(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 977 233**

(51) Int. Cl.:

H03K 3/78 (2006.01)
G09C 1/00 (2006.01)
H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.03.2020 E 20160738 (9)**

(97) Fecha y número de publicación de la concesión europea: **17.01.2024 EP 3709516**

(54) Título: **Dispositivo y procedimiento para el cifrado de datos basado en hardware con conmutadores resistivos complementarios**

(30) Prioridad:

11.03.2019 DE 102019203288

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.08.2024

(73) Titular/es:

FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNGDER ANGEWANDTEN FORSCHUNG E.V. (100.0%)
Hansastr. 27c
80686 München, DE

(72) Inventor/es:

DU, NAN;
SCHMIDT, HEIDEMARIE;
ECKE, RAMONA y
SCHULZ, STEFAN

(74) Agente/Representante:

PONTI & PARTNERS, S.L.P.

DESCRIPCIÓN

Dispositivo y procedimiento para el cifrado de datos basado en hardware con conmutadores resistivos complementarios

[0001] La solicitud se refiere al cifrado de datos basado en hardware con un circuito electrónico y, en particular, a un dispositivo y un procedimiento para el cifrado de datos basado en hardware con conmutadores resistivos complementarios. Además, la solicitud se refiere a la estructura del circuito electrónico y a un procedimiento para cifrar los datos.

[0002] En un mundo cada vez más digitalizado y conectado, el uso selectivo de las modernas tecnologías de la información y la comunicación es la clave decisiva para el éxito económico. Volúmenes de datos en rápido crecimiento (2018: 1,6 zettabytes ($1{,}6 \cdot 10^{21}$ bytes) [1]) se deben cifrar para una infraestructura de datos segura.

[0003] Los cifrados de datos digitales, también conocidas como tecnologías de cifrado basadas en software, ofrecen una buena estrategia para proteger los datos. El cifrado basado en software ha sido la solución estándar para el cifrado de datos hasta ahora. Actualmente, los archivos o carpetas individuales o incluso todo el disco duro (en el contexto de un cifrado de disco completo) se pueden cifrar con la ayuda de programas de software. Para este propósito, ya está disponible en el mercado un gran número de soluciones de software de varios proveedores. Sin embargo, un tiempo y un esfuerzo informático considerables y el aumento del consumo de energía asociado son desventajas del cifrado de disco completo basado en software. Un procedimiento basado en software ya no será practicable en el futuro, dadas las cantidades de datos que se espera que crezcan rápidamente y que se tengan que procesar.

[0004] El cifrado basado en hardware resuelve los problemas del cifrado basado en software y permite el uso de nuevos conceptos y protocolos de cifrado.

[0005] En la criptografía basada en hardware, los datos o las señales intercambiadas se cifran a través de los componentes de hardware (hardware de cifrado) directamente en el soporte de datos en tiempo real sin el uso de software adicional, protegiéndolos de información no deseada. Si el medio de almacenamiento se pierde físicamente, los datos almacenados siguen siendo seguros. En la operación en tiempo real, el uso de criptografía de hardware permite adicionalmente longitudes de clave más largas de lo que era posible anteriormente. Por lo tanto, el cifrado de hardware ofrece considerables ventajas de seguridad y, al mismo tiempo, reduce la carga del sistema, ya que el cifrado no requiere una energía de procesador.

[0006] Una solución conocida para almacenar claves para aplicaciones criptográficas es la llamada función física no clonable (Physical Unclonable Function, PUF).

[0007] Al igual que una huella dactilar, la PUF es una propiedad individual que está vinculada a un objeto físico (hardware de cifrado). Hoy en día, las PUF se utilizan para identificar componentes de circuitos integrados o como un reemplazo para almacenar claves para aplicaciones criptográficas. El desafío al realizar una PUF es encontrar un objeto físico (hardware de cifrado) que tenga una propiedad individual impredecible.

[0008] Debido al comportamiento estocástico de los memristores, los memristores son candidatos potenciales ideales para la realización de hardware de cifrado. Los memristores son componentes microelectrónicos novedosos cuya resistencia eléctrica se puede ajustar específicamente dependiendo del flujo de corriente y, a continuación, permanece no volátil sin que se aplique un voltaje externo, de ahí la palabra artificial que consiste en memoria y resistencia. Se sospecha que los memristores no son susceptibles al ruido y a las influencias ambientales debido a su comportamiento no volátil. Al mismo tiempo, sin embargo, las propiedades individuales de los memristores dependen en gran medida e incontrolablemente del procedimiento de fabricación y, por lo tanto, son impredecibles.

[0009] Por ejemplo, los memristores se describieron en [6].

[0010] Ya se desarrollaron varios protocolos diferentes para PUF en diferentes aplicaciones. Por ejemplo, la plataforma $BiFeO_3$ (BFO) (BFO/ $BiFeO_3$ = bismuto-óxido de hierro) abre la posibilidad de usar la plataforma BFO como PUF en la criptografía basada en hardware debido a las propiedades memristivas de BFO. Por ejemplo, un protocolo describe cómo se utilizará el cambio de resistencia no lineal no volátil de los memristores BFO para la generación de armónicos más altos que se pueden usar para cifrar y descifrar fácilmente conjuntos de datos digitales [2], [3]. Estos armónicos superiores se pueden transmitir al receptor de forma inalámbrica y pueden ser decodificados por el receptor utilizando criptografía basada en hardware. La minimización de la autocorrelación de estos armónicos más altos se ha demostrado fundamentalmente utilizando criptografía basada en BFO [3].

[0011] El conjunto de datos transmitidos solo se puede decodificar si están disponibles el memristor BFO idéntico y el generador de números aleatorios idéntico, así como el circuito de criptografía idéntico utilizado por el transmisor para descifrar los datos. También se mostró cómo el memristor basado en BFO se puede utilizar para

proteger datos personales en el campo de la medicina [4].

[0012] La propiedad del protocolo del conjunto de datos transmitidos solo se decodifica si están disponibles el memristor BOF idéntico y el generador de números aleatorios idéntico, así como el circuito de criptografía idéntico utilizado por el transmisor para descifrar los datos, lo que representa una brecha de seguridad. Hasta ahora, esta brecha de seguridad no se ha podido cerrar.

[0013] En 2014, se realizó un memristor $BiFeO_3$ con dos barreras reconfigurables [5], [2] y se mostró un procedimiento para realizar una lógica reconfigurable sobre la base de un memristor $BiFeO_3$ con dos barreras reconfigurables [5], [2].

[0014] El documento US 2015/0358151 A1 describe un interruptor resistivo complementario que tiene dos terminales externos entre los cuales se disponen dos capas piezoeléctricas o ferroeléctricas con un terminal interno. Se modifica al menos una región de las capas. Lo que también se describe es una estructura de resistencia conectable con al menos un contacto Schottky a al menos dos capas piezoeléctricas o ferroeléctricas vecinas, una capa piezoeléctrica y ferroeléctrica policristalina con cristalitos modificados, así como un procedimiento y circuitos para cifrar y descifrar una secuencia de bits.

[0015] Además, se describe la integración del interruptor resistivo complementario en las intersecciones de una estructura de red como una puerta lógica en un circuito lógico.

[0016] Por lo tanto, un objeto de la invención es proporcionar conceptos para el cifrado mejorado.

[0017] Según la invención, el objeto se resuelve mediante un codificador según la reivindicación 1, mediante un decodificador según la reivindicación 12, mediante un sistema según la reivindicación 25, mediante un procedimiento según la reivindicación 27, mediante un procedimiento según la reivindicación 28 y mediante un programa informático según la reivindicación 29.

[0018] Se proporciona un codificador para codificar un valor binario de entrada de una secuencia de datos de entrada binarios generando una corriente de salida de una señal de corriente de salida. El codificador incluye un módulo de control y un elemento resistivo conmutable. El elemento resistivo conmutable está configurado para estar en un primer estado o en un segundo estado diferente dependiendo de un primer voltaje de entrada en un primer punto en el tiempo y dependiendo de un segundo voltaje de entrada en un segundo punto en el tiempo posterior. El módulo de control está configurado para aplicar el primer voltaje de entrada al elemento resistivo conmutable en el primer punto en el tiempo para que el primer voltaje de entrada dependa de dicho valor binario de entrada. Además, el módulo de control está configurado para aplicar el segundo voltaje de entrada al elemento resistivo conmutable en el segundo punto en el tiempo, de modo que el segundo voltaje de entrada depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una primera secuencia de datos pseudoaleatorios binarios. Además, el módulo de control está configurado para aplicar un tercer voltaje de entrada al elemento resistivo conmutable en un tercer punto en el tiempo después del segundo punto en el tiempo, de modo que el tercer voltaje de entrada depende de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una segunda secuencia de datos pseudoaleatorios binarios. El elemento resistivo conmutable está configurado, al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, para emitir dicha corriente de salida de modo que dicha corriente de salida depende del tercer voltaje de entrada y depende de si el elemento resistivo conmutable está en el primer estado o en el segundo estado.

[0019] Además, se proporciona un decodificador para decodificar una corriente de entrada de una señal de corriente de entrada emitiendo un valor binario de salida de una secuencia de datos de salida binaria. El decodificador incluye un módulo de control, un elemento resistivo conmutable y un comparador. El elemento resistivo conmutable está configurado para estar en un primer estado o en un segundo estado diferente dependiendo de un primer voltaje de entrada en un primer punto en el tiempo y dependiendo de un segundo voltaje de entrada en un segundo punto en el tiempo posterior. El módulo de control está configurado para aplicar el primer voltaje de entrada al elemento resistivo conmutable en el primer punto en el tiempo de modo que el primer voltaje de entrada depende de un valor binario de muestra de una pluralidad de valores binarios de muestra. Además, el módulo de control está configurado para aplicar el segundo voltaje de entrada al elemento resistivo conmutable en el segundo punto en el tiempo de modo que el segundo voltaje de entrada depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una primera secuencia de datos pseudoaleatorios binarios. Además, el módulo de control está configurado para aplicar un tercer voltaje de entrada al elemento resistivo conmutable en un tercer punto en el tiempo después del segundo punto en el tiempo, de modo que el tercer voltaje de entrada depende de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una segunda secuencia de datos pseudoaleatorios binarios. El elemento resistivo conmutable está configurado, al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, para proporcionar una corriente de salida al comparador de modo que dicha corriente de salida depende del tercer voltaje de entrada y depende de si el elemento resistivo conmutable está en el primer estado o en el segundo estado. El comparador está configurado

para realizar una comparación entre dicha corriente de salida y dicha corriente de entrada, donde el comparador está configurado, dependiendo de la comparación y dicho valor binario de muestra, para determinar dicho valor binario de salida, y donde el comparador está configurado para emitir dicho valor binario de salida.

