(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 632 958**

(51) Int. CI.:

G06F 21/60 (2013.01)
G06F 21/86 (2013.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.06.2008 PCT/IB2008/052282**

(87) Fecha y número de publicación internacional: **18.12.2008 WO08152577**

(96) Fecha de presentación y número de la solicitud europea: **10.06.2008 E 08763275 (8)**

(97) Fecha y número de publicación de la concesión europea: **24.05.2017 EP 2174255**

(54) Título: **Método y dispositivo para proporcionar seguridad digital**

(30) Prioridad:

14.06.2007 EP 07110236

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.09.2017

(73) Titular/es:

INTRINSIC ID B.V. (100.0%)
HIGH TECH CAMPUS 9
5656 AE EINDHOVEN, NL

(72) Inventor/es:

KURSAWE, KLAUS y
TUYLS, PIM, T.

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y dispositivo para proporcionar seguridad digital

Campo de la invención

La presente invención se refiere a proporcionar seguridad digital, y más particularmente a proporcionar seguridad digital por medio de una función física inclonable y reconfigurable, “PUF”.

Antecedentes de la invención

Almacenar información digital en un dispositivo de una forma segura e invulnerable a falsificaciones que sea resistente a los ataques físicos es difícil y caro. Las funciones físicas inclonables (PUF) se han propuesto como una forma efectiva en coste de almacenar información de forma inclonable. Las PUF se introdujeron primero por Pappu como una forma de generar claves seguras para finalidades criptográficas. Una PUF puede componerse de un sistema físico complejo con muchos componentes aleatoriamente distribuidos. La información está contenida en una pieza de material barata, producida aleatoriamente, altamente complicada, y la información se lee mediante la realización de mediciones físicas sobre la PUF y la realización de algunos cálculos adicionales.

La ventaja de las PUF sobre almacenamiento electrónico se basa en los siguientes hechos: 1) dado que consisten en muchos componentes aleatorios, es prácticamente imposible realizar una copia física, 2) las PUF proporcionan una evidencia de falsificación inherente debido a su sensibilidad a cambios en las condiciones de medición, y 3) el borrado de datos es automático si se daña la PUF por una sonda dado que responderán de modo diferente a los estímulos aplicados a ellas.

Dado que una PUF no puede copiarse o modelizarse, es inclonable, y por ello una clave que se controle por una PUF no puede entregarse al exterior o copiarse. Esto hace las PUF atractivas como medida de protección contra ataques basados en la copia del material clave (ataque a la estación de origen) y para sistemas de gestión de derechos digitales (DRM).

La seguridad de una memoria no volátil es un bloque constructivo importante en el diseño de un hardware seguro, y normalmente no hay una solución funcional para ofrecer una protección adecuada contra un atacante de alto nivel. Mientras que la memoria estática puede asegurarse directamente mediante el uso de una PUF, esto no es posible hasta el momento para memorias dinámicas. Dichas memorias son necesarias por ejemplo para comprobadores de suma, contadores, y claves criptográficas actualizables.

El documento WO 2007/031908 A2 divulga dispositivos de función física inclonable para la determinación de la autenticidad de un artículo, sistemas para determinación de la autenticidad de un artículo físico, y métodos para determinación de la autenticidad de un artículo. Un patrón de la función física inclonable del dispositivo de función física inclonable se daña cuando se usa el artículo por primera vez.

En el documento “Extracting Secret Keys from Integrated Circuits”, por Daihyun Lim, Massachusetts Institute of Technology, mayo de 2004, se presenta la forma de mejorar una PUF mediante la introducción de un grado de dinamicidad. En el documento Lim describe una PUF reconfigurable, que se implementa en un sistema físico que comprende un circuito integrado. La característica de retardo de la PUF se cambia por medio del desplazamiento de la tensión de umbral de un transistor de puerta flotante. El desplazamiento es provocado por el cambio de la cantidad de carga en la puerta flotante. Este desplazamiento cambia el retardo del transistor, y por ello la característica de retardo de toda la PUF. Esta clase de técnica anterior de capacidad de reconfiguración se basa en el procedimiento de almacenar un valor diferente en un registro programable, en donde el transistor de puerta flotante representa el registro. Desafortunadamente, esto no es tan seguro como sería deseable, dado que un atacante puede conseguir leer el valor del registro o la señal que cambia el valor. Entonces el atacante será capaz de reponer el valor a su estado antiguo. Otro ataque posible es reponer el valor a cero por medio de hardware antes de que se use por primera vez la PUF. Es deseable mejorar la operación de reconfiguración para incrementar la seguridad.

Sumario de la invención

Es un objetivo de la presente invención proporcionar una forma segura e invulnerable a falsificaciones para proporcionar seguridad digital y almacenamiento de datos dinámicos que alivie los inconvenientes anteriormente mencionados de la técnica anterior tal como se ha descrito anteriormente.

Estos objetivos se consiguen mediante un método y un dispositivo para proporcionar seguridad digital por medio de una función física inclonable y reconfigurable, de acuerdo con la presente invención tal como se define en las reivindicaciones 1 y 18, respectivamente.

Cuando se implementan la RPUF en un CI o similar y se utilizan las respuestas aleatorias inherentes de la RPUF, y

se combina esto con la capacidad para reconfigurar la RPUF, se ofrece un almacenamiento barato y seguro que puede usarse para autenticar información dinámica en hardware seguro. La implementación de una función nueva, diferente por la RPUF permite numerosos casos de nuevo uso. Más destacable es la capacidad para asegurar datos dinámicos, tales como contadores seguros, comprobadores de suma, claves criptográficas actualizables, o información de configuración, o semillas para generadores de números pseudoaleatorios y otros datos críticos de seguridad.

Estos y otros aspectos, características y ventajas de la invención serán evidentes a partir de y clarificados con referencia a las realizaciones descritas a continuación en el presente documento.

Breve descripción de los dibujos

La invención se describirá ahora con más detalle y con referencia a los dibujos adjuntos en los que:

la Fig. 1 ilustra un dibujo esquemático de una función física inclonable y reconfigurable de acuerdo con la presente invención;
la Fig. 2 es un diagrama de flujo de acuerdo con una realización de la presente invención;
la Fig. 3 es un diagrama de flujo de acuerdo con una realización del método para proporcionar seguridad digital cuando se usa para proporcionar almacenamiento de datos seguro; y
la Fig. 4 ilustra una realización del dispositivo para proporcionar seguridad digital de acuerdo con la presente invención.

