(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 593 302**

(51) Int. CI.:

G06K 19/073 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.03.2012 PCT/KR2012/002417**

(87) Fecha y número de publicación internacional: **04.10.2012 WO12134239**

(96) Fecha de presentación y número de la solicitud europea: **30.03.2012 E 12765862 (3)**

(97) Fecha y número de publicación de la concesión europea: **17.08.2016 EP 2693370**

(54) Título: **Aparato y método para generar un valor digital**

(30) Prioridad:

31.03.2011 KR 20110029431
30.03.2012 KR 20120033362

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.12.2016

(73) Titular/es:

ICTK CO., LTD. (100.0%)
2, 3th Floor, Jawon Building, 912-31 Daechi-dong, Gangnam-gu
Seoul 135-280, KR

(72) Inventor/es:

KIM, TAE WOOK;
KIM, DONG KYUE y
CHOI, BYONG DEOK

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Aparato y método para generar un valor digital

Antecedente

1. Campo de la invención

Las realizaciones de ejemplo se relacionan con un campo de seguridad digital, y más en particular, con un aparato y método para generar una clave de identificación (ID) utilizada para un método de codificación y decodificación, una firma digital, y similares que puede ser necesaria para la seguridad de un aparato electrónico, la seguridad integrada de un sistema, la seguridad de un sistema en un chip (SoC), la seguridad de una tarjeta inteligente, la seguridad de un módulo universal de identidad de suscriptor (USIM), y similares.

2. Descripción de la técnica relacionada.

Los recientes desarrollos en tecnología tales como la etiqueta electrónica, y similares, han incrementado la necesidad de insertar una identificación única (ID), que será denominada en lo sucesivo como una clave de ID, a un chip producido en masa. De acuerdo con esto, subsiste el deseo por desarrollar un aparato y método para generar un valor digital aleatorio, por ejemplo, una clave de ID, un ID único, y similares.

Sin embargo, con el fin de utilizar la clave ID como una ID única se puede requerir de un aparato o un chip, un alto nivel de aleatoriedad y una invariancia de tiempo. En este caso, la aleatoriedad puede indicar que las probabilidades de los bits digitales que forman una clave ID generada que corresponden a los valores digitales de “1” y “0” puede ser aleatoria, y la invariancia de tiempo puede indicar que la clave de ID generada puede ser invariante durante el tiempo.

Sin embargo, subsiste un tema porque un aparato para generar un valor digital puede generar un valor digital que puede satisfacer la aleatoriedad deseada, pero no satisfaga el nivel deseado de confiabilidad, esto es, la invariancia de tiempo debido a un ruido, envejecimiento diferencial, y similares.

De acuerdo con esto, subsiste un deseo de un aparato y método para generar un valor digital no clonable que pueda ser insensible al ruido y a los cambios ambientales tal como un cambio en una temperatura externa, y similares, y se pueda garantizar por ser invariante en el tiempo.

El documento US 6, 161, 213 se relaciona con un dispositivo de identificación con circuito integrado (ICID) que va a ser incorporado en un circuito integrado y el cual incluye un arreglo de celdas electrónicas en las cuales la magnitud de una señal de salida de cada celda es una función de variaciones paramétricas que ocurren aleatoriamente que varían de celda a celda. El ICID incluye un circuito para medir la salida de cada celda y para producir datos de salida que tengan un valor que refleje la combinación particular de las características medidas de todos los elementos del arreglo.

El documento US-A1-2008/0279373 se relaciona con un sistema para asegurar un chip de circuito integrado utilizado en un dispositivo electrónico al utilizar un circuito u otra entidad para producir funciones físicamente no clonables (PUF) para generar una palabra de seguridad, tal como un RSA público o una clave privada.

El documento CA-A1-2, 482, 635 se relaciona con la autenticación de circuitos integrados por medio de los cuales se fabrica un grupo de dispositivos con base en un diseño común, teniendo cada dispositivo una correspondiente pluralidad de características medibles que es única en el grupo para ese dispositivo, y cada dispositivo tiene un módulo de medición para medir las características medibles.