[0020] Además, se proporciona un procedimiento de codificación de un valor binario de entrada de una secuencia de datos de entrada binarios generando una corriente de salida de una señal de corriente de salida. Un elemento resistivo conmutable está configurado para estar en un primer estado o en un segundo estado diferente dependiendo de un primer voltaje de entrada en un primer punto en el tiempo y dependiendo de un segundo voltaje de entrada en un segundo punto en el tiempo posterior. El procedimiento incluye:

- aplicar el primer voltaje de entrada al elemento resistivo conmutable en el primer punto en el tiempo de modo que el primer voltaje de entrada depende de dicho valor binario de entrada;
- aplicar el segundo voltaje de entrada al elemento resistivo conmutable en el segundo punto en el tiempo de modo que el segundo voltaje de entrada depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una primera secuencia de datos pseudoaleatorios binarios;
- aplicar un tercer voltaje de entrada al elemento resistivo conmutable en un tercer punto en el tiempo después del segundo punto en el tiempo, de modo que el tercer voltaje de entrada depende de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una segunda secuencia de datos pseudoaleatorios binarios; y
- al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, emitir dicha corriente de salida por el elemento resistivo conmutable; de modo que dicha corriente de salida depende del tercer voltaje de entrada y depende de si el elemento resistivo conmutable está en el primer estado o en el segundo estado,

[0021] Además, se proporciona un procedimiento de decodificación de una corriente de entrada de una señal de corriente de entrada emitiendo un valor binario de salida de una secuencia de datos de salida binaria. Un elemento resistivo conmutable está configurado para estar en un primer estado o en un segundo estado diferente dependiendo de un primer voltaje de entrada en un primer punto en el tiempo y dependiendo de un segundo voltaje de entrada en un segundo punto en el tiempo posterior. El procedimiento incluye:

- aplicar el primer voltaje de entrada al elemento resistivo conmutable en el primer punto en el tiempo de modo que el primer voltaje de entrada depende de un valor binario de muestra de una pluralidad de valores binarios de muestra;
- aplicar el segundo voltaje de entrada al elemento resistivo conmutable en el segundo punto en el tiempo de modo que el segundo voltaje de entrada depende de un valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de una primera secuencia de datos pseudoaleatorios binarios;
- aplicar un tercer voltaje de entrada al elemento resistivo conmutable en un tercer punto en el tiempo después del segundo punto en el tiempo, de modo que el tercer voltaje de entrada depende de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una segunda secuencia de datos pseudoaleatorios binarios;
- al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, proporcionar una corriente de salida por el elemento resistivo conmutable; de modo que dicha corriente de salida depende del tercer voltaje de entrada y depende de si el elemento resistivo conmutable está en el primer estado o en el segundo estado, y
- realizar una comparación entre dicha corriente de salida y dicha corriente de entrada, determinar dicho valor binario de salida dependiendo de la comparación y de dicho valor binario de muestra, y emitir dicho valor binario de salida.

[0022] Además, se proporcionan programas informáticos que tienen cada uno un código de programa para realizar uno de los procedimientos descritos anteriormente.

[0023] Las realizaciones preferidas de la invención se pueden encontrar en las reivindicaciones de patente dependientes.

[0024] A continuación, se describen realizaciones preferidas de la invención con referencia a los dibujos, donde:

La Fig. 1 muestra un codificador para codificar un valor binario de entrada de una secuencia de datos de entrada binaria generando una corriente de salida de una señal de corriente de salida según una realización.
La Fig. 2 muestra un decodificador para decodificar una corriente de entrada de una señal de corriente de entrada emitiendo un valor binario de salida de una secuencia de datos de salida binaria según una realización.
La Fig. 3 muestra un sistema según una realización.
La Fig. 4 muestra una corriente de lectura I de una resistencia complementaria según una realización.
La Fig. 5 muestra esquemáticamente un diagrama de circuito de bloques para el cifrado y descifrado de datos binarios utilizando dos generadores de números aleatorios según una realización.
La Fig. 6 ilustra cómo los datos binarios se cifran en tres elementos analógicos de datos, cada uno usando tres

amplitudes diferentes según una realización.
La Fig. 7 muestra esquemáticamente un diagrama de circuito de bloques para el cifrado y descifrado de datos binarios utilizando tres generadores de números aleatorios según una realización.

[0025] La Fig. 1 muestra un codificador 100 para codificar un valor binario de entrada de una secuencia de datos de entrada binarios generando una corriente de salida de una señal de corriente de salida según una realización. El codificador 100 incluye un módulo de control 110 y un elemento resistivo conmutable 120.

[0026] El elemento resistivo conmutable 120 (también denominado interruptor resistivo complementario) está configurado para estar en un primer estado o en un segundo estado diferente dependiendo de un primer voltaje de entrada en un primer punto en el tiempo y dependiendo de un segundo voltaje de entrada en un segundo punto en el tiempo posterior.

[0027] El módulo de control 110 está configurado para aplicar el primer voltaje de entrada al elemento resistivo conmutable 120 en el primer punto en el tiempo de modo que el primer voltaje de entrada depende de dicho valor binario de entrada.

[0028] Además, el módulo de control 110 está configurado para aplicar el segundo voltaje de entrada al elemento resistivo conmutable 120 en el segundo punto en el tiempo, de modo que el segundo voltaje de entrada depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una primera secuencia de datos pseudoaleatorios binarios.

[0029] Además, el módulo de control 110 está configurado para aplicar un tercer voltaje de entrada al elemento resistivo conmutable 120 en un tercer punto en el tiempo después del segundo punto en el tiempo, de modo que el tercer voltaje de entrada depende de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una segunda secuencia de datos pseudoaleatorios binarios.

[0030] El elemento resistivo conmutable 120 está configurado, al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, para emitir dicha corriente de salida de modo que dicha corriente de salida depende del tercer voltaje de entrada y depende de si el elemento resistivo conmutable 120 está en el primer estado o en el segundo estado.

[0031] Según una realización, por ejemplo, el elemento resistivo conmutable 120 se puede configurar, al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, para emitir dicha corriente de salida de tal manera que:

- dicha corriente de salida comprende un primer valor de corriente de salida si el tercer voltaje de entrada comprende un primer valor de voltaje de entrada y el elemento resistivo conmutable 120 está en el primer estado,
- dicha corriente de salida comprende un segundo valor de corriente de salida mayor que el primer valor de corriente de salida si el tercer voltaje de entrada comprende un segundo valor de voltaje de entrada y el elemento resistivo conmutable 120 está en el primer estado,
- dicha corriente de salida comprende un tercer valor de corriente de salida si el tercer voltaje de entrada comprende el primer valor de voltaje de entrada y el elemento resistivo conmutable 120 está en el segundo estado, y
- de tal manera que dicha corriente de salida comprende un cuarto valor de corriente de salida más pequeño que el tercer valor de corriente de salida si el tercer voltaje de entrada comprende el segundo valor de voltaje de entrada y el elemento resistivo conmutable 120 está en el segundo estado.

[0032] En este caso, por ejemplo, el primer valor de corriente de salida y el cuarto valor de corriente de salida pueden ser iguales o diferentes, y, por ejemplo, el segundo valor de corriente de salida y el tercer valor de corriente de salida pueden ser iguales o diferentes.

[0033] En una realización, por ejemplo, el elemento resistivo conmutable 120 puede ser un memristor.

[0034] Según una realización, por ejemplo, el módulo de control 110 puede comprender un primer generador pseudoaleatorio 111, por ejemplo, que se puede configurar para generar la primera secuencia de generador pseudoaleatorio. O, por ejemplo, el módulo de control 110 puede incluir el primer generador pseudoaleatorio 111, por ejemplo, que se puede configurar para generar la primera secuencia de generador pseudoaleatorio, y, por ejemplo, donde el módulo de control 110 puede incluir un segundo generador pseudoaleatorio 112, por ejemplo, que se puede configurar para generar la segunda secuencia de generador pseudoaleatorio (cf. Fig. 5 y Fig. 7).

[0035] En una realización, por ejemplo, el módulo de control 110 se puede configurar para vincular dicho valor binario de entrada a dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la segunda secuencia de datos pseudoaleatorios binarios por medio de una operación booleana para obtener un valor binario de combinación. En este caso, por ejemplo, el módulo de control 110 se puede configurar para aplicar el primer

voltaje de entrada al elemento resistivo conmutable 120 en el primer punto en el tiempo, de modo que el primer voltaje de entrada dependa del valor binario de combinación. Además, por ejemplo, el módulo de control 110 se puede configurar para aplicar el tercer voltaje de entrada al elemento resistivo conmutable 120 en el tercer punto en el tiempo, de modo que el tercer voltaje de entrada dependa de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la segunda secuencia de datos pseudoaleatorios binarios.

[0036] Según una realización, por ejemplo, la operación booleana puede ser una operación XOR o una operación XNOR.

[0037] En una realización, por ejemplo, el módulo de control 110 se puede configurar para aplicar el tercer voltaje de entrada al elemento resistivo conmutable 120 en el tercer punto en el tiempo, de modo que el tercer voltaje de entrada no dependa de dicho valor binario de entrada.

[0038] Según una realización, por ejemplo, el módulo de control 110 se puede configurar para aplicar el primer voltaje de entrada al elemento resistivo conmutable 120 de modo que el primer voltaje de entrada sea positivo o negativo dependiendo de dicho valor binario de entrada. En este caso, por ejemplo, el módulo de control 110 se puede configurar para aplicar el segundo voltaje de entrada al elemento resistivo conmutable 120 de modo que el segundo voltaje de entrada sea positivo o negativo dependiendo de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios. Además, por ejemplo, el módulo de control 110 puede estar configurado para aplicar el tercer voltaje de entrada al elemento resistivo conmutable 120 de modo que el tercer voltaje de entrada sea positivo o negativo dependiendo de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o dependiendo de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la segunda secuencia de datos pseudoaleatorios binarios.

[0039] En una realización, por ejemplo, el módulo de control 110 se puede configurar para determinar una amplitud del primer valor de entrada y/o del segundo valor de entrada dependiendo de un valor pseudoaleatorio de una tercera secuencia de datos pseudoaleatoria.

[0040] Según una realización, por ejemplo, el módulo de control 110 se puede configurar para determinar uno de tres o más valores de amplitud diferentes para la amplitud del primer voltaje de entrada y/o del segundo voltaje de entrada dependiendo de dicho valor pseudoaleatorio de la tercera secuencia de datos pseudoaleatoria.

[0041] En una realización, por ejemplo, el módulo de control 110 puede incluir un tercer generador pseudoaleatorio 113, por ejemplo, que se puede configurar para generar la tercera secuencia de generador pseudoaleatorio de modo que cada valor pseudoaleatorio de la tercera secuencia de datos pseudoaleatorios adopte uno de tres o más valores numéricos diferentes.

