reivindicación 8, en donde la etapa de comunicación comprende además capturar y enviar la información relacionada con la seguridad a un lado contrario predeterminado a través del enlace de comunicación.

10. El método de acuerdo con la reivindicación 8 o 9, que comprende además una etapa de monitoreo de información, en donde se detecta un evento de seguridad en la información contenida en una señal recibida desde el lado contrario a través del enlace de comunicación.

11. El método de una o más de las reivindicaciones anteriores, que comprende además una etapa de monitoreo de acceso, en donde uno o más de los siguientes se detectan mediante uno o más sensores como un evento de seguridad:
- un intento o acto real de intrusión física en el dispositivo lector;
- un intento o acto real de acceder local o remotamente a una funcionalidad de control interno del dispositivo lector, en donde dicho acceso no está disponible para un usuario del dispositivo en el curso de su funcionamiento normal.

12. El método de acuerdo con la reivindicación 10 u 11, que comprende además una etapa de defensa de seguridad, en donde una o más de las siguientes medidas de seguridad se realizan en reacción a la detección de un evento de seguridad:
- bloquear el dispositivo lector para limitar o evitar su uso posterior;
- autodestruir al menos una parte funcional del dispositivo lector o destruir los datos almacenados en el mismo para evitar su uso o acceso por parte de un usuario.
- emitir un mensaje de error.

13. El método de una o más de las reivindicaciones anteriores, en donde la etapa de salida comprende firmar digitalmente datos que contienen el valor resumen generado y emitir la firma digital resultante como el primer resultado de lectura.

14. El método de una o más de las reivindicaciones anteriores, que comprende además una etapa de almacenamiento, en donde un resultado de lectura que se emite en la etapa de salida se almacena en un bloque de una cadena de bloques.

15. El método de acuerdo con la reivindicación 14, en donde la etapa de almacenamiento comprende:
almacenar un primer resultado de lectura que comprende los datos que representan el valor resumen generado en la etapa de procesamiento en un bloque de una primera cadena de bloques; y almacenar el resultado de la segunda lectura obtenida en la etapa de adquisición en un bloque de la segunda cadena de bloques que se separa de la primera cadena de bloques.

16. El método de acuerdo con la reivindicación 15, en donde la etapa de almacenamiento comprende, además:
al almacenar el resultado de la primera lectura en un bloque de la primera cadena de bloques, que incluye un puntero de cadena de bloques cruzada, que asigna de manera lógica el bloque de la primera cadena de bloques a un bloque correspondiente de la segunda cadena de bloques en el bloque de la primera cadena de bloques; y
al almacenar el resultado de la segunda lectura en un bloque de la segunda cadena de bloques, que incluye un puntero de cadena de bloques cruzada, que asigna de manera lógica el bloque de la segunda cadena de bloques a un bloque correspondiente de la primera cadena de bloques en el bloque de la segunda cadena de bloques.

17. Un dispositivo lector para leer una marca que comprende una función física no clonable, PUF, en donde el dispositivo lector se adapta para realizar el método de una o más de las reivindicaciones anteriores.

18. El dispositivo lector de acuerdo con la reivindicación 17 que comprende:
un estimulador que se configura para realizar la etapa de estimulación;
un detector PUF que se configura para realizar la etapa de detección;
un dispositivo de procesamiento configurado para realizar la etapa de procesamiento; y
un generador de salida que se configura para realizar la etapa de salida.

19. El dispositivo lector de acuerdo con la reivindicación 18, que comprende además uno o más de los siguientes:
- un dispositivo de autenticación configurado para realizar la etapa de autenticación de acuerdo con la reivindicación 7;
- un dispositivo de comunicación configurado para realizar la etapa de comunicación de acuerdo con la reivindicación 8 o 9;
- un dispositivo de monitoreo configurado para realizar la etapa de monitoreo de información de acuerdo con la reivindicación 10;
- un dispositivo de seguridad que comprende al menos un sensor y que se configura para realizar la etapa de monitoreo de acceso de acuerdo con la reivindicación 11;
- un acuerdo de defensa de seguridad que se configura para realizar la etapa de defensa de seguridad de acuerdo con la reivindicación 12;

- un dispositivo de almacenamiento de cadena de bloques configurado para realizar la etapa de almacenamiento de cualquiera de las reivindicaciones 14 a 16.

20. Un programa de ordenador que comprende instrucciones, que cuando se ejecuta en uno o más procesadores de un dispositivo lector de acuerdo con una o más de las reivindicaciones 17 a 19, hace que el dispositivo lector realice el método de acuerdo con una cualquiera de las reivindicaciones 1 a 16.

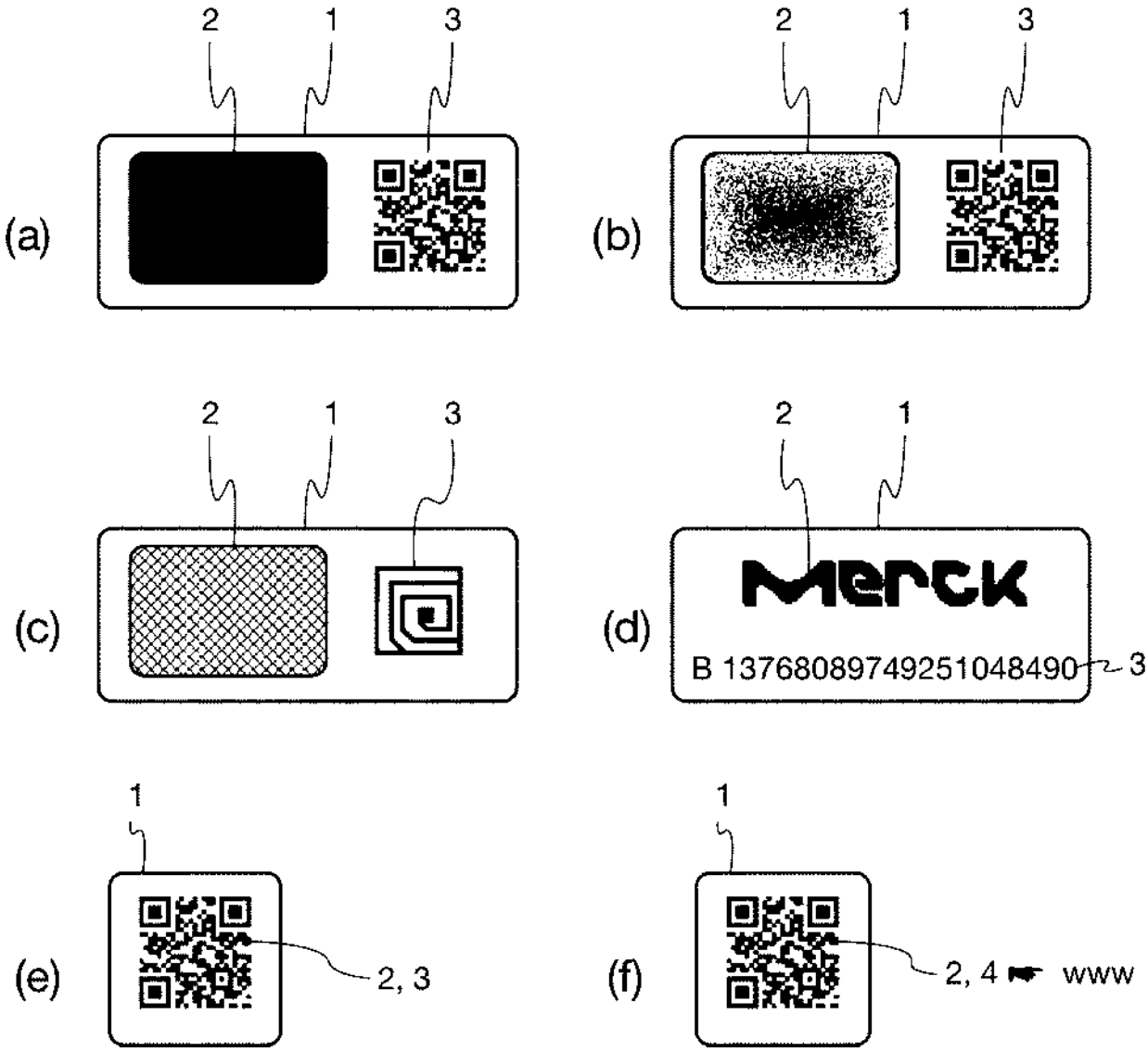
(a)
2
1
3
(b)
2
1
3
(c)
2
1
3
(d)
2
1
Merck
B 13768089749251048490
3
(e)
1
2, 3
(f)
1
2, 4
www