Resumen

De acuerdo con aspectos de la invención, se suministra un aparato y método para generar un valor digital, tal como se establece en las reivindicaciones 1 y 11, respectivamente.

En una realización, se suministra un aparato y método que puede generar un valor digital aleatorio que tenga una configuración simple, y puede congelar el valor generado de tal manera que se puede garantizar que es invariante en el tiempo, al configurar una función físicamente no clonabe, (PUF) a través de la variación del proceso de elaboración de un chip semicondutor.

En otra realización se suministra un aparato y método para generar un valor digital, que puede generar un valor digital aleatorio confiable y congela el valor generado de tal manera que este puede ser resistente al ruido y a los cambios ambientales, y se puede garantizar por ser invariante en el tiempo.

De acuerdo con una realización, se suministra un aparato para generar un valor digital, el aparato incluye un generador de valor digital para generar un valor digital aleatorio que utiliza la variación del proceso semiconductor, y una unidad que congela el valor digital que se puede conectar al generador de valor digital, y establecer a uno de un primer estado y un segundo estado basado en el valor digital generado, para congelar el valor digital.

Aquí, el generador de valor digital puede incluir un PUF.

En ciertas realizaciones, el PUF puede incluir un primer inversor y un segundo inversor que puede ser elaborado por un profeso equivalente, y puede tener diferentes valores eléctricos característicos que utilizan variación del proceso en el proceso de elaboración. Un terminal de salida del primer inversor y un terminal de entrada del segundo inversor se puede conectar a un primer nodo, y un terminal de entrada del primer inversor y un terminal de salida del segundo inversor se puede conectar a un segundo nodo que puede diferir del primer nodo. Cuando el primer nodo y el segundo nodo se acortan y posteriormente se abren, el generador de valor digital puede generar el valor digital con base en un nivel lógico de al menos uno del primer nodo y el segundo nodo que se determinan con base en una diferencia en el valor umbral lógico entre los inversores.

En ciertas realizaciones, el PUF puede incluir un amplificador diferencial, y el generador de valor digital puede generar el valor digital al comparar los valores de voltaje de dos nodos de salida cuando los dos nodos de salida del amplificador diferencial se acortan.

En ciertas realizaciones, el PUF puede incluir un cerrojo de establecer – reestablecer (SR), y el generador de valor digital puede generar el valor digital con base en un nivel lógico de al menos uno o dos nodos de salida que se pueden determinar con base en una diferencia en el valor umbral lógico de una compuerta lógica que constituye el cerrojo SR cuando un nivel lógico de “1” es entrado a dos nodos de entrada del cerrojo SR y un nivel lógico de “0” es entrado a los dos nodos de entrada del cerrojo SR.

En ciertas realizaciones, el PUF puede incluir un cerrojo SR, y el generador de valor digital puede generar un valor digital con base en un nivel lógico de al menos uno de dos nodos de salida que se pueden determinar con base en una diferencia en el valor umbral lógico de una compuerta lógica que constituye el cerrojo SR cuando los dos nodos de salida del cerrojo SR se acortan, y luego abrirlo mientras un nivel lógico de “0” es entrado a dos nodos de entrada del cerrojo SR.

En ciertas realizaciones, la unidad de congelamiento del valor digital puede incluir al menos un fusible que puede saltar o no saltar para congelar el valor digital, al recibir una sobrecorriente que corresponde al valor digital generado durante una primera operación del generador de valor digital.

En este caso, el primer estado puede corresponder a un estado en el cual el al menos un fusible puede saltar, y el segundo estado puede corresponder a un estado en el cual el al menos un fusible puede no saltar.

En ciertas realizaciones, la unidad de congelamiento del valor digital puede incluir al menos un dispositivo programable por una vez (OTP) que se puede programar con base en el valor digital generado durante una primera operación del generador de valor digital para congelar el valor digital.

De acuerdo con otro aspecto también se suministra un aparato para generar un valor digital, el aparato incluye un generador de valor digital para generar un valor digital aleatorio que utiliza la variación del proceso semiconductor, y, una unidad de almacenamiento del valor digital, conectada al generador de valor digital, para almacenar el valor digital generado.