[0042] Según la invención, por ejemplo, el módulo de control 110 incluye un multiplexor 115 y líneas, por ejemplo, donde el multiplexor 115 está configurado para conectar las líneas. En este caso, el módulo de control 110 está configurado para aplicar el primer voltaje de entrada, el segundo voltaje de entrada y el tercer voltaje de entrada al elemento resistivo conmutable 120 (véanse la Fig. 5 y Fig. 7) a través de las líneas y a través del multiplexor 115.

[0043] La Fig. 2 muestra un decodificador 200 para decodificar una corriente de entrada de una señal de corriente de entrada emitiendo un valor binario de salida de una secuencia de datos de salida binaria según una realización. El decodificador 200 incluye un módulo de control 210, un elemento resistivo conmutable 220 y un comparador 230.

[0044] El elemento resistivo conmutable 220 (también denominado interruptor resistivo complementario) está configurado para estar en un primer estado o en un segundo estado diferente dependiendo de un primer voltaje de entrada en un primer punto en el tiempo y dependiendo de un segundo voltaje de entrada en un segundo punto en el tiempo posterior.

[0045] El módulo de control 210 está configurado para aplicar el primer voltaje de entrada al elemento resistivo conmutable 220 en el primer punto en el tiempo de modo que el primer voltaje de entrada depende de un valor binario de muestra de una pluralidad de valores binarios de muestra.

[0046] Además, el módulo de control 210 está configurado para aplicar el segundo voltaje de entrada al elemento resistivo conmutable 220 en el segundo punto en el tiempo, de modo que el segundo voltaje de entrada depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una primera secuencia de datos pseudoaleatorios binarios.

[0047] Además, el módulo de control 210 está configurado para aplicar un tercer voltaje de entrada al elemento resistivo conmutable 220 en un tercer punto en el tiempo después del segundo punto en el tiempo, de modo que el tercer voltaje de entrada depende de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios

pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una segunda secuencia de datos pseudoaleatorios binarios.

[0048] El elemento resistivo conmutable 220 está configurado, al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, para proporcionar una corriente de salida al comparador 230 de modo que dicha corriente de salida depende del tercer voltaje de entrada y depende de si el elemento resistivo conmutable 220 está en el primer estado o en el segundo estado.

[0049] El comparador 230 está configurado para realizar una comparación entre dicha corriente de salida y dicha corriente de entrada, donde el comparador 230 está configurado para determinar dicho valor binario de salida dependiendo de la comparación y de dicho valor binario de muestra, y donde el comparador 230 está configurado para emitir dicho valor binario de salida.

[0050] Según una realización, por ejemplo, el comparador 230 se puede configurar para determinar dicho valor binario de muestra como dicho valor binario de salida y emitirlo si una magnitud de una diferencia entre la corriente de salida y dicha corriente de entrada es menor que un límite. En este caso, por ejemplo, el comparador 230 se puede configurar para determinar un valor binario invertido de dicho valor binario de muestra como dicho valor binario de salida y emitirlo si una magnitud de una diferencia entre la corriente de salida y dicha corriente de entrada es mayor o igual que el límite.

[0051] Según una realización, por ejemplo, el elemento resistivo conmutable 220 se puede configurar, al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, para proporcionar dicha corriente de salida al comparador 230 de tal manera que:

- dicha corriente de salida comprende un primer valor de corriente de salida si el tercer voltaje de entrada comprende un primer valor de voltaje de entrada y el elemento resistivo conmutable 220 está en el primer estado,
- dicha corriente de salida comprende un segundo valor de corriente de salida que es mayor que el primer valor de corriente de salida si el tercer voltaje de entrada comprende un segundo valor de voltaje de entrada y el elemento resistivo conmutable 220 está en el primer estado,
- dicha corriente de salida comprende un tercer valor de corriente de salida si el tercer voltaje de entrada comprende el primer valor de voltaje de entrada y el elemento resistivo conmutable 220 está en el segundo estado, y
- dicha corriente de salida comprende un cuarto valor de corriente de salida que es menor que el tercer valor de corriente de salida si el tercer voltaje de entrada comprende el segundo valor de voltaje de entrada y el elemento resistivo conmutable 220 está en el segundo estado.

[0052] En este caso, por ejemplo, el primer valor de corriente de salida y el cuarto valor de corriente de salida pueden ser iguales o diferentes, y, por ejemplo, el segundo valor de corriente de salida y el tercer valor de corriente de salida pueden ser iguales o diferentes.

[0053] En una realización, por ejemplo, el elemento resistivo conmutable 220 puede ser un memristor.

[0054] Según una realización, por ejemplo, el módulo de control 210 puede incluir un primer generador pseudoaleatorio 211, por ejemplo, que se puede configurar para generar la primera secuencia de generador pseudoaleatorio. O, por ejemplo, el módulo de control 210 puede incluir el primer generador pseudoaleatorio 211, por ejemplo, que se puede configurar para generar la primera secuencia de generador pseudoaleatorio, y, por ejemplo, donde el módulo de control 210 puede incluir un segundo generador pseudoaleatorio 212, por ejemplo, que se puede configurar para generar la segunda secuencia de generador pseudoaleatorio (cf. Fig. 5 y Fig. 7).

[0055] En una realización, por ejemplo, el módulo de control 210 se puede configurar para vincular dicho valor binario de entrada a dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la segunda secuencia de datos pseudoaleatorios binarios por medio de una operación booleana para obtener un valor binario de combinación. En este caso, por ejemplo, el módulo de control 210 se puede configurar para aplicar el primer voltaje de entrada al elemento resistivo conmutable 220 en el primer punto en el tiempo, de modo que el primer voltaje de entrada dependa del valor binario de combinación. Además, por ejemplo, el módulo de control 210 se puede configurar para aplicar el tercer voltaje de entrada al elemento resistivo conmutable 220 en el tercer punto en el tiempo, de modo que el tercer voltaje de entrada dependa de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la segunda secuencia de datos pseudoaleatorios binarios.

[0056] Según una realización, por ejemplo, la operación booleana puede ser una operación XOR o una operación XNOR.

[0057] En una realización, por ejemplo, el módulo de control 210 se puede configurar para aplicar el tercer voltaje de entrada al elemento resistivo conmutable 220 en el tercer punto en el tiempo, de modo que el tercer voltaje de entrada no dependa de dicho valor binario de entrada.

[0058] Según una realización, por ejemplo, el módulo de control 210 se puede configurar para aplicar el primer voltaje de entrada al elemento resistivo conmutable 220 de modo que el primer voltaje de entrada sea positivo o negativo dependiendo de dicho valor binario de entrada. En este caso, por ejemplo, el módulo de control 210 se puede configurar para aplicar el segundo voltaje de entrada al elemento resistivo conmutable 220 de modo que el segundo voltaje de entrada sea positivo o negativo dependiendo de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios. Además, por ejemplo, el módulo de control 210 puede estar configurado para aplicar el tercer voltaje de entrada al elemento resistivo conmutable 220 de modo que el tercer voltaje de entrada sea positivo o negativo dependiendo de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o dependiendo de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la segunda secuencia de datos pseudoaleatorios binarios.

[0059] En una realización, por ejemplo, el módulo de control 210 se puede configurar para determinar una amplitud del primer valor de entrada y/o del segundo valor de entrada dependiendo de un valor pseudoaleatorio de una tercera secuencia de datos pseudoaleatoria.

[0060] Según una realización, por ejemplo, el módulo de control 210 se puede configurar para determinar uno de tres o más valores de amplitud diferentes para la amplitud del primer voltaje de entrada y/o del segundo voltaje de entrada dependiendo de dicho valor pseudoaleatorio de la tercera secuencia de datos pseudoaleatoria.

[0061] En una realización, por ejemplo, el módulo de control 210 puede incluir un tercer generador pseudoaleatorio 213, por ejemplo, que se puede configurar para generar la tercera secuencia de generador pseudoaleatorio de modo que cada valor pseudoaleatorio de la tercera secuencia de datos pseudoaleatorios adopte uno de tres o más valores numéricos diferentes.

[0062] Según la invención, por ejemplo, el módulo de control 210 incluye un multiplexor 215 y líneas, por ejemplo, donde el multiplexor 215 está configurado para conectar las líneas. En este caso, el módulo de control 210 está configurado para aplicar el primer voltaje de entrada, el segundo voltaje de entrada y el tercer voltaje de entrada al elemento resistivo conmutable 220 (véanse la Fig. 5 y Fig. 7) a través de las líneas y a través del multiplexor 215.

[0063] La Fig. 3 muestra un sistema que incluye un codificador 100 según cualquiera de las realizaciones antes descritas para codificar un valor binario de entrada de una secuencia de datos de entrada binaria generando una corriente de salida de una señal de corriente de salida, y un decodificador 200 según cualquiera de las realizaciones descritas anteriormente para decodificar una corriente de entrada de una señal de corriente de entrada emitiendo un valor binario de salida de una secuencia de datos de salida binaria.

[0064] El decodificador 200 está configurado para usar y decodificar la corriente de entrada del codificador 100.

[0065] En una realización, por ejemplo, la primera secuencia de datos pseudoaleatoria binaria del codificador 100 y la primera secuencia de datos pseudoaleatoria binaria del decodificador 200 pueden ser iguales. En este caso, por ejemplo, la segunda secuencia de datos pseudoaleatoria binaria del codificador 100 y la segunda secuencia de datos pseudoaleatoria binaria del decodificador 200 pueden ser iguales. Por ejemplo, el elemento resistivo conmutable 220 del codificador 100 y el elemento resistivo conmutable 220 del decodificador 200 se pueden configurar, al mismo primer voltaje de entrada y al mismo segundo voltaje de entrada, para que ambos estén en el primer estado o para que ambos estén en el segundo estado. Además, por ejemplo, el elemento resistivo conmutable 220 del codificador 100 y el elemento resistivo conmutable 220 del decodificador 200 se pueden configurar, al aplicar el mismo tercer voltaje de entrada, para emitir o proporcionar una misma corriente de salida.

[0066] Las realizaciones describen un protocolo para la transmisión segura de datos por medio de PUF basadas en un memristor, donde se utiliza un generador aleatorio para el cifrado de datos y se utiliza otro generador aleatorio para el descifrado de datos.

[0067] Con respecto a los memristores, se hace referencia explícita al documento [6], en particular al documento [6], página 44, líneas 17 a 30, página 49, línea 20 - página 50, línea 26 y página 50, línea 33 - página 55, parte inferior.

[0068] Esto cierra una brecha de seguridad previamente existente en la transmisión de datos. Por ejemplo, el hardware descrito en [2] y [5] se puede usar en realizaciones para cifrar datos binarios y almacenar los datos cifrados. Según los conceptos descritos en las realizaciones, por ejemplo, el hardware almacena los datos cifrados y, por lo tanto, proporciona una protección directa contra un ataque ya que, según los conceptos descritos, un atacante no puede predecir el mecanismo de lectura. Con el fin de leer los datos, el atacante tendría que conocer el generador aleatorio para el cifrado de datos y el generador aleatorio para el descifrado de datos. Esto complica y/o impide el descifrado de datos para un atacante.