Figura 1

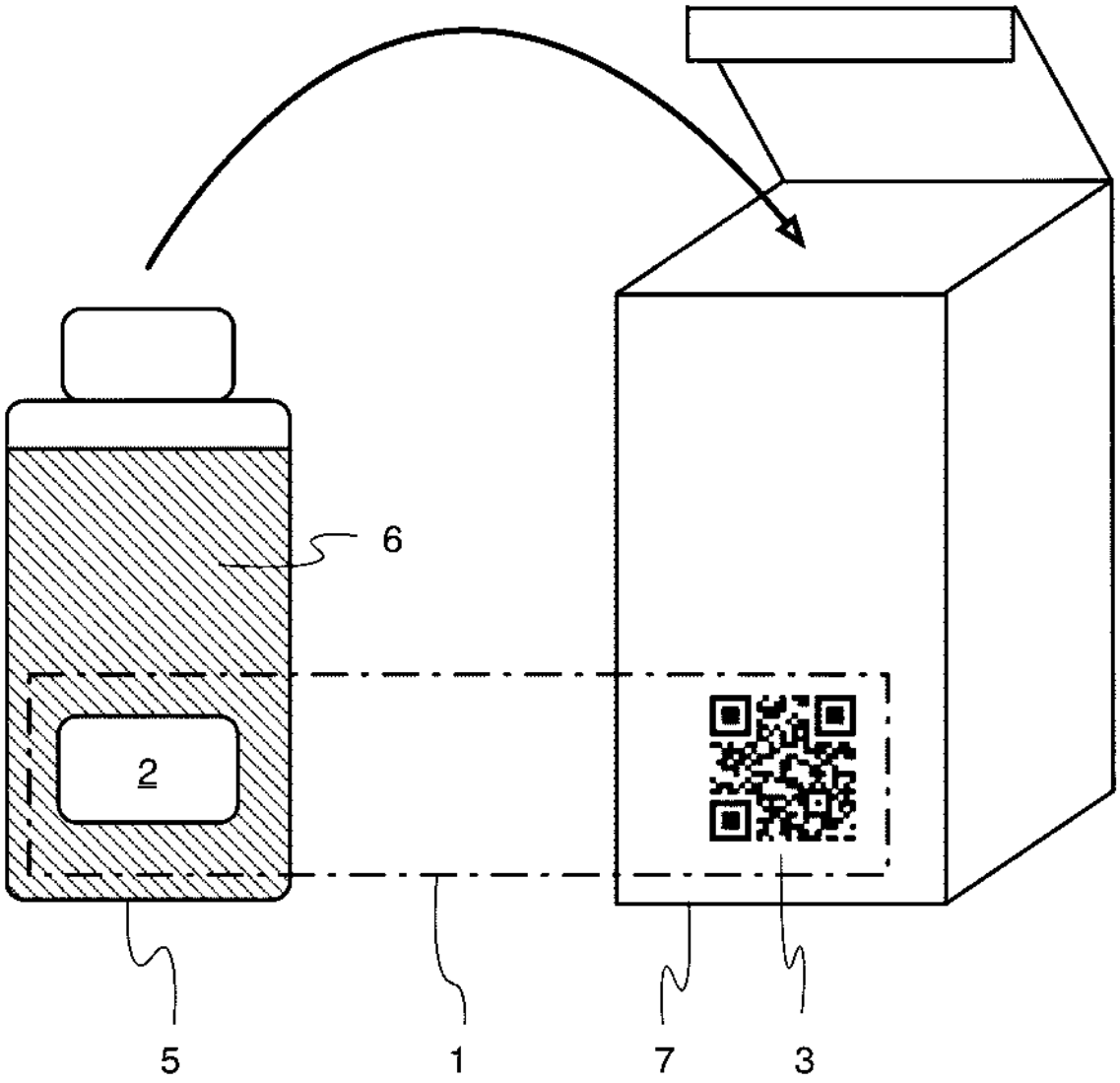

Figura 2

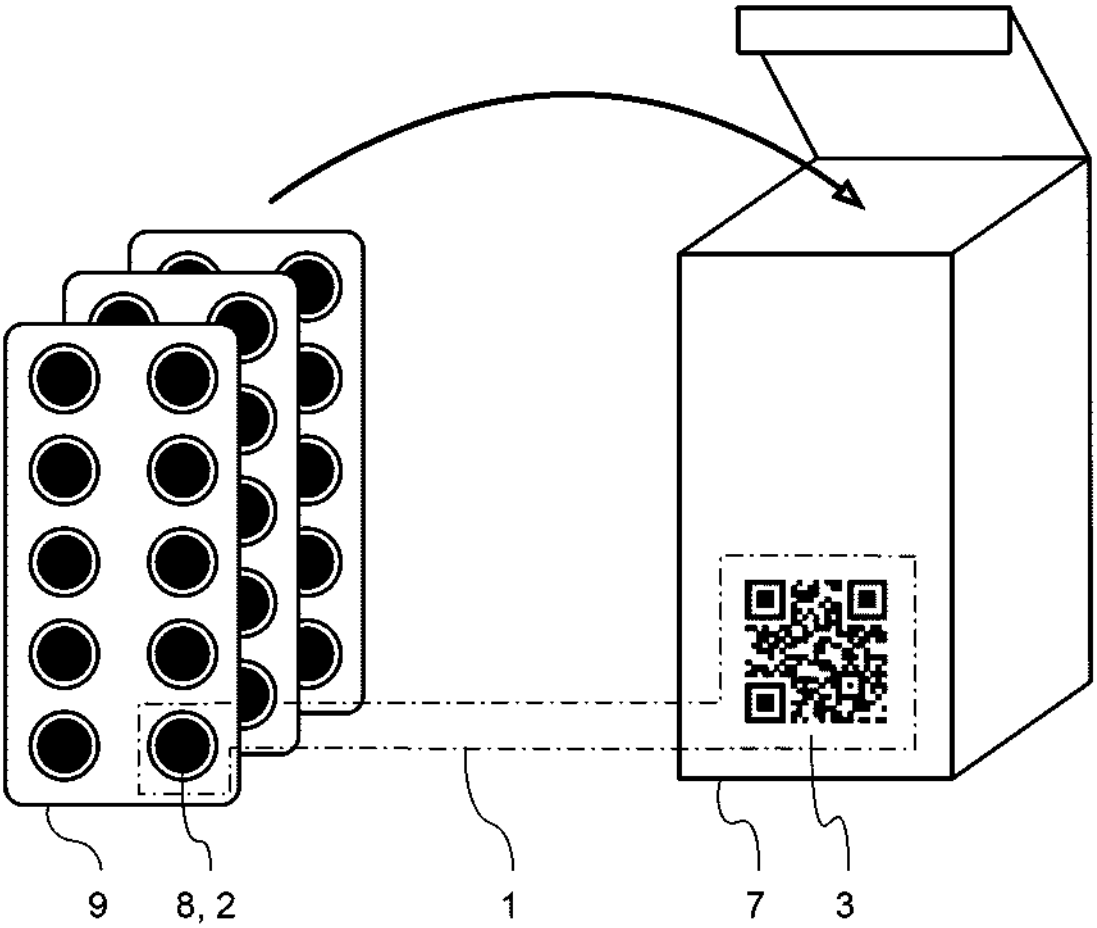

Figura 3

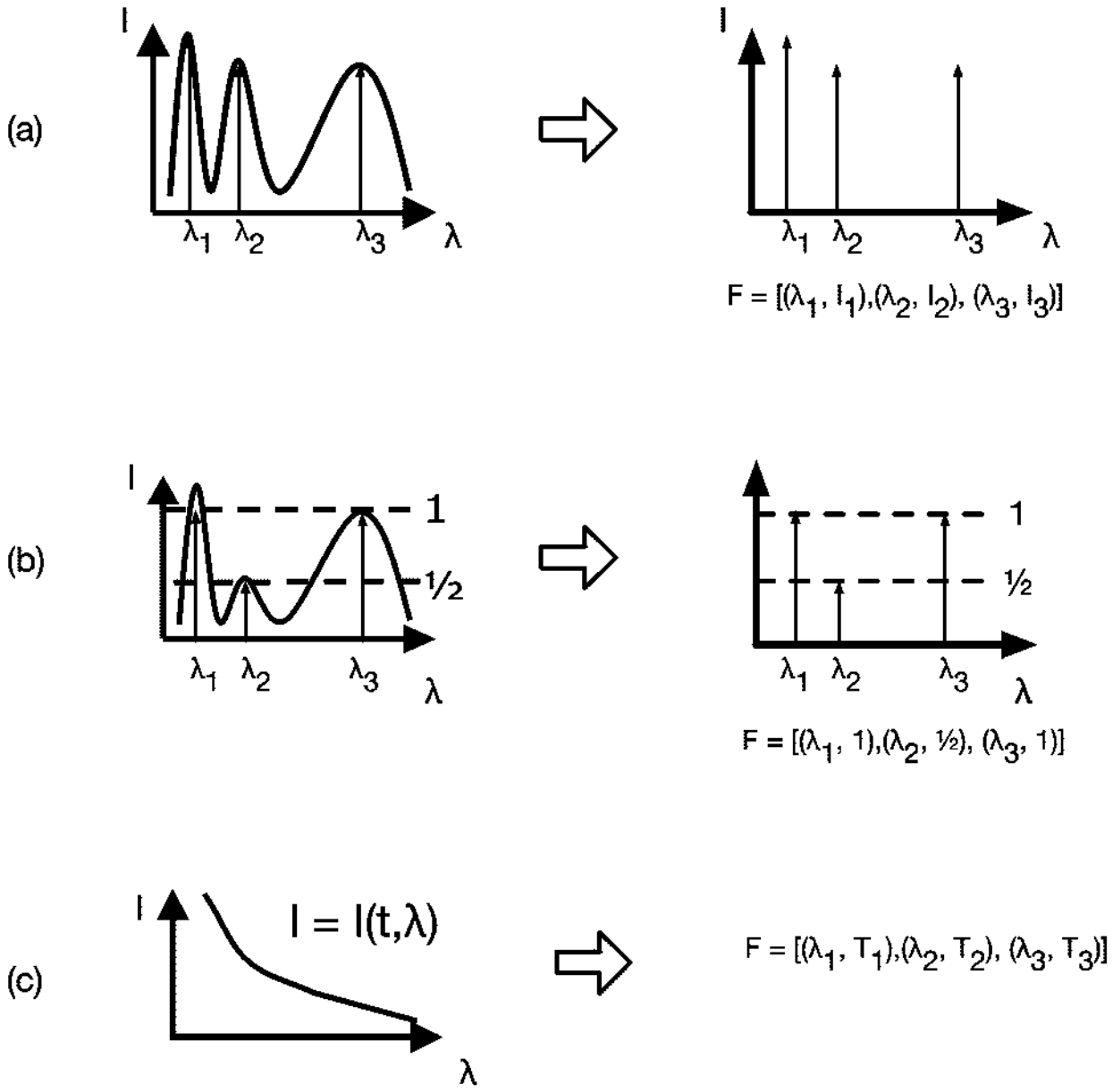
(a)
I
λ1 λ2 λ3 λ
I
λ1 λ2 λ3 λ
F = [(λ1, I1),(λ2, I2), (λ3, I3)]
(b)
I
1
½
λ1 λ2 λ3 λ
1
½
λ1 λ2 λ3 λ
F = [(λ1, 1),(λ2, ½), (λ3, 1)]
(c)
I
I = I(t,λ)
λ
F = [(λ1, T1),(λ2, T2), (λ3, T3)]

Figura 4

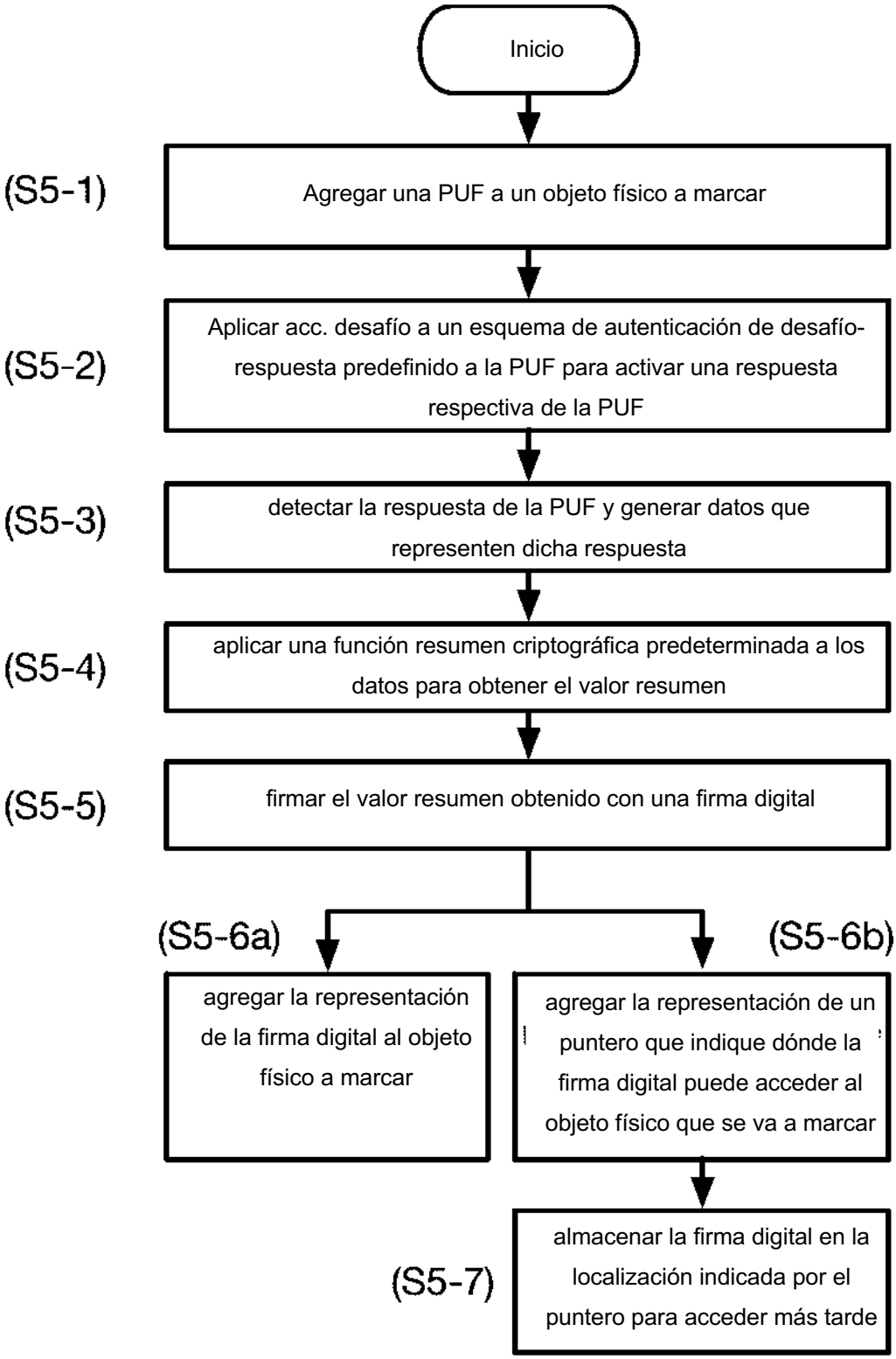
Inicio
(S5-1)
Agregar una PUF a un objeto físico a marcar
(S5-2)
Aplicar acc. desafío a un esquema de autenticación de desafío-respuesta predefinido a la PUF para activar una respuesta respectiva de la PUF
(S5-3)
detectar la respuesta de la PUF y generar datos que representen dicha respuesta
(S5-4)
aplicar una función resumen criptográfica predeterminada a los datos para obtener el valor resumen
(S5-5)
firmar el valor resumen obtenido con una firma digital
(S5-6a)
(S5-6b)
agregar la representación de la firma digital al objeto físico a marcar
agregar la representación de un puntero que indique dónde la firma digital puede acceder al objeto físico que se va a marcar
(S5-7)
almacenar la firma digital en la localización indicada por el puntero para acceder más tarde