Aquí, el generador de valor digital puede incluir un PUF.

En ciertas realizaciones, el PUF puede incluir un primer inversor y un segundo inversor que se pueden elaborar mediante un proceso equivalente, y pueden tener diferentes valores característicos eléctricos que utilizan la variación del proceso en el proceso de elaboración. Un terminal de salida del primer inversor y un terminal de entrada del segundo inversor se pueden conectar a un primer nodo, y un terminal de entrada del primer inversor y un terminal de salida del segundo inversor se pueden conectar a un segundo nodo que puede diferir del primer nodo. Cuando el primer nodo y el segundo nodo se acortan y luego se abren, el generador de valor digital puede generar el valor digital con base en el nivel lógico de al menos uno del primer nodo y el segundo nodo.

En ciertas realizaciones, el PUF puede incluir un amplificador diferencial, y el generador de valor digital puede generar el valor digital al comparar los valores de voltaje de dos nodos de salida cuando los dos nodos de entrada del amplificador diferencial se acortan.

En ciertas realizaciones, el PUF puede incluir un cerrojo SR, y el generador de valor digital puede generar el valor digital con base en el nivel lógico de al menos uno de dos nodos de salida que se puede determinar con base en una diferencia en el valor umbral lógico de una compuerta lógica que constituye el cerrojo SR cuando un nivel lógico de “1” es entrado a dos nodos de entrada del cerrojo SR, y luego un nivel lógico de “0” es entrado a los dos nodos de entrada del cerrojo SR.

En ciertas realizaciones, el PUF puede incluir un cerrojo SR, y el generador de valor digital puede generar el valor digital con base en el nivel lógico de al menos uno de dos nodos de salida que se puede determinar con base en la diferencia en un valor umbral lógico de una compuerta lógica que constituye el cerrojo SR cuando los dos nodos de salida del cerrojo SR se acortan, y luego abrirlo mientras un nivel lógico de “0” es entrado a los dos nodos de entrada del cerrojo SR.

La unidad de almacenamiento de valor digital puede incluir al menos un dispositivo de memoria no volátil que puede almacenar el valor digital generado durante la primera operación del generador de valor digital.

En este caso, el al menos un dispositivo de memoria no volátil puede corresponder a un dispositivo programable multitiempo o programable muchas veces (MTP)

El al menos un dispositivo de memoria no volátil puede corresponder al menos a uno de una memoria eléctricamente borrable y programable de solo lectura (EEPROM), una memoria flash, una memoria de Silixio-Oxido – Nitruro - Oxido – silicio (SONOS), una Memoria de Acceso Aleatoria Ferroeléctrica (FRAM), y una Memoria Resistiva de Acceso Aleatorio (RRAM).

De acuerdo con otro aspecto se suministra un método para generar un valor digital, el método incluye generar, mediante un generador de valor digital de un aparato para generar un valor digital, un valor digital aleatorio que utilice la variación de proceso de al menos un dispositivo incluido en el generador de valor digital, y congelar, mediante una unidad de congelamiento de valor digital que se conecta al generador de valor digital, el valor digital generado cuando la unidad de congelamiento de valor digital se fija a uno de un primer estado y a un segundo estado con base en el valor digital generado.

En este caso, el congelamiento del valor digital puede incluir aplicar una sobrecorriente a al menos un fusible incluido en la unidad de congelamiento de valor digital, con base en el valor digital generado durante una primera operación del generador de valor digital, y congelar el valor digital dependiendo de si el al menos un fusible se salta por la sobrecorriente.

El congelamiento del valor digital puede incluir programar al menos un dispositivo OTP incluido en la unidad de congelamiento de valor digital, con base en el valor digital generado en una primera operación del generador de valor digital, el congelamiento del valor digital dependiendo de si se programa el al menos un dispositivo OTP.