[0069] En general, un memristor comprende un mecanismo de escritura estocástica y un mecanismo de lectura determinista. Según el procedimiento, se utiliza un memristor que tiene dos barreras reconfigurables para almacenar los datos con un generador aleatorio para el cifrado de datos booleano PRSG 112; 212 de los datos de entrada binarios y una secuencia aleatoria de números binarios booleana PRSG 111; 211 generados por medio de un generador aleatorio por medio de una función booleana seleccionada aleatoriamente. La secuencia de los dos pulsos de escritura C.HV1 y C.HV2 define los pares de estados no volátiles (LRSp, HRSn) y (LRSn, HRSp). El último par de estados escrito y establecido de manera no volátil se lee con el pulso de lectura seleccionado aleatoriamente C.LV.

[0070] En una realización, por ejemplo, la lectura se realiza en el esquema de "lectura de nivel", no en el esquema de "lectura de punta". Entre otras cosas, es una ventaja que el intervalo de voltaje para HRS en particular no se tenga que ajustar exactamente según los mV (véase la Fig. 4).

[0071] Dado que el cifrado se lleva a cabo de manera no volátil en el interruptor resistivo complementario M, los datos de entrada binarios se pueden cifrar secuencialmente. La lectura de los datos cifrados se lleva a cabo con el generador aleatorio booleano PRSG 112; 212, de modo que se utiliza la misma función booleana para el cifrado y la lectura.

[0072] Esto significa que, mediante un memristor que tiene dos barreras reconfigurables M, los datos se cifran secuencialmente de manera estocástica junto con una secuencia numérica binaria seleccionada estocásticamente y también se descifran estocásticamente. El problema del descifrado estocástico se resuelve utilizando un memristor ya conocido cuya resistencia se puede escribir de manera no volátil con dos polaridades diferentes del voltaje de escritura y cuya resistencia se puede leer con dos polaridades diferentes del voltaje de lectura (Fig. 5).

[0073] Según el concepto, se utiliza un memristor que tiene dos barreras reconfigurables para almacenar los datos con un generador aleatorio para el cifrado de datos booleano PRSG 112; 212 de los datos de entrada binarios y una secuencia aleatoria de números binarios booleana PRSG 111; 211 generados mediante un generador aleatorio mediante la función booleana seleccionada aleatoriamente.

[0074] Opcionalmente, la seguridad se puede aumentar, por ejemplo, mediante el uso de un tercer generador aleatorio PRSG **|V0|** 113; 213 para cifrar la amplitud de escritura de modo que los datos de entrada binarios se proyecten en datos cifrados analógicos. A través de este mapeo ambiguo, la seguridad en el cifrado de datos y en el descifrado de datos se puede aumentar aún más, por ejemplo.

[0075] La secuencia de los dos pulsos de escritura C.HV1 y C.HV2 define los pares de estados no volátiles (LRSp, HRSn), (LRSp', HRSn') y (LRSp", HRSn") tales como (LRSn, HRSp), (LRSn', HRSp') y (LRSn", HRSp").

[0076] La amplitud V0 de los dos pulsos de escritura C.HV1 y C.HV2 se selecciona aleatoriamente por medio del generador aleatorio PRSG **|V0|** 113; 213 y determina cuál de los tres pares de estados no volátiles (LRSp, HRSn), (LRSp', HRSn') y (LRSp", HRSn") se escribe con la mayor diferencia en la corriente de escritura I. Cuanto mayor sea la amplitud V0 de los pulsos de escritura, mayor será la diferencia en la corriente de escritura, es decir, las corrientes de escritura con respecto a los pares de etapas (LRSp", HRSn"') y (LRSn", HRSp"). En la amplitud más pequeña V0 de los pulsos de escritura, la diferencia en la corriente de escritura es la más pequeña, es decir, las corrientes de escritura con respecto a los pares de estados (LRSp, HRSn) y (LRSn, HRSp). Esto abre la posibilidad de cifrar datos de entrada binarios como datos analógicos.

[0077] La Fig. 6 ilustra cómo los datos binarios se cifran en tres elementos de datos analógicos utilizando tres amplitudes diferentes V0 según una realización.

[0078] Al igual que para el interruptor resistivo complementario M con una amplitud fija V0 de los pulsos de escritura (Fig. 4), el último par de estados escrito y configurado de manera no volátil se lee con el pulso de lectura seleccionado aleatoriamente C.LV. En una realización, por ejemplo, la lectura se realiza en el esquema de "lectura de nivel", no en el esquema de "lectura de punta".

[0079] Dado que el cifrado se lleva a cabo de manera no volátil en el interruptor resistivo complementario M con una amplitud seleccionada aleatoriamente V0 de los pulsos de escritura, los datos de entrada binarios se pueden cifrar secuencialmente como datos analógicos. Leer los datos cifrados llevados a cabo con el generador aleatorio booleano PRSG 112; 212 para que se use la misma función booleana para cifrar y leer.

[0080] Esto significa que, mediante un memristor que tiene dos barreras reconfigurables M, los datos se cifran secuencialmente de manera estocástica junto con una secuencia numérica binaria seleccionada estocásticamente y también se descifran estocásticamente. El problema del descifrado estocástico se resuelve utilizando un memristor ya conocido cuya resistencia se puede escribir de manera no volátil con dos polaridades diferentes del voltaje de escritura y cuya resistencia se puede leer con dos polaridades diferentes del voltaje de lectura (Fig. 7).

[0081] La Fig. 4 muestra una corriente de escritura I de una resistencia complementaria (de un elemento

resistivo conmutable 120; 220) según una realización con una secuencia de pulsos de escritura C.HV1 y C.HV2 en una escala logarítmica al voltaje de escritura C.LV. Dependiendo de la polaridad del voltaje de escritura C.LV, a una polaridad positiva del voltaje de escritura, se lee la corriente de escritura I_{LRSp} en el estado resistivo LRSp en el par de estados (LRSp, HRSn) y se lee la corriente de escritura I_{HRSp} en el estado resistivo HRSp en el par de estados (LRSn, HRSp), y a una polaridad negativa del voltaje de escritura, se lee la corriente de escritura IHRSn en el estado resistivo HRSn en el par de estados (LRSp, HRSn) y se lee la corriente de escritura I_{LRSn} en el estado resistivo LRSn en el par de estados (LRSn, HRSp).

[0082] La Fig. 5 muestra esquemáticamente un diagrama de circuito de bloques para el cifrado y descifrado de datos binarios utilizando dos generadores de números aleatorios booleanos PRSG 112; 212 y PRSG Boolean 111; 211 según una realización.

[0083] La Fig. 6 muestra la corriente de escritura I de una resistencia complementaria donde se han escrito tres pares de estados por medio de una secuencia de pulsos de escritura C.HV1 y C.HV2 con tres amplitudes diferentes V0 de los pulsos de escritura.

[0084] Dependiendo de la polaridad del voltaje de lectura C.LV, a una polaridad positiva del voltaje de lectura, se lee la corriente de lectura $I_{LRSp}/I_{LRSp}‘/I_{LRSp}$" en el estado resistivo LRSp/LRSp'/LRSp" en el par de estados (LRSp, HRSn)/(LRSp‘, HRSn‘)/(LRSp", HRSn") y se lee la corriente de lectura $I_{HRSp}/I_{HRSp}'/I_{HRSp}$" en el estado resistivo HRSp/HRSp'/HRSp" en el par de estados (LRSn, HRSp)/(LRSn‘, HRSp')/(LRSn", HRSp"), y a una polaridad negativa del voltaje de lectura, se lee la corriente $I_{HRSn}/ I_{HRSn}‘/I_{HRSn}$" en el estado resistivo HRSn/HRSn'/HRSn" en el par de estados (LRSp, HRSn)/(LRSn', HRSn')/(LRSp", HRSn") y se lee la corriente de lectura $I_{LRSn}/I_{LRSn}‘/I_{LRSn}$“ en el estado resistivo LRSn/LRSn'/LRSn” en el par de estados (LRSn, HRSp)/(LRSn', HRSp')/(LRSn", HRSp").

[0085] La Fig. 7 muestra esquemáticamente un diagrama de circuito de bloques para el cifrado y descifrado de datos binarios utilizando tres generadores de números aleatorios booleanos PRSG 112; 212, booleano PRSG 111; 211 y PRSG **|V0|** 113; 213 según una realización.

[0086] Aunque se describieron algunos aspectos dentro del contexto de un dispositivo, se debe entender que dichos aspectos también representan una descripción del procedimiento correspondiente, de modo tal que un bloque o un componente estructural de un dispositivo también se debe entender como una etapa de un procedimiento correspondiente o como una característica de una etapa de un procedimiento. En analogía con eso, los aspectos que se describieron dentro del contexto o como etapa de un procedimiento también representan una descripción de un bloque correspondiente o un detalle o característica de un dispositivo correspondiente. Algunas o todas las etapas del procedimiento se pueden llevar a cabo mediante el uso de un dispositivo de hardware, tal como un microprocesador, un ordenador programable o un circuito electrónico. En algunas realizaciones, algunas o varias de las etapas más importantes del procedimiento se pueden realizar mediante dicho dispositivo.

[0087] Dependiendo de ciertos requisitos de implementación específicos, las realizaciones de la invención se pueden implementar en un hardware o un software. La implementación se puede efectuar mediante el uso de un medio de almacenamiento digital, por ejemplo, un disco flexible, un DVD, un disco Blue-ray, un CD, una ROM, una PROM, una EPROM, una EEPROM o una memoria FLASH, un disco duro o cualquier otra memoria magnética u óptica que tenga señales de control legibles electrónicamente almacenadas en el mismo que puedan cooperar, o cooperen, con un sistema informático programable de modo tal que se lleve a cabo el procedimiento respectivo. Por eso, el medio de almacenamiento digital puede ser legible por ordenador.

[0088] Por consiguiente, algunas realizaciones que no cubre esta invención comprenden un soporte de datos que tiene señales de control legibles electrónicamente, capaces de cooperar con un sistema informático programable, de modo tal que se lleva a cabo cualquiera de los procedimientos descritos en esta invención.

[0089] En general, las realizaciones de la presente invención se podrían implementar como un producto de programa informático que tiene un código de programa, el código de programa siendo efectivo para realizar cualquiera de los procedimientos cuando el producto de programa informático se ejecuta en un ordenador.

[0090] El código de programa también se puede almacenar en un soporte legible por máquina, por ejemplo.