Descripción de realizaciones preferidas

El concepto de una función física inclonable (PUF) y reconfigurable se ilustra en el dibujo esquemático tal como se muestra en la Fig. 1. Una PUF reconfigurable (100), que se designa en lo que sigue del presente documento como una RPUF, está constituida por componentes físicos tales como moléculas o cadenas poliméricas que se distribuyen de modo único para la RPUF individual. La evaluación de una RPUF se realiza mediante el sometimiento de la RPUF a uno o más estímulos, es decir señales eléctricas que se aplican a la PUF. La respuesta de una RPUF a un cierto estímulo es, debido a la compleja física que gobierna la interacción entre la RPUF y el estímulo, aparentemente aleatoria. Por ello, cuando se aplica un estímulo c a la RPUF (100) en un punto específico en la RPUF puede medirse una primera respuesta r_1. A continuación se aplica una acción externa, X en la Fig. 1, de modo que los componentes de la RPUF se redistribuyen o reconfiguran. A continuación, cuando se aplica el mismo estímulo c, en el mismo punto específico, se mide una segunda respuesta r_2.

En la Fig. 2 se muestra un diagrama de flujo para una realización del método para proporcionar seguridad digital. El método de acuerdo con la presente invención se inicia en la etapa 200, en la que se proporciona una RPUF 100 tal como se describe en la Fig. 1. La RPUF se configura preferentemente en este punto para utilizarse como almacenamiento de alguna información, como por ejemplo una clave que puede usarse para cifrado. Si se decide, en la etapa 215, que ya no se requiere la información almacenada en la RPUF el método continúa en la etapa 210, en la que se realiza una reconfiguración de la RPUF, en la que los componentes de la RPUF se redistribuyen de tal manera que ya no tienen el mismo comportamiento estímulo-respuesta que la RPUF original.

En una realización del método la etapa 210 que comprende la etapa de aplicar una fuerza externa, etapa 211, y dependiendo de la realización específica, es decir de cómo está constituida la RPUF, la fuerza externa puede ser al menos una de entre tensión, presión, luz láser, radiación, partículas y calor exteriores.

En una realización alternativa el método comprende adicionalmente etapas para proporcionar datos de traducción. Esta es una clase de datos de ayuda que se describen para aplicaciones PUF de la técnica anterior. Los datos de ayuda, o información secundaria, son datos asociados a un estímulo y respuesta, que se almacenan normalmente juntos con el par estímulo y respuesta para ayuda y se proporcionan normalmente, en aplicaciones PUF de la técnica anterior, para mejorar la fiabilidad de respuesta de la PUF. Sin embargo, de acuerdo con la presente invención los datos de traducción se usan en diferentes maneras que no deberían confundirse con datos de ayuda ordinarios.

En una realización de acuerdo con la invención los datos de traducción se usan para traducir una respuesta desde un cierto estímulo recibido en una RPUF reconfigurada en la respuesta esperada para el mismo estímulo según se recibe desde la RPUF original antes de la reconfiguración.

En una realización alternativa los datos de traducción se usan adicionalmente para calcular nuevos datos de traducción. Esto es, en esta realización, después de la reconfiguración de la RPUF, la nueva respuesta desde la RPUF se traduce en una respuesta traducida tal como se esperaba desde la RPUF original, no la respuesta original en sí. Por ello, los nuevos datos de traducción deben contener los datos de traducción originales.

La etapa 200, como se ha descrito anteriormente, es seguida en este caso por la etapa 201. En esta realización la RPUF se evalúa en uno o más puntos cruciales. Para una evaluación completa deberían evaluarse todos los puntos,

pero esto no es muy práctico y no es necesario en la mayor parte de los casos. En la etapa 201 la RPUF se estimula con un primer estímulo c en un punto p, es decir se suministra una señal de estímulo en el punto p sobre la RPUF. En la etapa 202 se obtiene la respuesta r1 para el estímulo c mediante la medición de la señal de respuesta de acuerdo con alguna técnica anterior. La respuesta r1 se almacena en la etapa 203. Continuando en la etapa 204 el método comprende la generación de datos de traducción w para el punto p, datos de traducción w que se basan en el primer estímulo c y en la respuesta r1. Estos datos se almacenan entonces en la etapa 205. El almacenamiento de las etapas 203 y 205 se realiza preferentemente en una memoria temporal (protegida). Las etapas 201 a 205 se realizan para todos los puntos cruciales de la RPUF. Tras la valoración de la RPUF, el procedimiento continúa en la etapa 210, en la que se reconfigura la RPUF. La reconfiguración se describe con más detalle en la sección que cubre la descripción del dispositivo de acuerdo con la presente invención.

En una realización alternativa los datos de traducción que se generan en la etapa 204 se codifican de acuerdo con una forma previamente conocida para almacenamiento.

En otra realización del método de acuerdo con la presente invención, la etapa de reconfiguración 210 es seguida por la etapa 221. La RPUF reconfigurada es estimulada ahora en los mismos puntos que la RPUF original. Así, en la etapa 221, la RPUF es estimulada con un primer estímulo c en al menos un punto p seguida por la etapa de medición de la respuesta r2 en la etapa 222. En la siguiente etapa, etapa 223, la segunda respuesta r2 se transforma en la respuesta igual a r1 desde la RPUF original usando los datos de traducción w almacenados. Esto es, la evaluación de la RPUF previamente a la reconfiguración y almacenamiento de los datos de traducción asociados a un cierto punto y estímulo ayuda a la transformación de una respuesta producida en la RPUF reconfigurada en una respuesta igual a la producida por la RPUF original. Esto se realiza almacenando la RPUF una máscara XOR en una NVRAM no segura. La RPUF se estimula para dar una respuesta y la respuesta se somete a la función XOR junto con la máscara. El conocimiento de la máscara no da a un atacante ninguna ventaja si la respuesta correspondiente no es conocida, de modo que no hay necesidad de almacenamiento seguro de la máscara. Para generar los nuevos datos de traducción, se calcula la diferencia entre la respuesta de la RPUF nueva y original (es decir con la XOR entre ellas). La diferencia entonces el somete a la función XOR con los datos de traducción antiguos, dando como resultado nuevos datos de traducción, que traducirán la nueva respuesta desde la RPUF en lo que se tradujo la respuesta original desde la RPUF.