De acuerdo con otro aspecto se suministra un método para generar un valor digital, el método incluye generar, mediante un generador de valor digital de un aparato para generar un valor digital, un valor digital aleatorio que utiliza la variación de proceso de al menos un dispositivo incluido en el generador de valor digital, y almacenar, mediante una unidad de almacenamiento de valor digital que está conectada al generador de valor digital, el valor digital generado.

En este caso, el almacenamiento del valor digital puede incluir programar al menos un dispositivo de memoria no volátil incluido en el generador de valor digital, con base en el valor digital generado.

El al menos un dispositivo de memoria no volátil puede corresponder a un dispositivo MTP.

El al menos un dispositivo de memoria no volátil puede corresponder a al menos uno de EEPROM, una memoria flash, una memoria SONOS, una FRASM y una RRAM.

Efecto de la invención

De acuerdo con realizaciones de ejemplo, una configuración de un circuito que puede generar un valor digital que utiliza la variación de proceso en la elaboración de un chip semiconductor puede ser simple y se puede satisfacer la invariancia de tiempo, por medio de la cual se puede incrementar la confiabilidad del valor digital.

De acuerdo con realizaciones de ejemplo, aunque se puede elaborar otro chip semiconductor bajo el mismo diseño, una clave de identificación idéntica (ID) puede no ser generada y un chip semiconductor puede ser no clonable y así, se puede garantizar alta seguridad.

Breve descripción de los dibujos

Estos y/u otros aspectos, características y ventajas de la invención serán evidentes y más fácilmente apreciados de la siguiente descripción de las realizaciones de ejemplo, tomadas en conjunto con los dibujos que la acompañan en los cuales:

La Figura 1 es un diagrama de bloque que ilustra un aparato para generar un valor digital de acuerdo con una realización de ejemplo;

La Figura 2 es un diagrama que ilustra una configuración de una unidad de congelamiento de valor digital de acuerdo con una realización de ejemplo;

La Figura 3 es un diagrama que ilustra una configuración de una unidad de congelamiento del valor digital de acuerdo con otra realización de ejemplo;

La Figura 4 es un diagrama de bloque que ilustra un aparato para generar un valor digital de acuerdo con otra realización de ejemplo;

La Figura 5 es un diagrama que describe una configuración de un generador de valor digital de acuerdo con una realización de ejemplo;

La Figura 6 es una gráfica que explica una operación del generador de valor digital de la Figura 5;

La Figura 7 es un diagrama que ilustra una configuración de un generador de valor digital de acuerdo con otra realización de ejemplo;

Las Figuras 8A y 8B son diagramas que ilustran una configuración de un generador de valor digital de acuerdo con otra realización de ejemplo;

La Figura 9 es un diagrama que ilustra una configuración de un generador de valor digital de acuerdo con otra realización de ejemplo;

La Figura 10 es un diagrama que ilustra una configuración de un aparato para generar un valor digital en la cual una unidad de congelamiento de valor digital de acuerdo con la realización de la Figura 2 se combina con un generador de valor digital de acuerdo con una realización de ejemplo de las Figuras 8A u 8B;

La Figura 11 es una gráfica que ilustra un proceso de congelamiento de un valor digital mediante una unidad de congelamiento de valor digital de acuerdo con una realización de ejemplo en la Figura 10;

Las Figuras 12A a 12D son diagramas en los cuales una unidad de congelamiento de valor digital está dispuesta en un aparato para generar un valor digital de acuerdo con diversas realizaciones de ejemplo;

Las Figuras 13A a 13D son diagramas que ilustran varias configuraciones de la unidad de congelamiento del valor digital cuando la unidad de congelamiento del valor digital se configura utilizando un dispositivo programable por una vez (OTP) de acuerdo con una realización de ejemplo;

Las Figuras 14A a 14E son diagramas en los cuales la unidad de congelamiento del valor digital se dispone en un aparato para generar un valor digital cuando un generador de valor digital se configura de acuerdo a la realización de la Figura 5 de acuerdo con una realización de ejemplo;