Figura 5

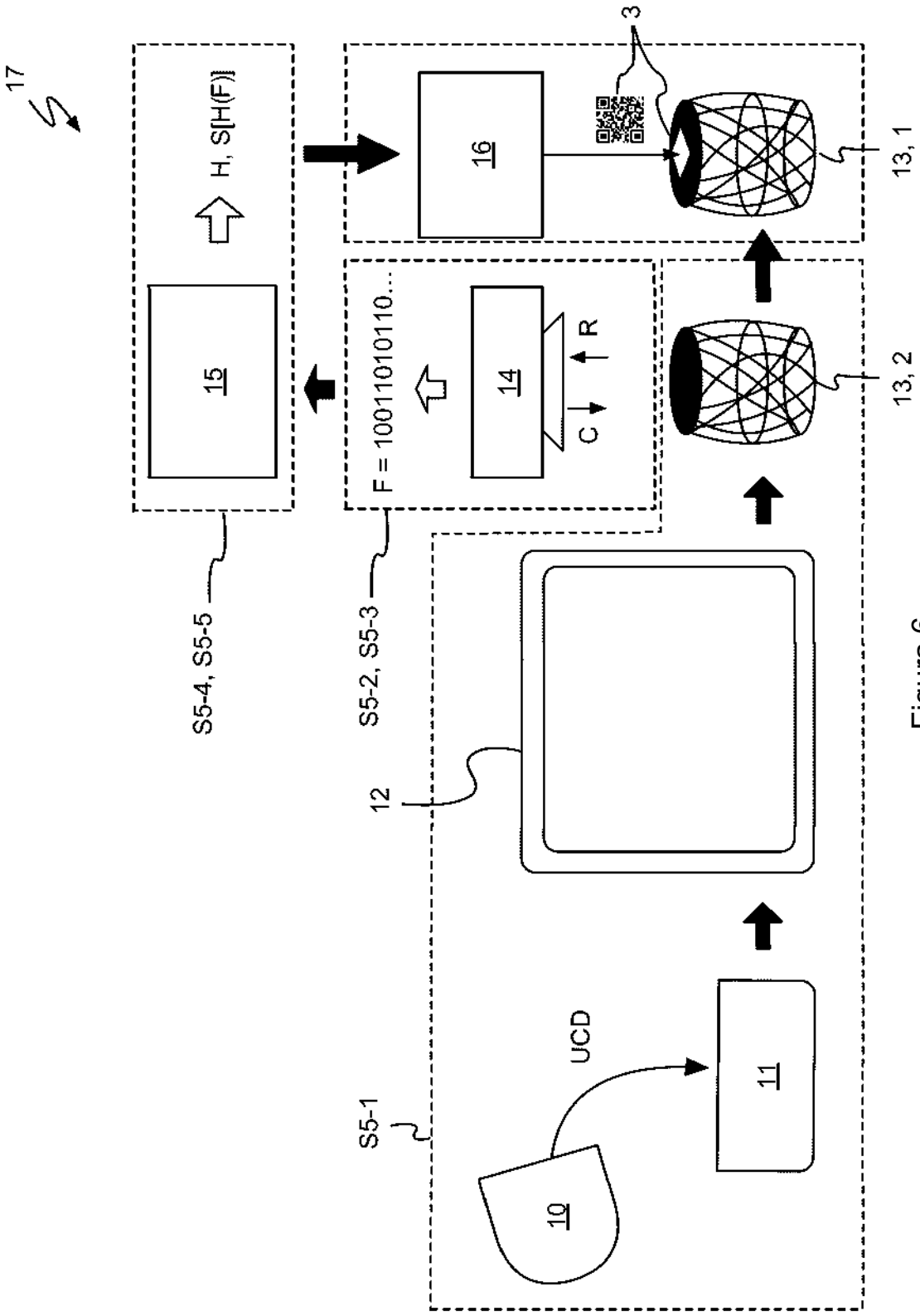
17
H, S[H(F)]
15
16
3
13, 1
F = 1001101011O...
14
R
C
13, 2
S5-4, S5-5
S5-2, S5-3
12
S5-1
UCD
11
10