En otra realización de acuerdo con la presente invención los datos de traducción w, estímulo c se almacenan usando una segunda RPUF reconfigurable para incrementar la seguridad, cuando no se tienen que almacenar los datos en una memoria no segura.

De acuerdo con una realización del método para proporcionar seguridad digital, la intención del método es proporcionar almacenamiento seguro de una clave K, véase la Fig. 3. En este caso la RPUF se estimula primero con un primer estímulo c en la etapa 201. A continuación se obtiene y almacena (temporalmente) una primera respuesta r1, etapas 202 y 203. Posteriormente se obtiene una clave aleatoria en la etapa 300. Esto puede realizarse estimulando la RPUF con un estímulo en un punto y usando la respuesta como una clave o puede proporcionarse externamente. Se generan a continuación datos de traducción w' en la etapa 304 basándose en la primera respuesta r1 y la clave aleatoria s. En la etapa 305 la clave K que se ha de almacenar se cifra usando la clave aleatoria s. Se almacena entonces la clave cifrada Es(K), en la etapa 306, junto con los datos de traducción w' y el estímulo c en un almacenamiento, que en esta realización es no seguro. Cuando se accede a la clave, en la etapa 307, la RPUF se estimula con el estímulo c que se recupera desde el almacenamiento, y esta etapa es seguida por la etapa 322, en la que se mide la respuesta r1. La clave aleatoria s se reconstruye ahora en la etapa 323 usando dicha respuesta medida r1 y los datos de traducción w' que se recuperan del almacenamiento. Finalmente se recupera del almacenamiento la clave cifrada Es(K) y se descifra en la etapa 324 usando la clave aleatoria s reconstruida. La clave K se almacena ahora temporalmente y está disponible para su uso, etapa 325. Para hacerlo difícil para un atacante la clave K se vuelve a cifrar tras su uso. Esto tiene lugar después de la etapa de reconfiguración 210 y las etapas 221 y 222 que siguen después de la reconfiguración de la RPUF como se ha descrito anteriormente. En la etapa 326, se genera una segunda clave aleatoria s2 usando la segunda respuesta r2 tal como se ha obtenido en la etapa 222, segunda clave aleatoria s2 que se usa para volver a cifrar la clave K, Es2(K) en la etapa 327. La segunda clave aleatoria s2 y dicha clave cifrada de nuevo Es2(K) se almacenan ahora en el almacenamiento (que puede ser un almacenamiento no seguro).

En una realización alternativa los segundos datos de traducción w2 se generan en la etapa 328 usando el estímulo c recuperado y la segunda respuesta r2, w2 que se usa para generar la segunda clave aleatoria s2.

La Fig. 4 ilustra una realización del dispositivo 400 para proporcionar seguridad digital de acuerdo con la presente invención. El dispositivo comprende una RPUF 100, que está preferentemente integrada en un CI para proporcionar un almacenamiento digital seguro.

Adicionalmente, el dispositivo 400 comprende una unidad de estímulo 410 para proporcionar estímulos a la RPUF 100, unidad de estímulo 410 que se implementa en este caso con un generador de señal 410, una unidad detectora 420, que se dispone para medir respuestas desde la RPUF 100. Las señales de salida desde la unidad de estímulo 410 y unidad detectora 420 se conectan a una unidad de procesamiento 440, que se dispone para recibir los datos

de estímulo y los datos de respuesta y procesar estos datos de acuerdo con los métodos descritos anteriormente y las aplicaciones específicas, que se explicarán adicionalmente a continuación. Las funciones realizadas por las unidades en el dispositivo 400 pueden combinarse en un procesador o pueden dividirse adicionalmente entre varios procesadores tales como procesadores de señales digitales y/o realizarse por hardware dedicado tal como circuitos integrados de aplicación específica ASIC, por ejemplo electrónica o circuitos lógicos cableados o dispositivos lógicos programables, u otras implementaciones en hardware o software.

Adicionalmente, el dispositivo 400 comprende una unidad de almacenamiento 450, que se implementa en este caso con una EEPROM, pero en realizaciones alternativas la unidad de almacenamiento se implementa con una RPUF o una PUF o cualquier dispositivo de memoria de la técnica anterior adecuado. En este caso, la unidad de almacenamiento puede elegirse finalmente para protegerse o para la elección de realizaciones menos caras que consisten en variantes de memoria no seguras ordinarias.

El dispositivo contiene una unidad de reconfiguración 430. La unidad de reconfiguración se diseña para proporcionar la acción externa que reconfigurará la RPUF 100 empleada.

El dispositivo 400 se proporciona adicionalmente con un medio de control 470, que controla las unidades que están contenidas dentro del dispositivo 400.

Se dispone una unidad de entrada/salida de datos 460 en el dispositivo 400 para la introducción de datos desde una fuente externa y para la salida de datos a la fuente externa.

En una realización del dispositivo de acuerdo con la presente invención la RPUF 100 se implementa mediante el uso de una PUF óptica normal que consiste en un material transparente que contiene partículas de dispersión de luz aleatoriamente distribuidas, partículas que constituyen los componentes distribuidos de la RPUF. En una realización alternativa la PUF óptica se provee adicionalmente con una capa reflectora alrededor de ella.

En realizaciones en las que la RPUF 100 se realiza con una PUF óptica normal la unidad de reconfiguración 430 se proporciona con un elemento de calentamiento para aplicar calor a la RPUF 100, lo que conducirá a una redistribución de las partículas de dispersión de luz. En una realización alternativa el calor se aplica con una fuente radiante, por ejemplo una lámpara de infrarrojos o un láser de infrarrojos. En una realización alternativa la unidad de reconfiguración 430 se proporciona con medios para aplicar mecánicamente tensiones a la RPUF 100, lo que puede conducir a la redistribución de las partículas de dispersión de luz de la PUF 100 óptica.

Cuando se usa una PUF óptica normal, la RPUF 100, el estímulo aplicado a la RPUF 100 y la respuesta medida desde la RPUF 100 se obtienen proporcionando a la unidad de estímulo 410 una fuente láser para exponer a la RPUF 100 a un haz láser incidente y disponer la unidad detectora 420 para medir la respuesta de luz correspondiente, es decir un patrón de luz moteado, desde la RPUF 100.