[0091] Otras realizaciones incluyen el programa informático para realizar cualquiera de los procedimientos descritos en esta invención, dicho programa informático siendo almacenado en un soporte legible a través de una máquina. En otras palabras, una realización del procedimiento inventivo es, por consiguiente, un programa informático que tiene un código de programa para realizar cualquiera de los procedimientos descritos en esta invención, cuando el programa informático se ejecuta en un ordenador. El soporte de datos, el medio de almacenamiento digital o el medio grabado son típicamente tangibles o no volátiles.

[0092] Otra realización que no cubre esta invención es, por consiguiente, un soporte de datos (un medio de almacenamiento digital o un medio legible por ordenador) donde se graba el programa informático para llevar a cabo

cualquiera de los procedimientos descritos en esta invención. El soporte de datos o el medio de almacenamiento digital o el medio legible por ordenador son típicamente tangibles y/o no volátiles.

[0093] Otra realización no cubierta por la invención es, por consiguiente, un flujo de datos o una secuencia de señales que representan el programa informático para realizar cualquiera de los procedimientos descritos en esta invención. El flujo de datos o la secuencia de señales se pueden configurar, por ejemplo, para que se transfieran a través de un enlace de comunicación de datos, por ejemplo, a través de Internet.

[0094] Otra realización no cubierta por la invención comprende un medio de procesamiento, por ejemplo, un ordenador, o un dispositivo lógico programable, configurado o adaptado para realizar cualquiera de los procedimientos descritos en esta invención.

[0095] Otra realización no cubierta por la invención incluye un ordenador donde se instala el programa informático para realizar cualquiera de los procedimientos descritos en esta invención.

[0096] Otra realización no cubierta por la invención incluye un dispositivo o un sistema configurado para transmitir un programa informático para realizar al menos uno de los procedimientos descritos en esta invención a un receptor. La transmisión puede ser electrónica u óptica, por ejemplo. El receptor puede ser, por ejemplo, un ordenador, un dispositivo móvil, un dispositivo de memoria o un dispositivo similar. El dispositivo o sistema puede incluir, por ejemplo, un servidor de archivos para transmitir el programa informático al receptor.

[0097] En algunas realizaciones, se puede usar un dispositivo lógico programable (por ejemplo, una matriz de puerta de campo programable, Field-Programmable Gate Array, FPGA) para realizar algunas o todas las funcionalidades de los procedimientos descritos en esta invención. En algunas realizaciones, una matriz de puerta de campo programable puede cooperar con un microprocesador para realizar cualquiera de los procedimientos descritos en esta invención. En general, los procedimientos se realizan, en algunas realizaciones, mediante cualquier dispositivo de hardware. Dicho dispositivo de hardware puede ser cualquier hardware aplicable de manera universal, tal como un procesador informático (CPU), o puede ser un hardware específico del procedimiento, tal como un ASIC.

[0098] Las realizaciones antes descritas meramente representan una ilustración de los principios de la presente invención. Se entiende que otras personas expertas en la materia valorarán las modificaciones y variaciones de las disposiciones y los detalles descritos en esta invención. Esta es la razón por la que se pretende que la invención solo se limite según el alcance de las siguientes reivindicaciones en lugar de los detalles específicos que se presentaron en esta invención por medio de la descripción y el análisis de las realizaciones.

Bibliografía

[0099]

[1] Cisco, The Zettabyte Era: Trends and Analysis, White Paper, (2014)

[2] US 9,812,640 B2, Complementary resistance switch, contact-connected polycrystalline piezo- or ferroelectric thin film layer, method for encrypting a bit sequence, T. You, H. Schmidt, N. Du, D. Bürger, I. Skorupa, N. Manjunath, 2017

[3] Nan Du y col., J. Appl. Phys. 115, 124501 (2014).

[4] A. Ascoli, V. Senger, R. Tetzlaff, N. Du, O. G. Schmidt y H. Schmidt, “BiFeO3 memristor-based encryption of medical data”, Int. Symp. Circ. y Syst. (ISCAS), 2016.

[5] T. Usted , Y. Shuai, W. Luo, N. Du, D. Bürger, I. Skorupa, R. Hübner, S. Henker, C. Mayr, R. Schüffny, T. Mikolajick, O.G. Schmidt y H. Schmidt, Exploiting Memristive BiFeO3 Bilayer Structures for Compact Sequential Logics, Adv. Funct. Mater. 2014, DOI: 10.1002/adfm.201303365.

[6] WO 2014/111481 A2, Complementary resistor switch, contact-connected polycrystalline piezo- or ferroelectric thin-film layer, method for encrypting a bit sequence, T. You, H. Schmidt, N. Du, D. Bürger, I. Skopura, Y. Shuai, 2014.

REIVINDICACIONES

1. Un codificador (100) para codificar un valor binario de entrada de una secuencia de datos de entrada binarios generando una corriente de salida de una señal de corriente de salida, donde el codificador (100) incluye:

un módulo de control (110); y
un elemento resistivo conmutable (120) configurado para estar en un primer estado o en un segundo estado diferente dependiendo de un primer voltaje de entrada en un primer punto en el tiempo y dependiendo de un segundo voltaje de entrada en un segundo punto en el tiempo posterior,
donde el módulo de control (110) está configurado para aplicar el primer voltaje de entrada al elemento resistivo conmutable (120) en el primer punto en el tiempo de modo que el primer voltaje de entrada depende de dicho valor binario de entrada,
donde el módulo de control (110) está configurado para aplicar el segundo voltaje de entrada al elemento resistivo conmutable (120) en el segundo punto en el tiempo, de modo que el segundo voltaje de entrada depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una primera secuencia de datos pseudoaleatorios binarios,
donde el módulo de control (110) está configurado para aplicar un tercer voltaje de entrada al elemento resistivo conmutable (120) en un tercer punto en el tiempo después del segundo punto en el tiempo, de modo que el tercer voltaje de entrada depende de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una segunda secuencia de datos pseudoaleatorios binarios, y
donde el elemento resistivo conmutable (120) está configurado, al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, para emitir dicha corriente de salida de modo que dicha corriente de salida depende del tercer voltaje de entrada y depende de si el elemento resistivo conmutable (120) está en el primer estado o en el segundo estado,
donde el módulo de control (110) comprende un multiplexor (115) y líneas, donde el multiplexor (115) está configurado para conectar las líneas,
donde el módulo de control (110) está configurado para aplicar el primer voltaje de entrada, el segundo voltaje de entrada y el tercer voltaje de entrada al elemento resistivo conmutable (120) a través de las líneas y a través del multiplexor (115).

2. El codificador (100) según la reivindicación 1,

donde el elemento resistivo conmutable (120) se puede configurar, al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, para emitir dicha corriente de salida,
de modo que dicha corriente de salida comprende un primer valor de corriente de salida si el tercer voltaje de entrada comprende un primer valor de voltaje de entrada y el elemento resistivo conmutable (120) está en el primer estado,
de modo que dicha corriente de salida comprende un segundo valor de corriente de salida mayor que el primer valor de corriente de salida si el tercer voltaje de entrada comprende un segundo valor de voltaje de entrada y el elemento resistivo conmutable (120) está en el primer estado,
de modo que dicha corriente de salida comprende un tercer valor de corriente de salida si el tercer voltaje de entrada comprende el primer valor de voltaje de entrada y el elemento resistivo conmutable (120) está en el segundo estado, y
de modo que dicha corriente de salida comprende un cuarto valor de corriente de salida más pequeño que el tercer valor de corriente de salida si el tercer voltaje de entrada comprende el segundo valor de voltaje de entrada y el elemento resistivo conmutable (120) está en el segundo estado,
donde el primer valor de corriente de salida y el cuarto valor de corriente de salida son iguales o diferentes, y donde el segundo valor de corriente de salida y el tercer valor de corriente de salida son iguales o diferentes.

3. El codificador (100) según la reivindicación 1 o 2,

donde el elemento resistivo conmutable (120) es un memristor.

4. El codificador (100) según cualquiera de las reivindicaciones anteriores,

donde el módulo de control (110) incluye un primer generador pseudoaleatorio (111) configurado para generar la primera secuencia de generador pseudoaleatorio, o
donde el módulo de control (110) incluye el primer generador pseudoaleatorio (111) configurado para generar la primera secuencia de generador pseudoaleatorio, y donde el módulo de control (110) incluye un segundo generador pseudoaleatorio (112) configurado para generar la segunda secuencia de generador pseudoaleatorio.

5. El codificador (100) según cualquiera de las reivindicaciones anteriores,

donde el módulo de control (110) está configurado para vincular dicho valor binario de entrada a dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la segunda secuencia de datos pseudoaleatorios binarios por medio de una operación booleana para obtener un valor binario de combinación,
donde el módulo de control (110) está configurado para aplicar el primer voltaje de entrada al elemento resistivo conmutable (120) en el primer punto en el tiempo de modo que el primer voltaje de entrada depende del valor binario de combinación,
donde el módulo de control (110) está configurado para aplicar el tercer voltaje de entrada al elemento resistivo conmutable (120) en el tercer punto en el tiempo de modo que el tercer voltaje de entrada depende de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la segunda secuencia de datos pseudoaleatorios binarios.

6. El codificador (100) según la reivindicación 5,

donde la operación booleana es una operación XOR o una operación XNOR.

7. El codificador (100) según la reivindicación 5 o 6,

donde el módulo de control (110) está configurado para aplicar el tercer voltaje de entrada al elemento resistivo conmutable (120) en el tercer punto en el tiempo para que el tercer voltaje de entrada no dependa de dicho valor binario de entrada.

8. El codificador (100) según cualquiera de las reivindicaciones anteriores,

donde el módulo de control (110) está configurado para aplicar el primer voltaje de entrada al elemento resistivo conmutable (120) de modo que el primer voltaje de entrada sea positivo o negativo dependiendo de dicho valor binario de entrada, y
donde el módulo de control (110) está configurado para aplicar el segundo voltaje de entrada al elemento resistivo conmutable (120) de modo que el segundo voltaje de entrada sea positivo o negativo dependiendo de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios, y
donde el módulo de control (110) está configurado para aplicar el tercer voltaje de entrada al elemento resistivo conmutable (120) de modo que el tercer voltaje de entrada sea positivo o negativo dependiendo de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o dependiendo de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la segunda secuencia de datos pseudoaleatorios binarios.

9. El codificador (100) según la reivindicación 8,

donde el módulo de control (110) está configurado para determinar una amplitud del primer voltaje de entrada y/o del segundo voltaje de entrada dependiendo de un valor pseudoaleatorio de una tercera secuencia de datos pseudoaleatoria.

10. El codificador (100) según la reivindicación 9,

donde el módulo de control (110) está configurado para determinar uno de tres o más valores de amplitud diferentes para la amplitud del primer voltaje de entrada y/o del segundo voltaje de entrada dependiendo de dicho valor pseudoaleatorio de la tercera secuencia de datos pseudoaleatoria.