Figura 6

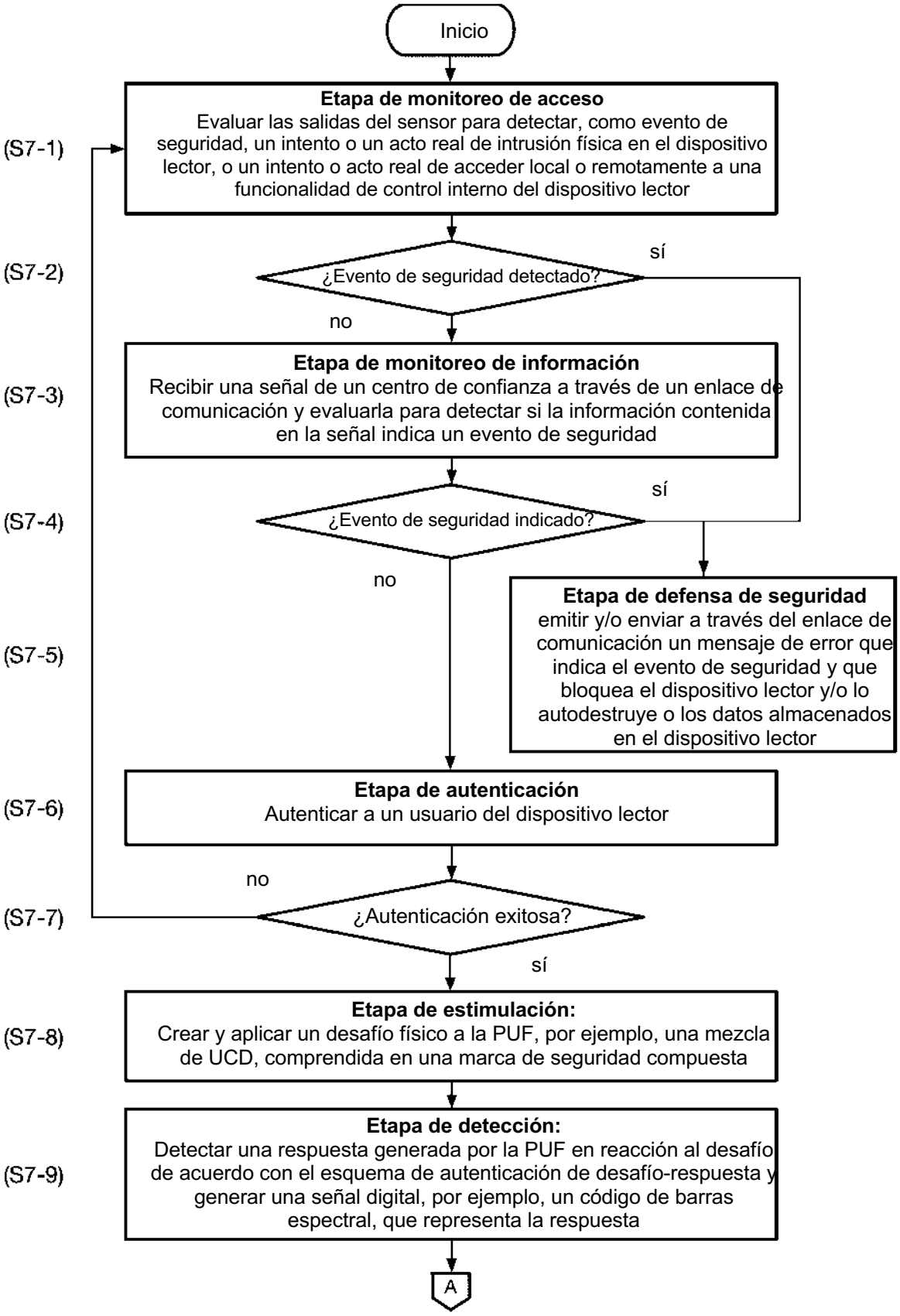
Inicio
(S7-1)
Etapa de monitoreo de acceso
Evaluar las salidas del sensor para detectar, como evento de seguridad, un intento o un acto real de intrusión física en el dispositivo lector, o un intento o acto real de acceder local o remotamente a una funcionalidad de control interno del dispositivo lector
(S7-2)
¿Evento de seguridad detectado?
sí
no
(S7-3)
Etapa de monitoreo de información
Recibir una señal de un centro de confianza a través de un enlace de comunicación y evaluarla para detectar si la información contenida en la señal indica un evento de seguridad
(S7-4)
¿Evento de seguridad indicado?
sí
no
(S7-5)
Etapa de defensa de seguridad
emitir y/o enviar a través del enlace de comunicación un mensaje de error que indica el evento de seguridad y que bloquea el dispositivo lector y/o lo autodestruye o los datos almacenados en el dispositivo lector
(S7-6)
Etapa de autenticación
Autenticar a un usuario del dispositivo lector
no
(S7-7)
¿Autenticación exitosa?
sí
(S7-8)
Etapa de estimulación:
Crear y aplicar un desafío físico a la PUF, por ejemplo, una mezcla de UCD, comprendida en una marca de seguridad compuesta
(S7-9)
Etapa de detección:
Detectar una respuesta generada por la PUF en reacción al desafío de acuerdo con el esquema de autenticación de desafío-respuesta y generar una señal digital, por ejemplo, un código de barras espectral, que representa la respuesta
A

FIGURA 7A

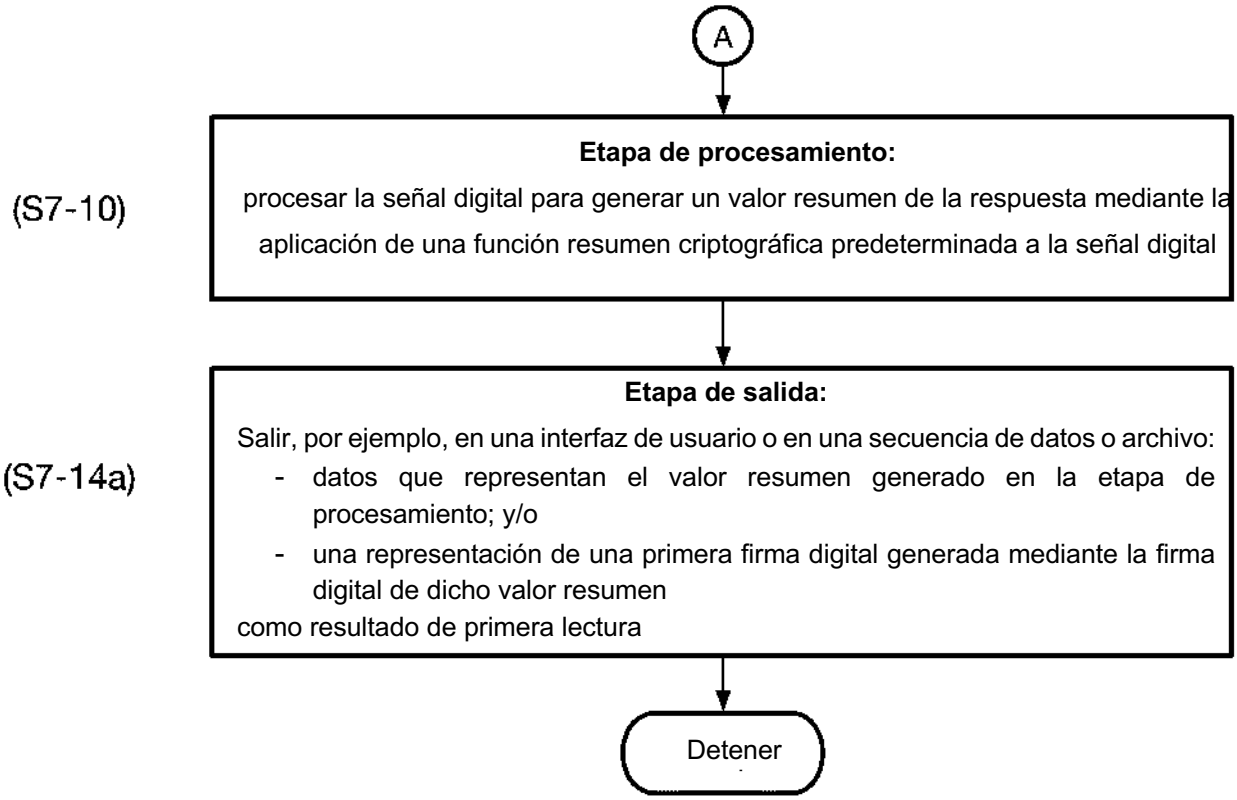
A
Etapa de procesamiento:
procesar la señal digital para generar un valor resumen de la respuesta mediante la aplicación de una función resumen criptográfica predeterminada a la señal digital
(S7-10)
Etapa de salida:
Salir, por ejemplo, en una interfaz de usuario o en una secuencia de datos o archivo:
- datos que representan el valor resumen generado en la etapa de procesamiento; y/o
- una representación de una primera firma digital generada mediante la firma digital de dicho valor resumen
como resultado de primera lectura
(S7-14a)
Detener