En una realización del dispositivo de acuerdo con la presente invención la RPUF 100 se realiza mediante el uso de una PUF de degradación, tal como una PUF óptica fabricada de plástico o algún polímero que cambia sus propiedades con el tiempo cuando es influido por, por ejemplo, operaciones de lectura sobre la RPUF 100. Cuando se aplica una luz láser al material plástico durante demasiado tiempo, el plástico se deforma y la distribución de las partículas de dispersión de luz cambia involuntariamente, incluso cuando no se pretende reconfiguración para la RPUF 100. Cuando se usa una PUF de degradación el dispositivo funciona de acuerdo con el método usando datos de traducción para la traducción de las nuevas respuestas en las antiguas tal como ya se ha descrito anteriormente.

En una realización alternativa del dispositivo de acuerdo con la presente invención, la RPUF se realiza como un recubrimiento que contiene muchas partículas aleatoriamente distribuidas con diferentes constantes dieléctricas. Las respuestas se obtienen por medio de mediciones de la capacidad del recubrimiento. Esta RPUF se reconfigura mediante la redistribución de las partículas por medio de tensiones mecánicas o calor.

En una realización del dispositivo de acuerdo con la presente invención, se usa otro tipo de RPUF, en la que los componentes distribuidos de la RPUF se realizan por medio de bits cuánticos, cúbits. La RPUF se realiza como sigue. Un cúbit tiene la propiedad de que tiene dos bases (normalmente llamadas las bases *X* y *Z*) y en cada base hay dos estados perfectamente distinguibles, denominados usualmente como los estados *arriba* y *abajo*. De modo que el cúbit puede configurarse en una base (*X* o *Z*) y en cada base en un estado, *arriba* o *abajo*. Para cada uno de los estados se conecta un bit clásico, por ejemplo: *arriba*: 1 y *abajo*: 0.

Suponiendo que se configura un cúbit en el estado *arriba* en la base *X*, si el cúbit se mide en la base *X*, la medición devuelve el estado *arriba* y por ello el valor de 1; sin embargo cuando se mide en la base *Z*, la base complementaria de aquella en la que se configuró, la medición devuelve 0 o 1 con una probabilidad del 50 %. Esto es consecuencia del hecho de que el estado del cúbit ha colapsado aleatoriamente en el estado *arriba* y *abajo* en la base *Z*. Para ser capaz de usar el cúbit para almacenamiento de información, los estímulos, es decir el anuncio de la base en la que han de medirse, ha de almacenarse en la memoria 450 en el dispositivo 400.

Así, la medición de la RPUF 100 en la base complementaria provocará que los cúbits se redistribuyan de modo impredecible en la nueva base en el estado *arriba* o *abajo*, y por ello la RPUF se reconfigura. El nuevo estímulo que consiste en las nuevas bases en las que se han de medir los cúbits sustituye al estímulo antiguo.

En lo que sigue, la intención del dispositivo es almacenar una clave K con seguridad en la unidad de almacenamiento 450 del dispositivo 400. La clave K se suministra a través de la unidad de entrada/salida de datos 460. La RPUF 100 se usa como sigue. Durante la inscripción la unidad de estímulo 410 aplica un estímulo c a la RPUF 100 y se mide su respuesta r por la unidad detectora 420. A continuación se elige una clave aleatoria s, que se proporciona desde la unidad de entrada/salida de datos 460 o en realizaciones alternativas se recupera desde la unidad de almacenamiento 450 o se obtiene desde la RPUF mediante la aplicación de un estímulo arbitrario y la recepción de una respuesta que se usa como s, y se generan datos de traducción w por la unidad de procesamiento 440. A continuación se cifra la clave K en la unidad de procesamiento 440 con la cadena: Es(K). Este cifrado puede ser simplemente un cifrado de un paso. Finalmente, los datos de traducción w, el estímulo c y la Es(K) se almacenan en la unidad de almacenamiento 450 del CI, que se realiza con una EEPROM. Dado que esta unidad de almacenamiento 450 no es segura, un atacante tiene acceso a todos los datos almacenados en la EEPROM.

Para acceder a la clave K se realizan las siguientes etapas.

Los medios de estímulo 410 estimulan la RPUF con un estímulo c y la unidad detectora 420 mide su respuesta r'. La unidad de procesamiento 440 recupera los datos de traducción desde la EEPROM 450 y reconstruye s a partir de r' y w usando un algoritmo de datos de traducción (extractor Fuzzy). La unidad de procesamiento 440 recupera Es(K) desde la EEPROM 450. Usando s, la unidad procesadora 440 descifra Es(K) en K y la pone durante un tiempo tan corto como sea posible en alguna memoria volátil (por ejemplo RAM) (no mostrada). La unidad de procesamiento 440 comienza la realización de las operaciones de seguridad necesarias como por ejemplo operaciones criptográficas con la clave K. La unidad de reconfiguración 430 es instruida por los medios de control para reconfigurar la RPUF 100, usando el método apropiado que depende de la implementación específica de las RPUF descrita anteriormente.

A continuación, usando el estímulo c la unidad de estímulo 410 aplica un estímulo a la RPUF reconfigurada y se mide una nueva respuesta r1 por medio de la unidad de detección 420. La unidad procesadora 440 aplica entonces los datos de traducción w para generar una nueva clave s1. La clave K vuelve a cifrarse con la clave s1 y se almacena Es1(K) en la EEPROM 450. La clave K se retira de la memoria volátil (no mostrada) tan pronto como sea posible, es decir a partir de ese punto en el tiempo cuando ya no es necesaria.

En una realización alternativa pueden generarse nuevos datos de traducción w1 en la unidad de procesamiento 440 para construir una nueva clave s1.

En una realización alternativa la RPUF 100 consiste en dos sistemas físicos individuales RPUF1 y RPUF2. Las funcionalidades del dispositivo de acuerdo con la presente invención se llevan a cabo entonces usando RPUF1 y RPUF2. A continuación, las claves s, s1,… para cifrar la clave K, se integran la primera por la RPUF1, la siguiente por la RPUF2, la siguiente por la RPUF1. Esto tiene la ventaja de que para volver a cifrar la clave K, ya no tiene que ponerse K en una memoria no volátil fuera de las PUF, lo que es claramente más seguro. Esto es especialmente ventajoso si la operación queda interrumpida, por ejemplo debido a la pérdida de la alimentación eléctrica, dado que no se revelan claves o datos, y la operación puede continuarse fácilmente de nuevo. Véase la tabla 1, en la que se compara el uso de solo una RPUF y el uso de dos RPUF. Obsérvese también que la clave antigua s, que es con la que se cifró la clave K ya no existe y ya no puede construirse dado que la PUF ha sido reconfigurada.