11. El codificador (100) según la reivindicación 10,

donde el módulo de control (110) incluye un tercer generador pseudoaleatorio (113) configurado para generar la tercera secuencia de generador pseudoaleatorio de modo que cada valor pseudoaleatorio de la tercera secuencia de datos pseudoaleatorios adopte uno de tres o más valores numéricos diferentes.

12. Un decodificador (200) para decodificar una corriente de entrada de una señal de corriente de entrada emitiendo un valor binario de salida de una secuencia de datos de salida binaria, incluyendo el decodificador (200):

un módulo de control (210),
un elemento resistivo conmutable (220) configurado para estar en un primer estado o en un segundo estado diferente dependiendo de un primer voltaje de entrada en un primer punto en el tiempo y dependiendo de un segundo voltaje de entrada en un segundo punto en el tiempo posterior, y
un comparador (230),
donde el módulo de control (210) está configurado para aplicar el primer voltaje de entrada al elemento resistivo conmutable (220) en el primer punto en el tiempo de modo que el primer voltaje de entrada depende de un valor binario de muestra de una pluralidad de valores binarios de muestra,

donde el módulo de control (210) está configurado para aplicar el segundo voltaje de entrada al elemento resistivo conmutable (220) en el segundo punto en el tiempo, de modo que el segundo voltaje de entrada depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una primera secuencia de datos pseudoaleatorios binarios,
donde el módulo de control (210) está configurado para aplicar un tercer voltaje de entrada al elemento resistivo conmutable (220) en un tercer punto en el tiempo después del segundo punto en el tiempo, de modo que el tercer voltaje de entrada depende de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una segunda secuencia de datos pseudoaleatorios binarios, y
donde el elemento resistivo conmutable (220) está configurado, al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, para proporcionar una corriente de salida al comparador (230) de modo que dicha corriente de salida depende del tercer voltaje de entrada y depende de si el elemento resistivo conmutable (220) está en el primer estado o en el segundo estado,
donde el comparador (230) está configurado para realizar una comparación entre dicha corriente de salida y dicha corriente de entrada, donde el comparador (230) está configurado, dependiendo de la comparación y dicho valor binario de muestra, para determinar dicho valor binario de salida, y donde el comparador (230) está configurado para emitir dicho valor binario de salida,
donde el módulo de control (210) comprende un multiplexor (215) y líneas, donde el multiplexor (215) está configurado para conectar las líneas,
donde el módulo de control (210) está configurado para aplicar el primer voltaje de entrada, el segundo voltaje de entrada y el tercer voltaje de entrada al elemento resistivo conmutable (220) a través de las líneas y a través del multiplexor (215).

13. El decodificador (200) según la reivindicación 12,

donde el comparador (230) está configurado para determinar dicho valor binario de muestra como dicho valor binario de salida y emitir el mismo si una magnitud de una diferencia entre la corriente de salida y dicha corriente de entrada es menor que un valor umbral y,
donde el comparador (230) está configurado para determinar un valor binario invertido de dicho valor binario de muestra como dicho valor binario de salida y emitirlo si una magnitud de una diferencia entre la corriente de salida y dicha corriente de entrada es mayor o igual que el valor umbral.

14. El decodificador (200) según la reivindicación 12 o 13,

donde el elemento resistivo conmutable (220) está configurado, al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, para proporcionar dicha corriente de salida al comparador (230),
de modo que dicha corriente de salida comprende un primer valor de corriente de salida si la tercera tensión de entrada comprende un primer valor de tensión de entrada y el elemento resistivo conmutable (220) está en el primer estado,
de modo que dicha corriente de salida comprende un segundo valor de corriente de salida que es mayor que el primer valor de corriente de salida si el tercer voltaje de entrada comprende un segundo valor de voltaje de entrada y el elemento resistivo conmutable (220) está en el primer estado,
de modo que dicha corriente de salida comprende un tercer valor de corriente de salida si el tercer voltaje de entrada comprende el primer valor de voltaje de entrada y el elemento resistivo conmutable (220) está en el segundo estado, y
de modo que dicha corriente de salida comprende un cuarto valor de corriente de salida que es menor que el tercer valor de corriente de salida si el tercer voltaje de entrada comprende el segundo valor de voltaje de entrada y el elemento resistivo conmutable (220) está en el segundo estado,
donde el primer valor de corriente de salida y el cuarto valor de corriente de salida son iguales o diferentes, y donde el segundo valor de corriente de salida y el tercer valor de corriente de salida son iguales o diferentes.

15. El decodificador (200) según cualquiera de las reivindicaciones 12 a 14,

donde el elemento resistivo conmutable (220) es un memristor.

16. El decodificador (200) según cualquiera de las reivindicaciones 12 a 15,

donde el módulo de control (210) incluye un primer generador pseudoaleatorio (211) configurado para generar la primera secuencia de generador pseudoaleatorio, o
donde el módulo de control (210) incluye el primer generador pseudoaleatorio (211) configurado para generar la primera secuencia de generador pseudoaleatorio, y donde el módulo de control (210) incluye un segundo generador pseudoaleatorio (212) configurado para generar la segunda secuencia de generador pseudoaleatorio.

17. El decodificador (200) según cualquiera de las reivindicaciones 12 a 16,

donde el módulo de control (210) está configurado para vincular dicho valor binario de muestra a dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la segunda secuencia de datos pseudoaleatorios binarios por medio de una operación booleana para obtener un valor binario de combinación,
donde el módulo de control (210) está configurado para aplicar el primer voltaje de entrada al elemento resistivo conmutable (220) en el primer punto en el tiempo de modo que el primer voltaje de entrada depende del valor binario de combinación,
donde el módulo de control (210) está configurado para aplicar el tercer voltaje de entrada al elemento resistivo conmutable (220) en el tercer punto en el tiempo de modo que el tercer voltaje de entrada depende de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la segunda secuencia de datos pseudoaleatorios binarios.

18. El decodificador (200) según la reivindicación 17,

donde la operación booleana es una operación XOR o una operación XNOR.

19. El decodificador (200) según la reivindicación 17 o 18,

donde el módulo de control (210) está configurado para aplicar el tercer voltaje de entrada al elemento resistivo conmutable (220) en el tercer punto en el tiempo para que el tercer voltaje de entrada no dependa de dicho valor binario de muestra.

20. El decodificador (200) según cualquiera de las reivindicaciones 12 a 19,

donde el módulo de control (210) está configurado para aplicar el primer voltaje de entrada al elemento resistivo conmutable (220) de modo que el primer voltaje de entrada sea positivo o negativo dependiendo de dicho valor binario de entrada,
donde el módulo de control (210) está configurado para aplicar el segundo voltaje de entrada al elemento resistivo conmutable (220) de modo que el segundo voltaje de entrada sea positivo o negativo dependiendo de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios, y
donde el módulo de control (210) está configurado para aplicar el tercer voltaje de entrada al elemento resistivo conmutable (220) de modo que el tercer voltaje de entrada sea positivo o negativo dependiendo de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o dependiendo de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la segunda secuencia de datos pseudoaleatorios binarios.

21. El decodificador (200) según la reivindicación 20,

donde el módulo de control (210) está configurado para determinar una amplitud del primer voltaje de entrada y/o del segundo voltaje de entrada dependiendo de un valor pseudoaleatorio de una tercera secuencia de datos pseudoaleatoria.

22. El decodificador (200) según la reivindicación 21,

donde el módulo de control (210) está configurado para determinar uno de tres o más valores de amplitud diferentes para la amplitud del primer voltaje de entrada y/o del segundo voltaje de entrada dependiendo de dicho valor pseudoaleatorio de la tercera secuencia de datos pseudoaleatoria.

23. El decodificador (200) según la reivindicación 22,

donde el módulo de control (210) incluye un tercer generador pseudoaleatorio (213) configurado para generar la tercera secuencia de generador pseudoaleatorio de modo que cada valor pseudoaleatorio de la tercera secuencia de datos pseudoaleatorios adopte uno de tres o más valores numéricos diferentes.

24. El decodificador (200) según cualquiera de las reivindicaciones 12 a 23,

donde cada valor binario de muestra de la pluralidad de valores binarios de muestra siempre comprende el mismo valor binario.

25. Un sistema, que incluye:

un codificador (100) según cualquiera de las reivindicaciones 1 a 11 para codificar un valor binario de entrada de una secuencia de datos de entrada binaria generando una corriente de salida de una señal de corriente de salida, y

un decodificador (200) según cualquiera de las reivindicaciones 12 a 24 para decodificar una corriente de entrada de una señal de corriente de entrada emitiendo un valor binario de salida de una secuencia de datos de salida binaria,
donde el decodificador (200) según cualquiera de las reivindicaciones 12 a 24 está configurado para usar la corriente de salida generada por el codificador (100) según cualquiera de las reivindicaciones 1 a 11 como corriente de entrada y decodificarla.

26. El sistema según la reivindicación 25,

donde la primera secuencia de datos pseudoaleatoria binaria del codificador (100) según cualquiera de las reivindicaciones 1 a 11 y la primera secuencia de datos pseudoaleatoria binaria del decodificador (200) según cualquiera de las reivindicaciones 12 a 24 son iguales,
donde la segunda secuencia de datos pseudoaleatoria binaria del codificador (100) según cualquiera de las reivindicaciones 1 a 11 y la segunda secuencia de datos pseudoaleatoria binaria del decodificador (200) según cualquiera de las reivindicaciones 12 a 24 son iguales,
donde el elemento resistivo conmutable (120) del codificador (100) según cualquiera de las reivindicaciones 1 a 11 y el elemento resistivo conmutable (220) del decodificador (200) según cualquiera de las reivindicaciones 12 a 24 están configurados, al mismo primer voltaje de entrada y al mismo segundo voltaje de entrada, para que ambos estén en el primer estado o para que ambos estén en el segundo estado, y
donde el elemento resistivo conmutable (120) del codificador (100) según cualquiera de las reivindicaciones 1 a 11 y el elemento resistivo conmutable (220) del decodificador (200) según cualquiera de las reivindicaciones 12 a 24 están configurados, al aplicar el mismo tercer voltaje de entrada, para proporcionar o emitir una misma corriente de salida.