FIGURA 7B

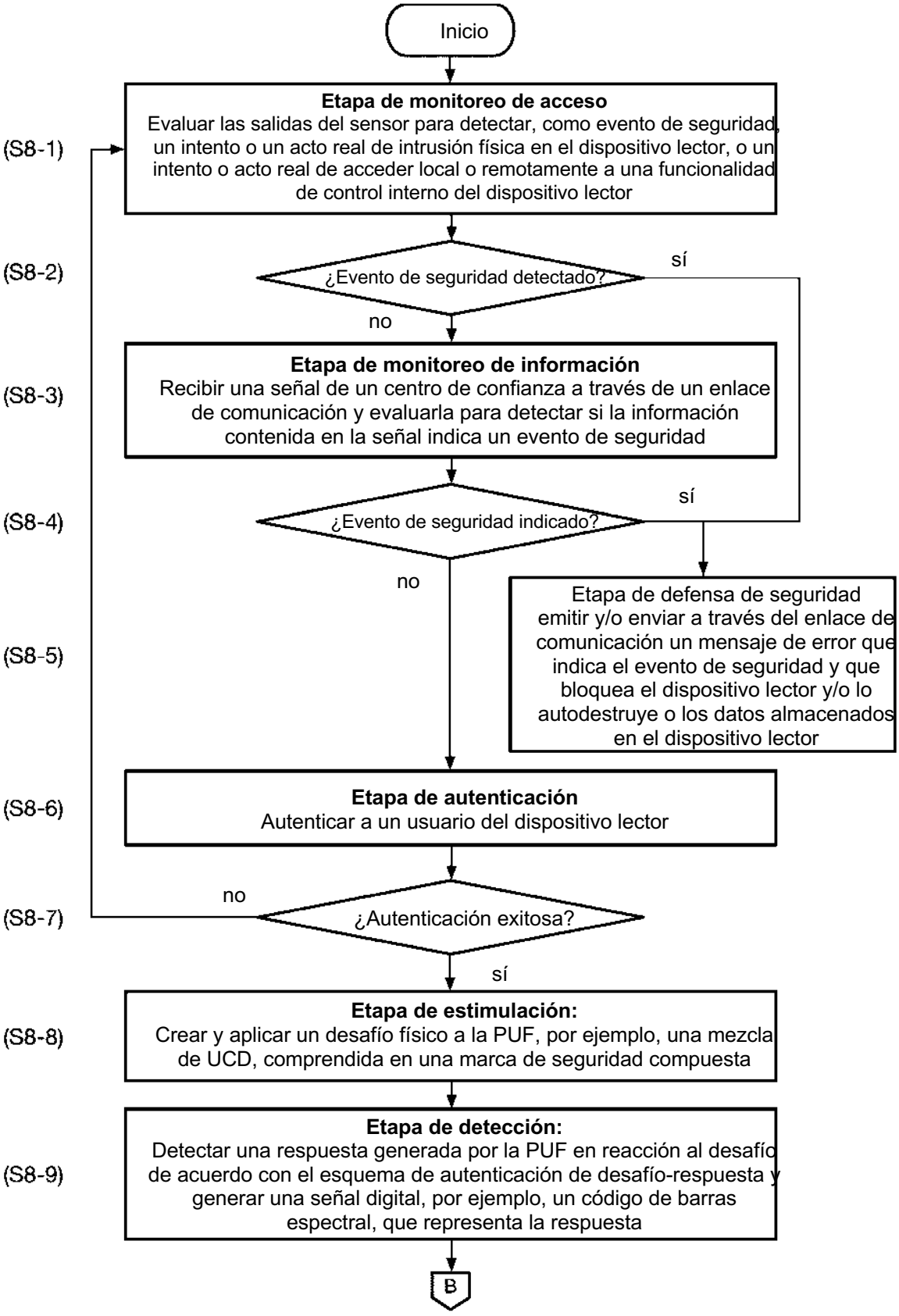
Inicio
(S8-1)
Etapa de monitoreo de acceso
Evaluar las salidas del sensor para detectar, como evento de seguridad, un intento o un acto real de intrusión física en el dispositivo lector, o un intento o acto real de acceder local o remotamente a una funcionalidad de control interno del dispositivo lector
(S8-2)
¿Evento de seguridad detectado?
sí
no
(S8-3)
Etapa de monitoreo de información
Recibir una señal de un centro de confianza a través de un enlace de comunicación y evaluarla para detectar si la información contenida en la señal indica un evento de seguridad
(S8-4)
¿Evento de seguridad indicado?
sí
no
(S8-5)
Etapa de defensa de seguridad
emitir y/o enviar a través del enlace de comunicación un mensaje de error que indica el evento de seguridad y que bloquea el dispositivo lector y/o lo autodestruye o los datos almacenados en el dispositivo lector
(S8-6)
Etapa de autenticación
Autenticar a un usuario del dispositivo lector
(S8-7)
no
¿Autenticación exitosa?
sí
(S8-8)
Etapa de estimulación:
Crear y aplicar un desafío físico a la PUF, por ejemplo, una mezcla de UCD, comprendida en una marca de seguridad compuesta
(S8-9)
Etapa de detección:
Detectar una respuesta generada por la PUF en reacción al desafío de acuerdo con el esquema de autenticación de desafío-respuesta y generar una señal digital, por ejemplo, un código de barras espectral, que representa la respuesta
B