Las Figuras 15A a 15E son diagramas que ilustran varias configuraciones de una unidad de congelamiento de valor digital cuando el generador de valor digital se configura de acuerdo a la realización de la Figura 5 y en la unidad de congelamiento del valor digital se configura utilizando un dispositivo OTP, de acuerdo con una realización de ejemplo;

Las Figuras 16A a 16D son diagramas en los cuales una unidad de congelamiento de valor digital se dispone en un aparato para generar un valor digital cuando el generador de valor digital se configura de acuerdo con una realización de la Figura 7, de acuerdo con otra realización de ejemplo;

Las Figuras 17A a 17D son diagramas que ilustran varias configuraciones de una unidad de congelamiento de valor digital cuando el generador de valor digital se configura de acuerdo con una realización de la Figura 7 y la unidad de congelamiento de valor digital se configura utilizando un dispositivo OTP, de acuerdo con otra realización de ejemplo;

La Figura 18 es un diagrama de flujo que ilustra un método para generar un valor digital de acuerdo con una realización de ejemplo; y

La Figura 19 es un diagrama de flujo que ilustra un método para generar un valor digital de acuerdo con otra realización de ejemplo.

Descripción detallada

Se hará ahora referencia en detalle a las realizaciones de ejemplo de la presente divulgación, cuyos ejemplos se ilustran en los dibujos que la acompañan, en donde los numerales de referencia similares se refieren a elementos similares en todas partes. Las realizaciones de ejemplo se describen abajo para explicar la presente divulgación al referirse a las figuras.

La Figura 1 es un diagrama de bloque que ilustra un aparato 100 para generar un valor digital de acuerdo a una realización de ejemplo.

El aparato 100 puede incluir un generador 110 de valor digital, y una unidad 120 de congelamiento de valor digital.

El generador 110 de valor digital puede generar un valor digital aleatorio en respuesta a una señal que se puede aplicar al generador 110 de valor digital. El valor digital aleatorio se puede generar utilizando la variación del proceso semiconductor que puede ocurrir en un proceso de fabricación de al menos un dispositivo semiconductor que constituye el generador 110 de valor digital. Lo anterior se describirá con más detalle.

La variación del proceso semiconductor puede ocurrir por varias razones. Por ejemplo, cuando se va a fabricar un transistor, la variación del proceso se puede originar por los parámetros de diseñó, por ejemplo, una longitud de compuerta eficiente, un coeficiente asociado con la concentración del dopaje, un índice asociado con un grosor del óxido, un voltaje umbral, y similares. La variación del proceso semiconductor puede dar como resultado de un fenómeno natural y puede ser reducida.

Generalmente, un proceso de elaboración de un semiconductor que tenga una variación infinitesimal del proceso se puede considerar como excelente. De acuerdo con esto, se han hecho varios intentos para reducir la variación del proceso en el campo tecnológico de un proceso semiconductor.

Sin embargo, el generador 110 de valor digital puede generar un valor digital aleatorio que utiliza la variación del proceso semiconductor. Por ejemplo, el valor digital aleatorio puede corresponder a uno de un valor de “1” y “0”.

Cuando el generador 110 de valor digital genera un valor digital aleatorio que utiliza la variación del proceso semiconductor, un problema que se relaciona con la invariancia de tiempo puede surgir debido a un cambio ambiental, por ejemplo, ruido, envejecimiento diferencial, temperaturas externas (por ejemplo ambiente) y similares. La invariancia de tiempo se puede relacionar con la confiabilidad basada en si el valor digital generado se puede utilizar en los campos de seguridad y autenticación y así, exista una demanda para una solución del problema anteriormente mencionado.

De acuerdo con esto, en ciertas realizaciones, la unidad 120 de congelamiento del valor digital puede garantizar la invariancia de tiempo para el valor digital generado por el generador 110 de valor digital, de tal manera que el valor digital es resistente al cambio ambiental, por ejemplo, ruido, temperaturas externas, y similares.

En ciertas realizaciones, la unidad 120 de congelamiento del valor digital se puede conectar al generador 110 de valor digital, y se puede establecer en uno de un primer estado y un segundo estado con base en el valor digital generado por el generador 110 de valor digital para congelar el valor digital.