27. Un procedimiento para codificar un valor binario de entrada de una secuencia de datos de entrada binarios generando una corriente de salida de una señal de corriente de salida, donde un elemento resistivo conmutable (120) está configurado para estar en un primer estado o en un segundo estado diferente dependiendo de un primer voltaje de entrada en un primer punto en el tiempo y dependiendo de un segundo voltaje de entrada en un segundo punto en el tiempo posterior, incluyendo el procedimiento:

aplicar el primer voltaje de entrada al elemento resistivo conmutable (120) en el primer punto en el tiempo de modo que el primer voltaje de entrada depende de dicho valor binario de entrada;
aplicar el segundo voltaje de entrada al elemento resistivo conmutable (120) en el segundo punto en el tiempo de modo que el segundo voltaje de entrada depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una primera secuencia de datos pseudoaleatorios binarios;
aplicar un tercer voltaje de entrada al elemento resistivo conmutable (120) en un tercer punto en el tiempo después del segundo punto en el tiempo, de modo que el tercer voltaje de entrada depende de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una segunda secuencia de datos pseudoaleatorios binarios; y
al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, emitir dicha corriente de salida por el elemento resistivo conmutable (120); de modo que dicha corriente de salida depende del tercer voltaje de entrada y depende de si el elemento resistivo conmutable (120) está en el primer estado o en el segundo estado,
donde el primer voltaje de entrada, el segundo voltaje de entrada y el tercer voltaje de entrada se aplican al elemento resistivo conmutable (120) a través de líneas y a través de un multiplexor (115), donde el multiplexor (115) está configurado para conectar las líneas.

28. Un procedimiento para decodificar una corriente de entrada de una señal de corriente de entrada emitiendo un valor binario de salida de una secuencia de datos de salida binaria, donde un elemento resistivo conmutable (220) está configurado para estar en un primer estado o en un segundo estado diferente dependiendo de un primer voltaje de entrada en un primer punto en el tiempo y dependiendo de un segundo voltaje de entrada en un segundo punto en el tiempo posterior, el procedimiento incluye:

aplicar el primer voltaje de entrada al elemento resistivo conmutable (220) en el primer punto en el tiempo de modo que el primer voltaje de entrada depende de un valor binario de muestra de una pluralidad de valores binarios de muestra;
aplicar el segundo voltaje de entrada al elemento resistivo conmutable (220) en el segundo punto en el tiempo de modo que el segundo voltaje de entrada depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una primera secuencia de datos pseudoaleatorios binarios;
aplicar un tercer voltaje de entrada al elemento resistivo conmutable (220) en un tercer punto en el tiempo después del segundo punto en el tiempo, de modo que el tercer voltaje de entrada depende de dicho valor binario pseudoaleatorio de la pluralidad de valores binarios pseudoaleatorios de la primera secuencia de datos pseudoaleatorios binarios o depende de un valor binario pseudoaleatorio de una pluralidad de valores binarios pseudoaleatorios de una segunda secuencia de datos pseudoaleatorios binarios;
al aplicar el tercer voltaje de entrada en el tercer punto en el tiempo, proporcionar una corriente de salida por el

elemento resistivo conmutable (220); de modo que dicha corriente de salida depende del tercer voltaje de entrada y depende de si el elemento resistivo conmutable (220) está en el primer estado o en el segundo estado, y realizar una comparación entre dicha corriente de salida y dicha corriente de entrada, determinar dicho valor binario de salida dependiendo de la comparación y de dicho valor binario de muestra, y emitir dicho valor binario de salida, donde el primer voltaje de entrada, el segundo voltaje de entrada y el tercer voltaje de entrada se aplican al elemento resistivo conmutable (120) a través de líneas y a través de un multiplexor (120), donde el multiplexor (215) está configurado para conectar las líneas.

29. Un programa informático que tiene un código de programa que, al ejecutar el programa mediante un ordenador, hace que el mismo realice el procedimiento según la reivindicación 27 o 28.

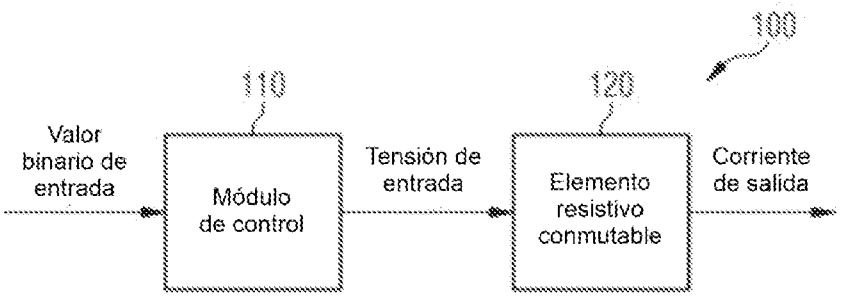

Fig. 1

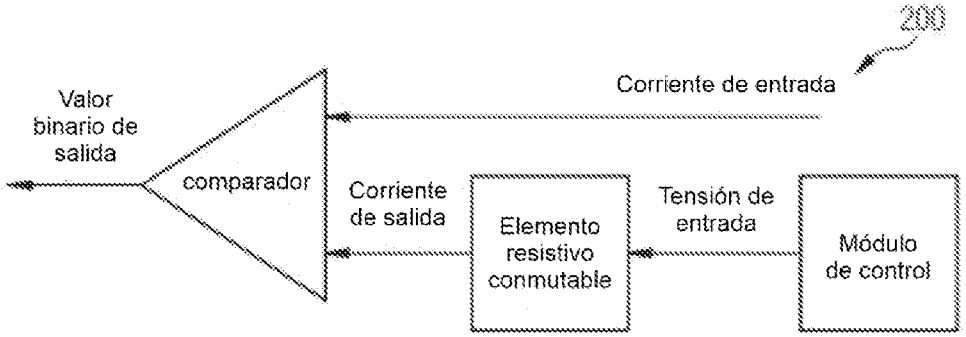

Fig. 2

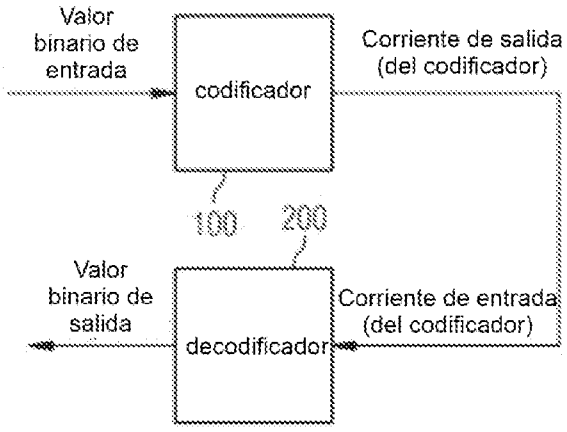

Fig. 3

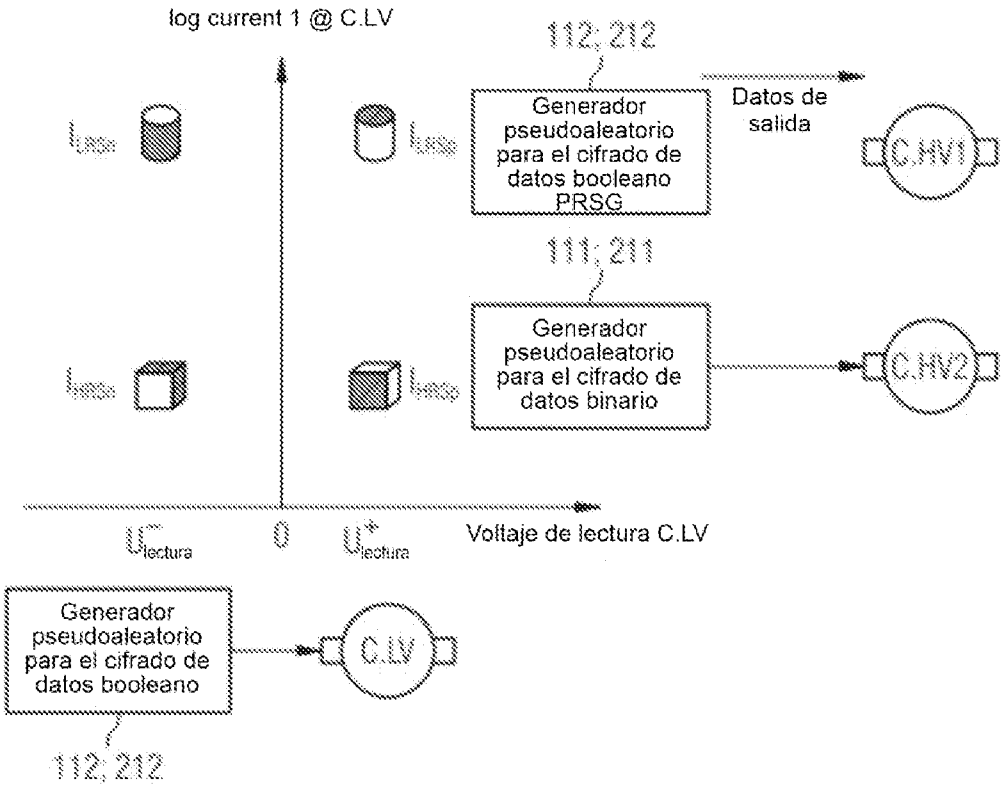
log current 1 @ C.LV
112; 212
Generador pseudoaleatorio para el cifrado de datos booleano PRSG
Datos de salida
C.HV1
111; 211
Generador pseudoaleatorio para el cifrado de datos binario
C.HV2
0
Voltaje de lectura C.LV
Generador pseudoaleatorio para el cifrado de datos booleano
C.LV
112; 212