Tabla 1. Una tabla para comparar las etapas para proporcionar claves y reconfiguración de la RPUF para un dispositivo o método para almacenamiento de datos con seguridad de acuerdo con la presente invención cuando se usa una RPUF, y dos RPUF respectivamente

Uso de una RPUF	Uso de dos RPUF, RPUF1 y RPUF2
Leer clave desde la RPUF Almacenar clave en RAM Reconfigurar RPUF Descifrar los datos con la clave desde la RAM Cifrar los datos con la nueva clave leída desde la RPUF reconfigurada	Reconfigurar la RPUF2 Crear la clave desde la RPUF1 Descifrar datos con la clave leída desde RPUF1 Cifrar los datos con la clave leída desde RPUF2 Reconfigurar la RPUF1

En una realización se usa el dispositivo 400 de acuerdo con la presente invención para proporcionar un contador seguro. Se cifra primero un valor del contador usando una clave derivada de la RPUF 100 de acuerdo con el método tal como se ha descrito anteriormente (etapa 300), y se almacena a continuación en la unidad de almacenamiento 450. Cuando el contador se incrementa/disminuye se realizan las siguientes funciones en el dispositivo 400:

- La unidad de procesamiento 440

    - recupera el valor del contador cifrado y el estímulo c desde el almacenamiento inseguro, EEPROM 450,
    - descifra el valor del contador cifrado usando la clave de RPUF que se obtiene mediante el estímulo de RPUF con c.

- La unidad de reconfiguración 430 reconfigura la RPUF 100.
- El valor del contador se incrementa/disminuye y se cifra usando una nueva clave de RPUF.
- El nuevo valor de contador cifrado se almacena en el almacenamiento inseguro, EEPROM 450.

Dado que las claves RPUF para descifrar los valores de contador antiguos nunca existen fuera de la RPUF, y se destruyen automáticamente cuando se reconfigura la RPUF, fallará cualquier ataque de reproducción sobre el contador. Cualquier dato dinámico, por ejemplo datos de configuración, valores de cifrado de datos críticos, y claves actualizables pueden asegurarse de forma similar tal como en las realizaciones descritas anteriormente.

Un caso de uso especial de la presente invención es la implementación de la norma TGG, en donde hardware seguro y barato necesita proporcionar todas las unidades anteriores del dispositivo 400. Especialmente el uso de una NVRAM segura es un aspecto crítico, dado que es el componente que determina los precios del hardware y un problema de seguridad principal.

En una realización alternativa, mediante el uso de dos PUF para la realización de las funcionalidades del dispositivo 400, es posible asegurar una cantidad arbitraria de memoria.

En una realización alternativa el dispositivo se usa como generador de semillas para un generador de números pseudoaleatorios mediante, después de que se realice la reconfiguración por la unidad de confederación 430, la aplicación de un estímulo a la RPUF 100 y la detección de la respuesta con la unidad de detención 420. A continuación se usa la respuesta como la semilla (alternativamente tras la realización de algún procesamiento de la señal sobre la respuesta en la unidad de procesamiento). De ahí que se utilice el hecho de que la respuesta desde la RPUF tras una reconfiguración es estadísticamente aleatoria.

Anteriormente, se han descrito realizaciones del método y dispositivo para proporcionar seguridad digital de acuerdo con la presente invención tal como se define en las reivindicaciones adjuntas. Estas deberían verse meramente como ejemplos no limitativos. Como se comprenderá por un experto en la materia, la invención se define solamente por el alcance de las reivindicaciones adjuntas. Se ha de observar que para las finalidades de la presente solicitud, y en particular con relación a la reivindicaciones adjuntas, la palabra “comprendiendo” no excluye otros elementos o etapas, que la palabra “un” o “una” no excluye una pluralidad, lo que per se será evidente para un experto en la materia.

REIVINDICACIONES

1. Un método para proporcionar seguridad digital por medio de una función física inclonable y reconfigurable, que comprende un sistema físico constituido por componentes distribuidos dispuestos para generar una primera respuesta cuando reciben un primer estímulo en un punto de dicho sistema físico, **caracterizado por**:

la etapa de reconfigurar físicamente dicha función física inclonable y reconfigurable mediante una unidad de reconfiguración, etapa que comprende la etapa de redistribuir dichos componentes de modo que generen una segunda respuesta, que difiere de dicha primera respuesta cuando se aplica de nuevo dicho primer estímulo en dicho punto afectando la reconfiguración física a la estructura física de la función física inclonable y reconfigurable, en donde dicha etapa de reconfiguración está condicionada por una etapa de determinación de si realizar o no una reconfiguración, estando constituido dicho acto de proporcionar seguridad digital por proporcionar almacenamiento seguro de un artículo digital, comprendiendo adicionalmente el método las etapas de:

obtener una primera clave aleatoria;
generar datos de traducción basándose en dicha primera respuesta de dicho primer estímulo en dicho punto y dicha primera clave aleatoria;
cifrar dicho artículo con dicha clave aleatoria;
almacenar los datos de traducción, dicho primer estímulo y dicho artículo cifrado;
acceder a dicho artículo previamente a la etapa de reconfigurar la función física inclonable y reconfigurable, en donde la etapa de acceder al artículo comprende las etapas de:

estimular la función física inclonable y reconfigurable con dicho estímulo almacenado;
medir una respuesta que corresponde al estímulo almacenado a partir de la función física inclonable y reconfigurable;
reconstruir dicha clave aleatoria usando dicha respuesta medida y dichos datos de traducción almacenados;
descifrar dicho artículo cifrado almacenado usando dicha clave aleatoria reconstruida, mediante lo cual dicho artículo está disponible para su uso.

2. Un método de acuerdo con la reivindicación 1, en el que dicha etapa de redistribución comprende la aplicación de una acción externa.

3. Un método de acuerdo con la reivindicación 2, en el que dicha acción externa es al menos una de entre tensión, presión, luz láser, radiación, partículas y calor externos.