Cada uno del primer estado y del segundo estado puede corresponder a los valores utilizados para leer el valor digital generado, por ejemplo, los valores que corresponden a “1” o “0”.

En lo sucesivo, varias realizaciones se describirán con referencia a las Figuras 2 a 19. Las realizaciones de ejemplo de la unidad 120 de congelamiento de valor digital se describirán con referencia a las Figuras 2 y 3, y las realizaciones de ejemplo del generador 110 de valor digital se describirán con referencia a las Figuras 5 a 9.

Adicionalmente, las realizaciones de ejemplo que incluyen el generador 110 de valor digital y la unidad 120 de congelamiento de valor digital se describirán con referencia a las Figuras 10 a 17D.

De acuerdo con ciertas realizaciones, la unidad de almacenamiento de valor digital que almacena y suministra el valor digital generado se puede incluir, en lugar de la unidad 120 de congelamiento del valor digital, para garantizar la invariancia de tiempo. La unidad de almacenamiento de valor digital se describirá con referencia a la Figura4

La Figura 2 es un diagrama que ilustra una configuración de la unidad 120 de congelamiento de valor digital de la Figura 1 de acuerdo con una realización de ejemplo.

En ciertas realizaciones, la unidad 120 de congelamiento de valor digital del aparato 100 en la Figura 1 puede incluir una unidad 210 de fusible que incluye un fusible 201 y un fusible 202, y una unidad 220 de control de fusible para cambiar los estados de conexión física del fusible 201 y el fusible 202, con base en el valor digital generado.

Cuando el generador 110 de valor digital de la Figura 1 suministra, a través del terminal OUT y un terminal OUT_BAR, valores digitales complementarios, por ejemplo, un valor de “1” y un valor de “0”, la unidad 220 de control de fusible de la unidad 120 de congelamiento de valor digital puede transferir una señal C de control y una señal Cb de control al fusible 201 y al fusible 202 incluido en la unidad 210 de fusible, respectivamente. Cuando se aplica una sobrecorriente a una del fusible 201 y el fusible 202, con base en la señal C de control y la señal Cb de control, uno del fusible 201 y el fusible 202 puede saltar.

Por ejemplo, cuando un valor del terminal OUT corresponde a “1” la unidad 220 de control de fusible puede hacer saltar el fusible 201. En este caso, además del caso del salto del fusible que corresponde a un valor digital de “1” un caso inverso del salto del fusible corresponde a un valor digital de “0” que también puede ser posible. En lo sucesivo, aunque se describen realizaciones con respecto al valor digital de “1” o “0”, también pueden ser posibles otras realizaciones.

Con el fin de que un fusible salte, al menos un terminal entre los terminales 211, 212, 213 y 214 del fusible 201 y el fusible 202 se puede conectar a un voltaje V_{DD} o a tierra. También, dependiendo de las realizaciones, los terminales 211, 212, 213, y 214 se pueden conectar a una pluralidad de nodos incluidos en el generador 110 de valor digital, respectivamente. Las realizaciones anteriores se describirán en detalle con referencia a las Figuras 12A a 12D, 14A a 14E y 16A a 16D

La unidad 120 de congelamiento del valor digital, puede cambiar un estado físico, con base en el valor digital generado por el generador 110 de valor digital, y se pueden fijar a un estado irreversible. De acuerdo con esto, la invariancia de tiempo, para el valor digital aleatorio generado por el generador 110 de valor digital se puede garantizar.

Cuando el valor digital va a ser leído en el futuro, el valor digital se puede leer al identificar un fusible saltado o un fusible no saltado del fusible 201 y el fusible 202 incluido en la unidad 210 de fusible de la unidad 120 de congelamiento de valor digital.

De acuerdo con otra realización de ejemplo, el estado de conexión de un circuito de un aparato para generar un valor digital se puede establecer con base en un resultado de identificar un fusible saltado o un fusible no saltado del fusible 201 y el fusible 202, por medio del cual el valor de salida del generador 110 de valor digital se puede congelar, y el valor de salida se puede leer como el valor digital.