FIGURA 8A

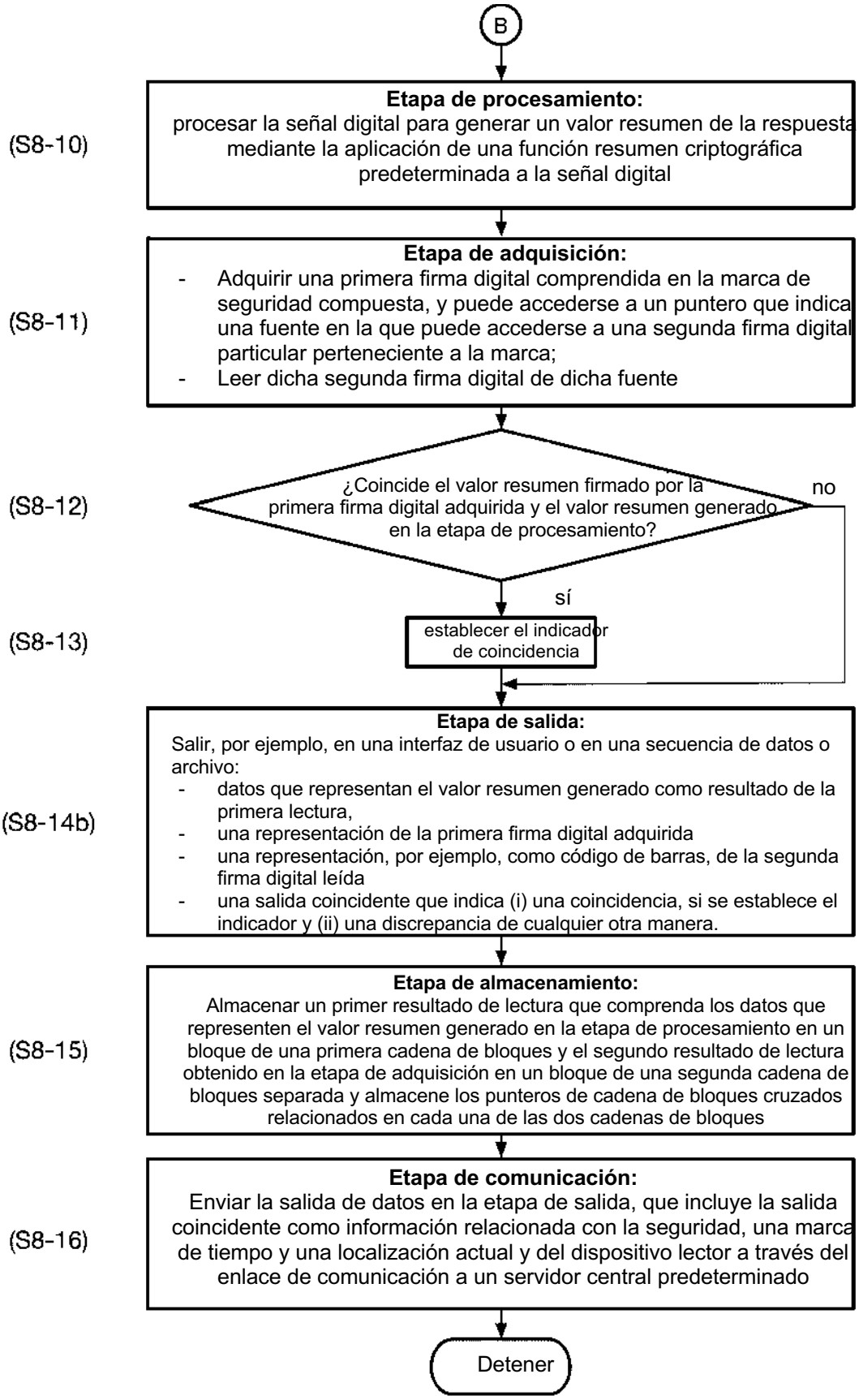
B
(S8-10)
Etapa de procesamiento:
procesar la señal digital para generar un valor resumen de la respuesta mediante la aplicación de una función resumen criptográfica predeterminada a la señal digital
(S8-11)
Etapa de adquisición:
- Adquirir una primera firma digital comprendida en la marca de seguridad compuesta, y puede accederse a un puntero que indica una fuente en la que puede accederse a una segunda firma digital particular perteneciente a la marca;
- Leer dicha segunda firma digital de dicha fuente
(S8-12)
¿Coincide el valor resumen firmado por la primera firma digital adquirida y el valor resumen generado en la etapa de procesamiento?
no
sí
(S8-13)
establecer el indicador de coincidencia
(S8-14b)
Etapa de salida:
Salir, por ejemplo, en una interfaz de usuario o en una secuencia de datos o archivo:
- datos que representan el valor resumen generado como resultado de la primera lectura,
- una representación de la primera firma digital adquirida
- una representación, por ejemplo, como código de barras, de la segunda firma digital leída
- una salida coincidente que indica (i) una coincidencia, si se establece el indicador y (ii) una discrepancia de cualquier otra manera.
(S8-15)
Etapa de almacenamiento:
Almacenar un primer resultado de lectura que comprenda los datos que representen el valor resumen generado en la etapa de procesamiento en un bloque de una primera cadena de bloques y el segundo resultado de lectura obtenido en la etapa de adquisición en un bloque de una segunda cadena de bloques separada y almacene los punteros de cadena de bloques cruzados relacionados en cada una de las dos cadenas de bloques
(S8-16)
Etapa de comunicación:
Enviar la salida de datos en la etapa de salida, que incluye la salida coincidente como información relacionada con la seguridad, una marca de tiempo y una localización actual y del dispositivo lector a través del enlace de comunicación a un servidor central predeterminado
Detener