4. Un método de acuerdo con la reivindicación 1, que comprende adicionalmente las etapas, previamente a dicha etapa de reconfiguración en al menos un punto sobre el sistema físico, de:

estimular la función física inclonable y reconfigurable con dicho primer estímulo de modo que se obtenga dicha primera respuesta; y
almacenar dicha respuesta.

5. Un método de acuerdo con la reivindicación 4, que comprende adicionalmente las etapas de:

generar datos de traducción asociados a dichos primer estímulo y primera respuesta; y
almacenar dichos datos de traducción asociados a dicho punto.

6. Un método de acuerdo con la reivindicación 1, que comprende adicionalmente la etapa de:

codificar dichos datos de traducción.

7. Un método de acuerdo con la reivindicación 5, que comprende adicionalmente la etapa de:

transformar dicha segunda respuesta en dicha primera respuesta mediante el uso de dichos datos de traducción.

8. Un método de acuerdo con la reivindicación 5, que comprende adicionalmente la etapa de:

almacenar temporalmente dichos datos de traducción.

9. Un método de acuerdo con la reivindicación 5, que comprende adicionalmente la etapa de:

almacenar de manera protectora dichos datos de traducción.

10. Un método de acuerdo con la reivindicación 1, en el que dichas etapas de almacenamiento se realizan en una

segunda función física inclonable y reconfigurable.

11. Un método de acuerdo con la reivindicación 1, en el que la etapa de evaluar dicho artículo comprende adicionalmente el almacenamiento temporal de dicho artículo descifrado.

12. Un método de acuerdo con la reivindicación 1, que comprende adicionalmente las etapas, después de la etapa de reconfigurar dicha función física inclonable y reconfigurable, de:

estimular con dicho primer estímulo la función física inclonable y reconfigurable reconfigurada;
medir dicha segunda respuesta desde la función física inclonable y reconfigurable;
generar una segunda clave aleatoria usando dicha segunda respuesta y dichos datos de traducción;
volver a cifrar dicho artículo usando dicha segunda clave aleatoria;
almacenar dicha segunda clave aleatoria y dicho artículo cifrado de nuevo.

13. Un método de acuerdo con la reivindicación 12, que comprende adicionalmente generar segundos datos de traducción a partir de dicho primer estímulo y dicha segunda respuesta, en el que dichos segundos datos de traducción se usan para generar dicha segunda clave aleatoria.

14. Un método de acuerdo con la reivindicación 13, en el que dicho artículo cifrado de nuevo se almacena en uno de entre una memoria protegida, una memoria insegura, una segunda función física inclonable y reconfigurable y una función física inclonable.

15. Un método de acuerdo con la reivindicación 1, en el que el uso de dicho artículo comprende la actualización de dicho artículo.

16. Un método de acuerdo con la reivindicación 1, en el que dicho artículo es una clave.

17. Un método de acuerdo con la reivindicación 1, en el que dicha primera clave aleatoria se obtiene mediante el estímulo con un segundo estímulo de dicha función física inclonable y reconfigurable.

18. Un dispositivo para proporcionar seguridad digital que comprende:

una función física inclonable y reconfigurable, que comprende un sistema físico constituido por componentes distribuidos dispuestos para generar una primera respuesta cuando reciben un primer estímulo en un punto de dicho sistema físico,
una unidad de estímulo para estimular dicha función física inclonable y reconfigurable;
una unidad detectora para la detección de dicha respuesta;
una unidad de procesamiento para el procesamiento de los datos de estímulo y respuesta;
una unidad de reconfiguración para reconfigurar físicamente dicha función física inclonable y reconfigurable, por medio de la redistribución de dichos componentes de modo que generen una segunda respuesta, que difiere de dicha primera respuesta cuando se aplica de nuevo dicho primer estímulo en dicho punto, afectando la reconfiguración física a la estructura física de la función física inclonable y reconfigurable, en donde dicha reconfiguración está condicionada por la determinación de si realizar o no una reconfiguración, proporcionando el dispositivo para proporcionar seguridad digital almacenamiento seguro de un artículo digital, estando dispuesto el dispositivo para proporcionar seguridad digital para:

obtener una primera clave aleatoria;
generar datos de traducción basándose en dicha primera respuesta de dicho primer estímulo en dicho punto y dicha primera clave aleatoria;
cifrar dicho artículo con dicha clave aleatoria;
almacenar los datos de traducción, dicho primer estímulo y dicho artículo cifrado;
acceder a dicho artículo previamente a la etapa de reconfigurar la función física inclonable y reconfigurable, en donde la etapa de acceder al artículo comprende las etapas de:

estimular la función física inclonable y reconfigurable con dicho estímulo almacenado;
medir una respuesta que corresponde al estímulo almacenado a partir de la función física inclonable y reconfigurable;
reconstruir dicha clave aleatoria usando dicha respuesta medida y dichos datos de traducción almacenados;
descifrar dicho artículo cifrado almacenado usando dicha clave aleatoria reconstruida, mediante lo cual dicho artículo está disponible para su uso.

19. Un dispositivo de acuerdo con la reivindicación 18, que comprende adicionalmente una unidad de almacenamiento para el almacenamiento de al menos datos de estímulo y respuesta, en el que dicha unidad de almacenamiento se implementa con una de entre una memoria protegida, una memoria insegura, una segunda función física inclonable y reconfigurable y una función física inclonable.

20. Un dispositivo de acuerdo con la reivindicación 19, en el que la función física inclonable y reconfigurable se implementa mediante un material óptico y dicha unidad de reconfiguración está dispuesta para aplicar una tensión externa al sistema físico.

21. Un dispositivo de acuerdo con la reivindicación 18, en el que la función física inclonable y reconfigurable se implementa mediante un material óptico y la unidad de reconfiguración está dispuesta para aplicar calor al sistema físico.

22. Un dispositivo de acuerdo con la reivindicación 18, en el que la función física inclonable y reconfigurable se implementa mediante un material óptico de degradación y en el que dicha unidad de reconfiguración está dispuesta para aplicar un gran número de operaciones de lectura.

23. Un dispositivo de acuerdo con la reivindicación 18, en el que los componentes de la función física inclonable y reconfigurable se basan en una cadena de bits cuánticos que están configurados en una primera base, y la unidad de reconfiguración está dispuesta para aplicar una medición externa sobre los bits cuánticos en una segunda base que es diferente de dicha primera base haciendo que dichos bits cuánticos se redistribuyan aleatoriamente para configurarse en dicha segunda base, mediante lo cual se reconfigura dicha función física inclonable y reconfigurable.