Para facilidad de referencia, de acuerdo con una realización, el generador 110 de valor digital puede incluir N celdas unitarias que pueden generar un valor digital único o un par de valores digitales complementarios para generar un valor digital de N-bits. Aquí, N puede corresponder a un número natural.

En este caso, la unidad 120 de congelamiento de valor digital puede incluir N unidades de fusible, para congelar el valor digital de N-bits. Aquí, cuando tanto el fusible 201 como el fusible 202 de la unidad 210 de fusible que corresponden a una celda unitaria predeterminada se saltan, o por el contrario, cuando tanto el fusible 201 como el fusible 202 no se saltan, un valor de la correspondiente celda unitaria se puede considerar como “invalido”.

Aquí, aunque se puede describir, para facilidad de la descripción, que el generador 110 de valor digital puede generar un valor digital único o un par de valores digitales, la presente invención no está limitada a la realización anterior.

De acuerdo con esto, al menos que se mencione otra cosa, las N celdas unitarias se pueden incluir en el generador 110 de valor digital, y los N valores digitales se pueden generar y congelar o almacenar, de acuerdo a la escalabilidad de un circuito.

Además, con referencia a la configuración de la unidad 210 de fusible de la Figura 2, aunque se puede describir que el valor digital se puede congelar al cambiar el estado físico con base en el valor digital generado por el generador 110 de valor digital, lo anterior se puede suministrar como solamente una realización de ejemplo. Cualquiera otra de las realizaciones modificadas para suministrar la invariancia de tiempo para el valor digital generado al cambiar una estructura física con base en el valor digital generado se puede incluir.

En ciertas realizaciones, la unidad 120 de congelamiento de valor digital se puede configurar utilizando un dispositivo programable por una vez (OTP). Aunque la unidad 210 de fusible que puede almacenar el valor digital generado una vez mediante un cambio en el estado físico se puede considerar como un dispositivo OTP, un dispositivo programable por una vez, diferente de una configuración de la unidad 210 de fusible, se denominará en lo sucesivo como un dispositivo OTP, como un ejemplo de una memoria no volátil. La realización anterior se describirá en detalle con referencia a la Figura 3

La Figura 3 es un diagrama que ilustra una configuración de la unidad de congelamiento de valor digital de acuerdo con otra realización de ejemplo.

Cuando un par de valores digitales generados por el generador 110 de valor digital se transfiere a la unidad 330 de control a través del terminal OUT y un terminal OUT_BAR, las compuertas de los dispositivos OTP incluidas en la unidad 120 de congelamiento del valor digital se puede controlar con base en la señal C de control y la señal Cb de control de la unidad 330 de control, por medio de la cual el valor digital se puede programar en los dispositivos 310 y 320 OTP no volátiles. En este caso, una vez que se programa el valor digital, el valor digital puede ser invariante.

De acuerdo con esto, de manera similar a las descripciones que se relacionan con la unidad 210 de fusible de la Figura 2, la invariancia de tiempo para un valor digital aleatorio generado por el generador 110 de valor digital se puede garantizar.

Por ejemplo, cuando un valor digital de “1” es transferido a la unidad 330 de control a través del terminal OUT, y un valor digital de “0” se transfiere a la unidad 330 de control, a través del terminal OUT_BAR, el valor digital de “1” se puede programar en el dispositivo 310 OTP, y el valor digital de “0” se puede programar en el dispositivo 320 OTP, con base en la señal C de control y la señal Cb de control de la unidad 330 de control. En ciertas realizaciones, puede no ser posible reescribir los valores programados.

Los terminales de ambos extremos de los dispositivos 310 y 320 OTP se pueden conectar a una pluralidad de nodos en el aparato 100 consistente con las realizaciones descritas, y varios ejemplos de tales conexiones se describirán posteriormente con referencia a las Figuras 13A a 13D, 15A a 15E y 17A a 17D.