Fig. 4

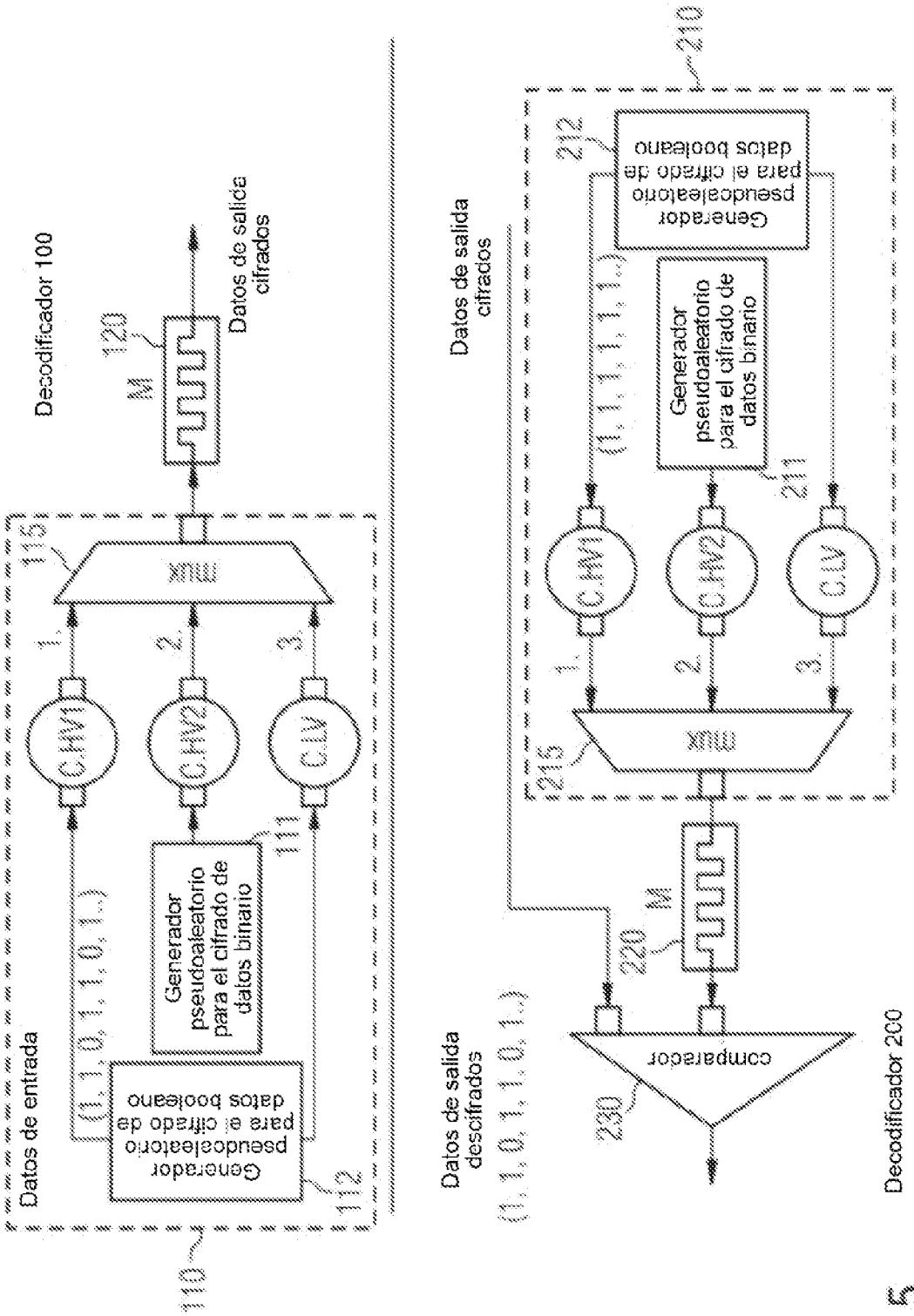
Decodificador 100
Datos de entrada
(1, 1, 0, 1, 1, 0, 1..)
Generador pseudoaleatorio para el cifrado de datos booleano
Generador pseudoaleatorio para el cifrado de datos binario
C.HV1
C.HV2
C.LV
1.
2.
3.
M
115
120
111
112
110
Datos de salida cifrados
Datos de salida descifrados
(1, 1, 0, 1, 1, 0, 1..)
comparador
230
220
215
211
212
210
Decodificador 200

Fig. 5

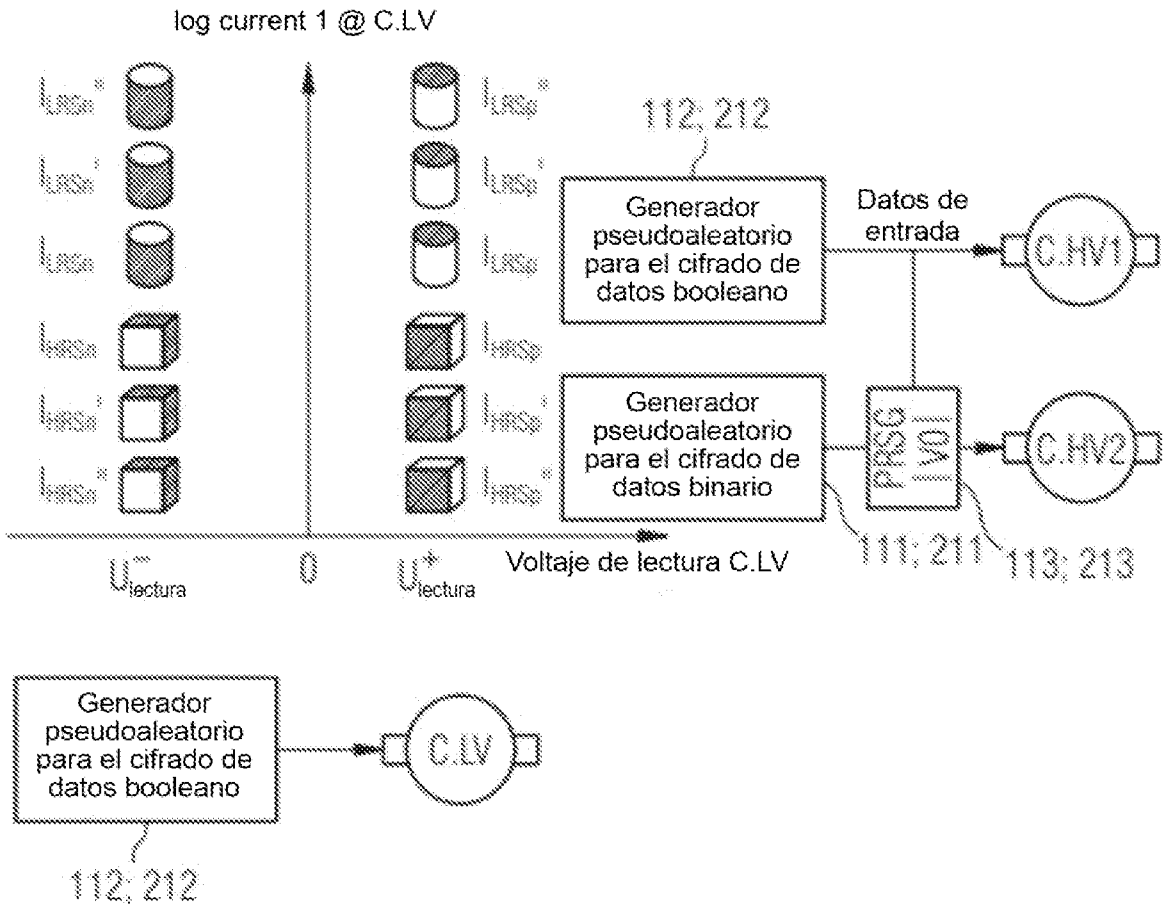
log current 1 @ C.LV
112; 212
Generador pseudoaleatorio para el cifrado de datos booleano
Datos de entrada
C.HV1
Generador pseudoaleatorio para el cifrado de datos binario
PRESET
C.HV2
111; 211
113; 213
0
Voltaje de lectura C.LV
Generador pseudoaleatorio para el cifrado de datos booleano
C.LV
112; 212

Fig. 6

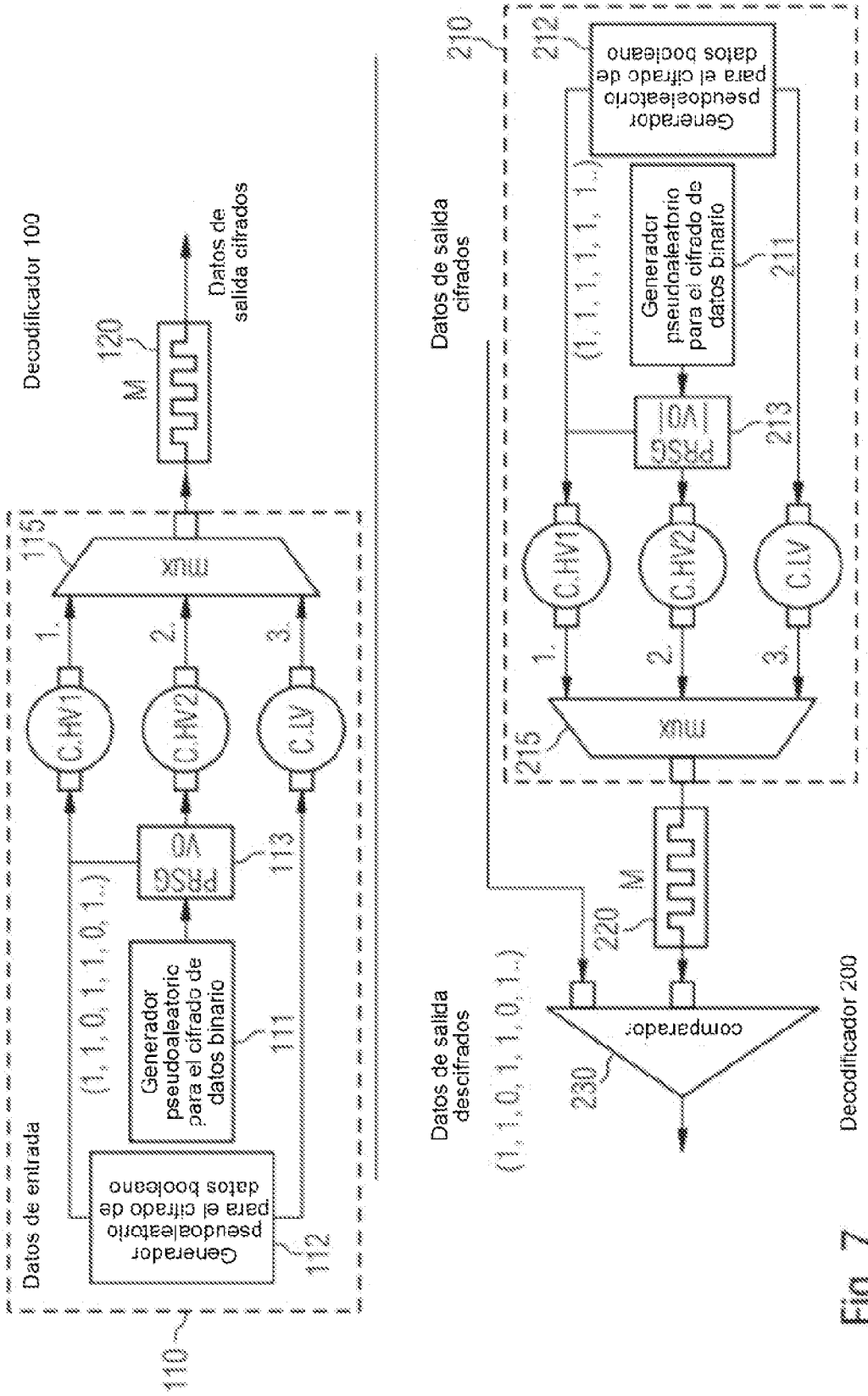
Decodificador 100
Datos de entrada
Datos de salida cifrados
Generador pseudoaleatorio para el cifrado de datos booleano
Generador pseudoaleatorio para el cifrado de datos binario
(1, 1, 0, 1, 1, 0, 1, ..)
C.HV1
C.HV2
C.LV
MUX
SEL
M
110
111
112
113
115
120
1.
2.
3.
Datos de salida descifrados
(1, 1, 0, 1, 1, 0, 1, ..)
Datos de salida cifrados
Generador pseudoaleatorio para el cifrado de datos booleano
Generador pseudoaleatorio para el cifrado de datos binario
(1, 1, 1, 1, 1, 1, 1, ..)
comparador
210
211
212
213
215
216
220
230
Decodificador 200

Fig. 7