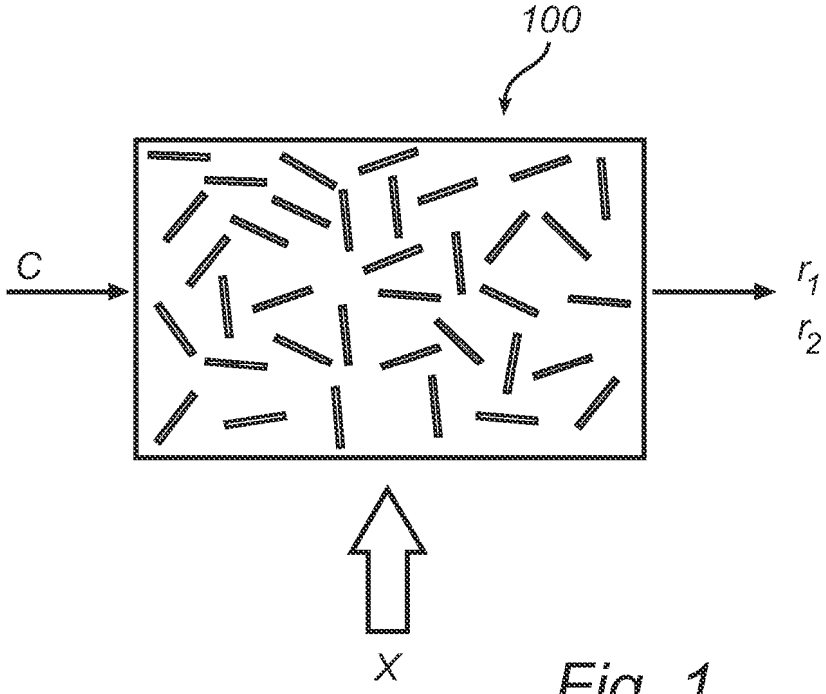

Fig. 1

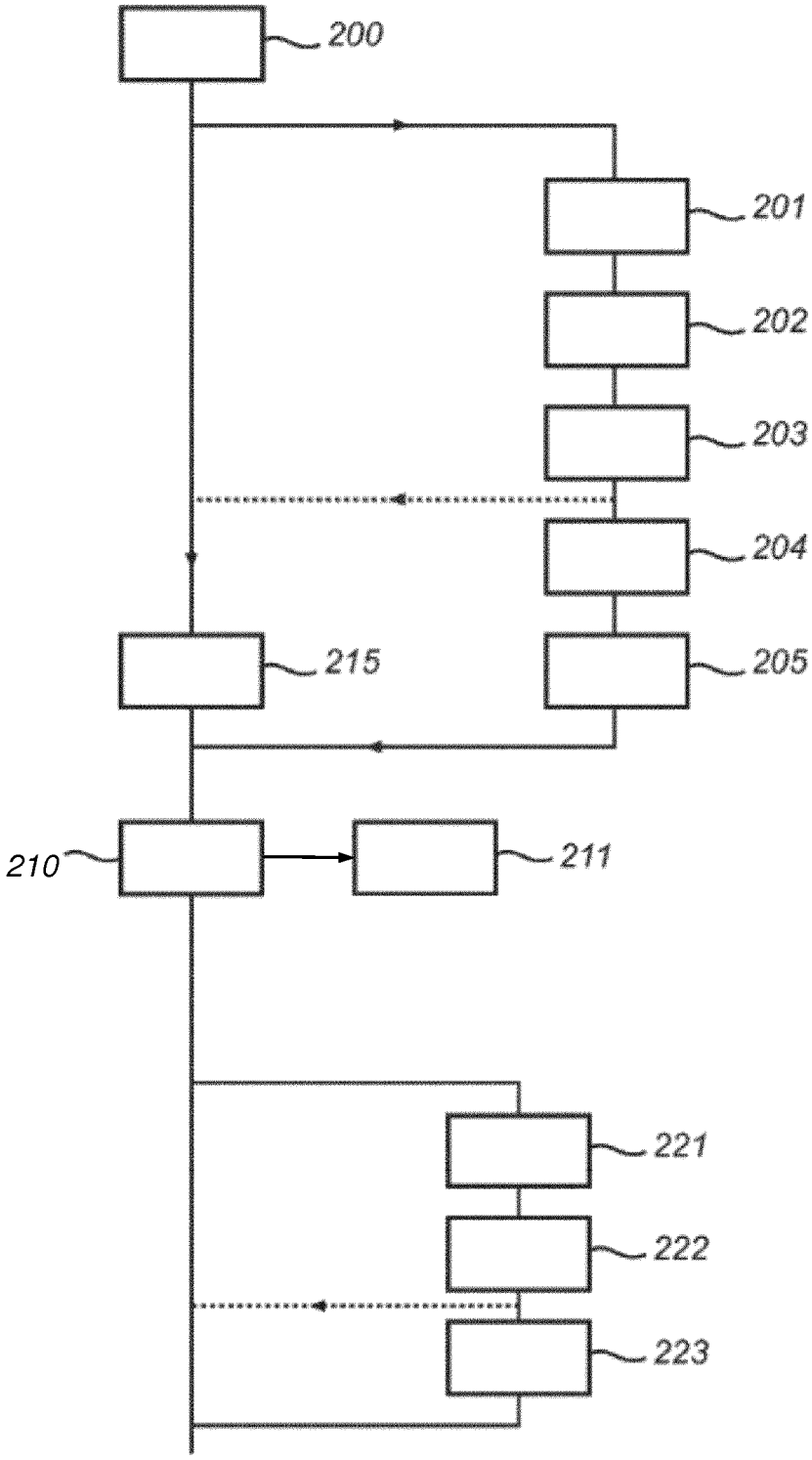

Fig. 2

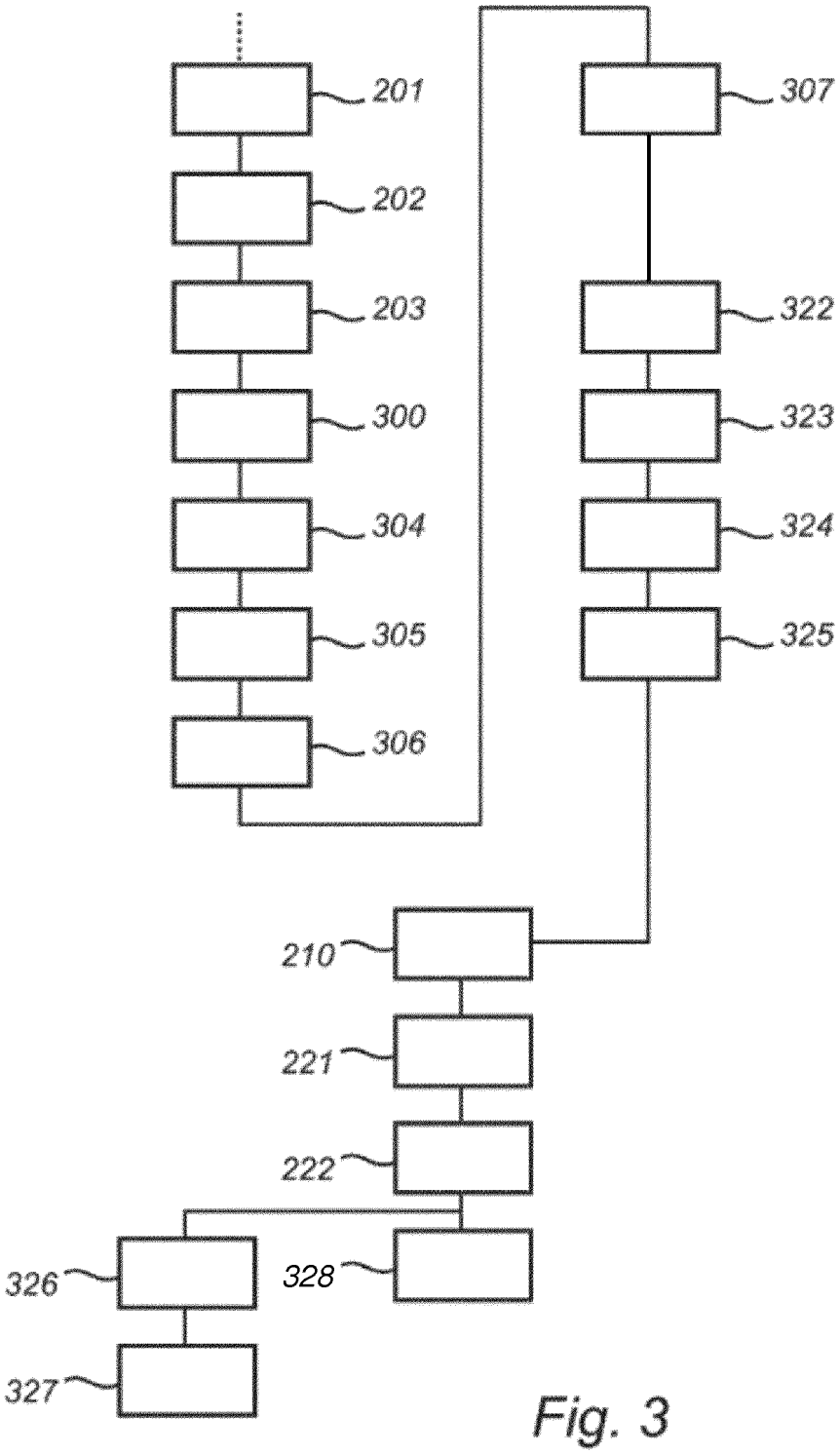