FIGURA 8B

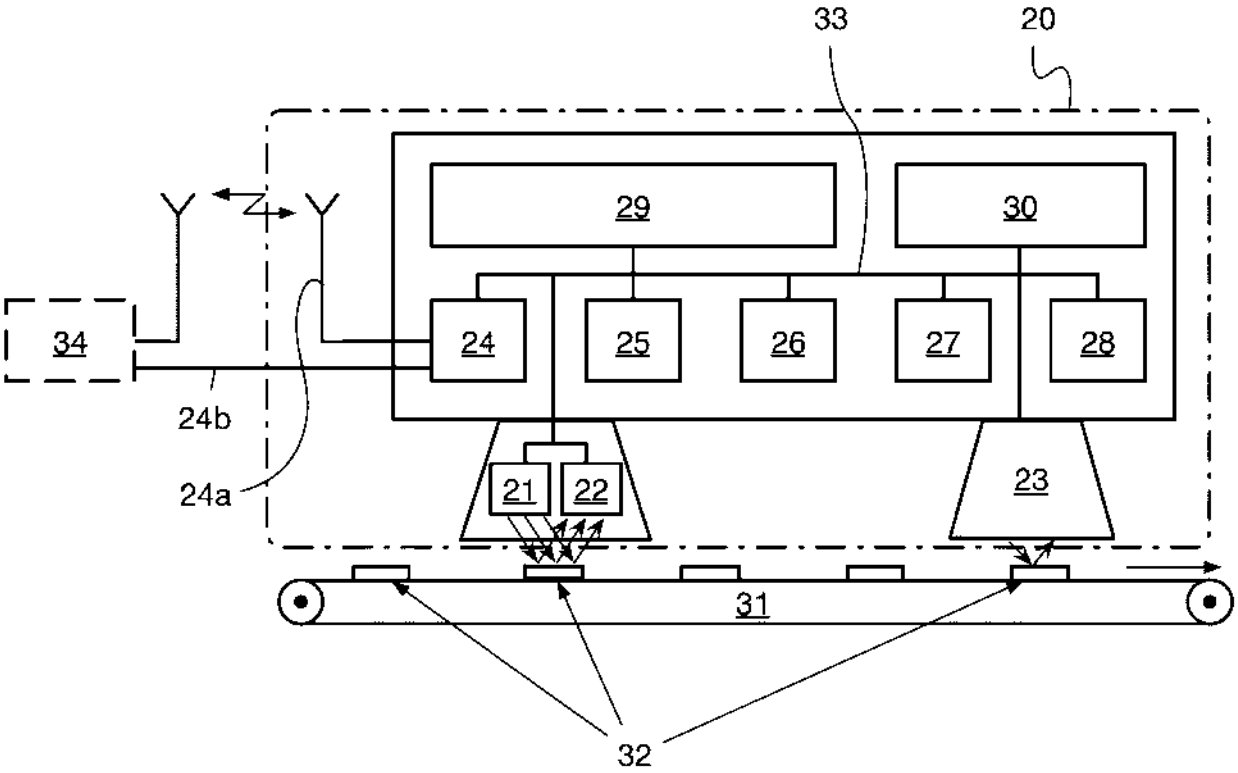

Figura 9

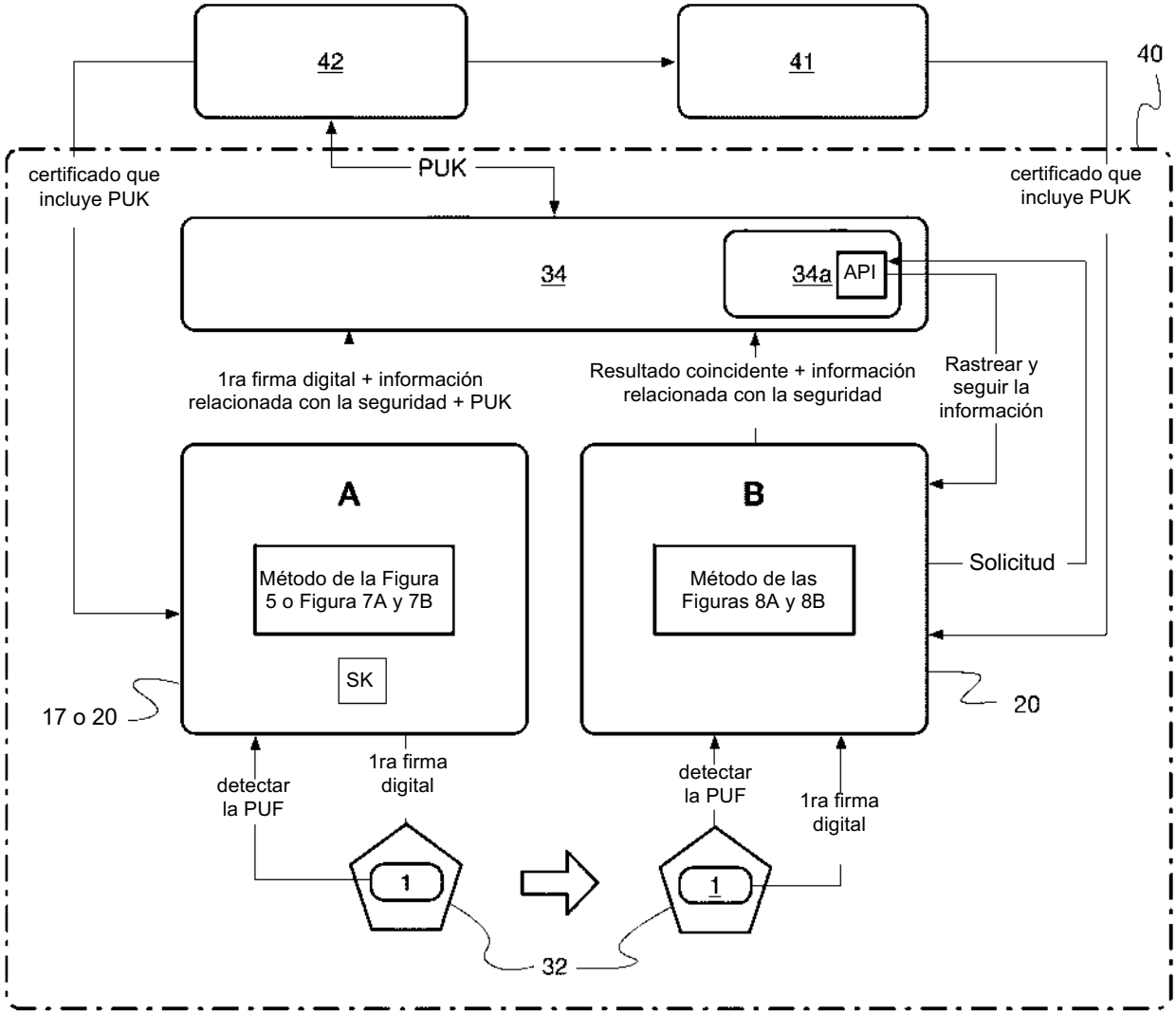
42
41
40
certificado que incluye PUK
PUK
certificado que incluye PUK
34
34a
API
1ra firma digital + información relacionada con la seguridad + PUK
Resultado coincidente + información relacionada con la seguridad
Rastrear y seguir la información
A
B
Método de la Figura 5 o Figura 7A y 7B
Método de las Figuras 8A y 8B
Solicitud
SK
17 o 20
20
detectar la PUF
1ra firma digital
detectar la PUF
1ra firma digital
1
1
32

Figura 10

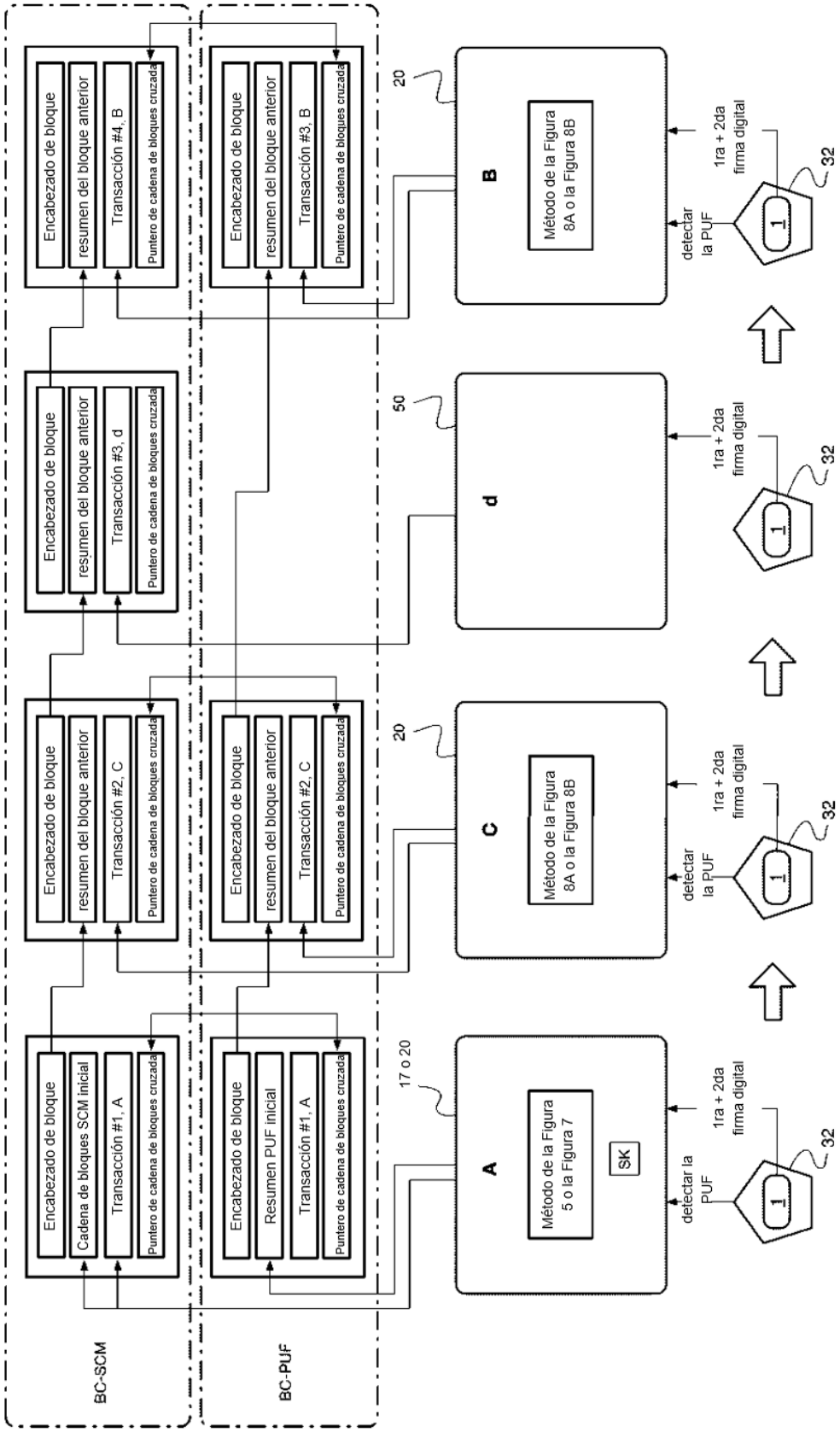
BC-SCM
BC-PUF
Encabezado de bloque
Cadena de bloques SCM inicial
Resumen PUF inicial
resumen del bloque anterior
Transacción #1, A
Transacción #2, C
Transacción #3, d
Transacción #3, B
Transacción #4, B
Puntero de cadena de bloques cruzada
17 o 20
20
50
A
B
C
d
Método de la Figura 5 o la Figura 7
Método de la Figura 8A o la Figura 8B
SK
detectar la PUF
1ra + 2da firma digital
1
32

Figura 11