201
202
203
300
304
305
306
307
322
323
324
325
210
221
222
326
327
328

Fig. 3

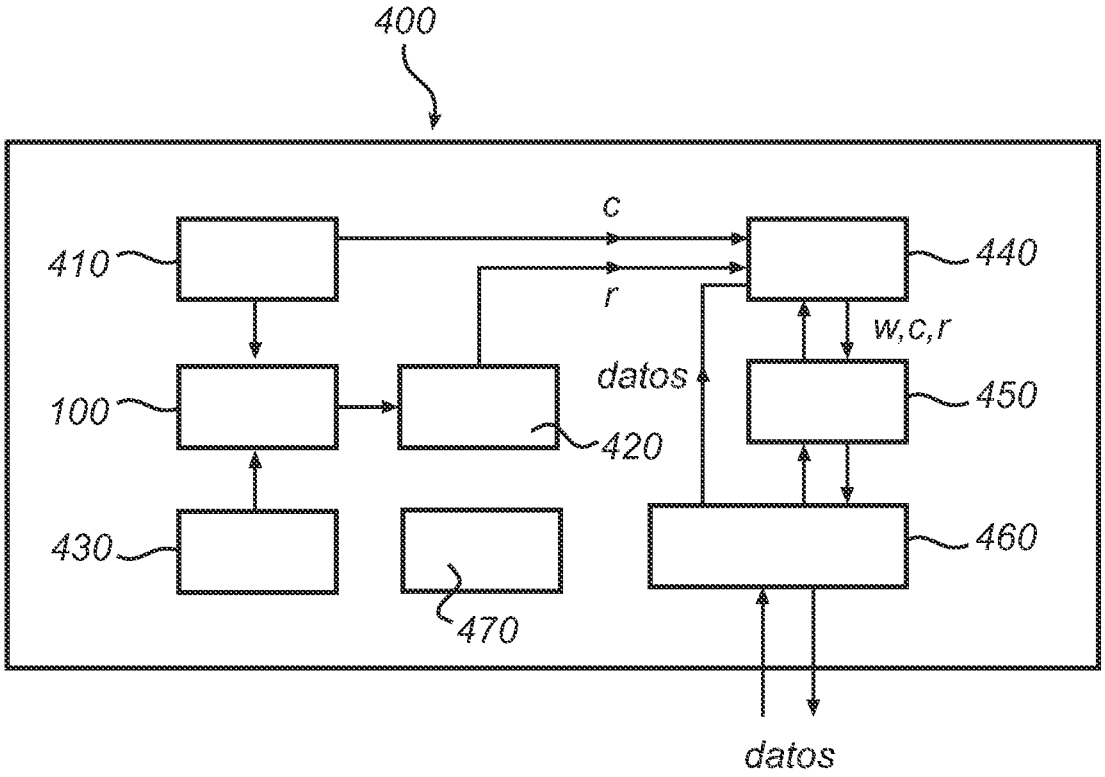

Fig. 4