Varias realizaciones pueden describir un método para configurar los dispositivos 310 y 320 OTP, a una memoria programable de solo lectura (PROM) o a una memoria programable de campo de solo lectura (FPROM). En las

realizaciones de las Figuras 1 a 3, en un proceso de aplicar un voltaje o una corriente al aparato 100, un valor digital de un par de valores digitales se puede generar utilizando la variación del proceso de uno o unos dispositivos semiconductores en el generador 110 de valor digital, y el valor digital del par de valores digitales se puede congelar inmediatamente en la unidad 210 de fusible o los dispositivos 310 y 320 OTP.

Sin embargo, consistente con las realizaciones descritas, el proceso de congelamiento se puede sustituir con un proceso de almacenar el valor digital generado en una memoria no volátil. Tales realizaciones se describirán con referencia a la Figura 4.

La Figura 4 es un diagrama de bloque que ilustra un aparato 400 para generar un valor digital de acuerdo con otra realización de ejemplo.

Un generador 410 de valor digital puede generar valores digitales complementarios para un terminal OUT y un terminal OUT_BAR, respectivamente, y los valores digitales se pueden almacenar en una unidad 420 de almacenamiento de valor digital que corresponde a una memoria no volátil.

La unidad 420 de almacenamiento de valor digital se puede configurar utilizando el dispositivo OTP anteriormente mencionado, o se puede configurar utilizando un dispositivo programable multitiempo o programable muchas veces (MTP).

El dispositivo MTP puede incluir todas las memorias no volátiles con una característica reescribible. El dispositivo MTP típicamente incluye cualquier tipo de memoria no volátil por ejemplo una memoria de solo lectura eléctricamente borrable y programable (EEPROM), una memoria flash, una memoria de Silicio- Óxido- Nitruro-Óxido-Silicio (SONOS), una memoria de Acceso Aleatorio Ferroelectrico (FRAM) una memoria de Acceso Aleatorio Resistiva (RRAM) y similares.

De acuerdo con esto, cuando la unidad 420 de almacenamiento de valor digital se configura utilizando el dispositivo MTP, pueden ser posibles realizaciones de una amplia variedad de esquemas de configuración.

En las realizaciones de las Figuras 1 a 3, cuando se genera un valor digital mediante el generador 110 de valor digital, el valor digital correspondiente se puede programar en la unidad 210 de fusible o los dispositivos 310 y 320 OTP y el valor digital programado puede ser irreversible y puede no regresar al valor preprogramado, sea física y eléctricamente. De acuerdo con esto, se ha expresado que el valor digital se congela.

Sin embargo, aunque la irreversibilidad puede no garantizarse en una realización descrita con referencia a la Figura 4, el valor digital generado por el generador 410 de valor digital se puede almacenar en la unidad 420 de almacenamiento de valor digital que corresponde a un dispositivo de memoria no volátil cuando se requiere reducir los gastos de elaboración y/o configuración o surgen otras varias necesidades.

Ya que puede existir una probabilidad de que la unidad 420 de almacenamiento de valor digital de la realización de la Figura 4 se pueda reprogramar, se puede garantizar una invariancia del nivel de tiempo considerablemente alta cuando se evita reescribir la unidad 420 de almacenamiento de valor digital.

Aunque se ha descrito que la unidad 420 de almacenamiento de valor digital se configura utilizando un dispositivo de memoria no volátil, se pueden incluir modificaciones a cualquiera de los tipos de dispositivos de memoria que puedan garantizar la invariancia de tiempo al almacenar el valor digital generado por el generador 410 de valor digital.

En lo sucesivo, varias realizaciones para configuraciones del generador 110 o 410 de valor digital se describirá con detalle con referencia a las Figuras 5 a 9.

La Figura 5 es un diagrama para describir una configuración del generador 110 o 410 de valor digital de acuerdo con una realización de ejemplo.

El generador 110 o 410 de valor digital se puede configurar utilizando un circuito 500 de la Figura 5.

Un primer inversor 510 puede tener un primer valor umbral lógico. Un segundo inversor 540 puede tener un segundo valor umbral lógico. Un valor umbral lógico se puede referir a un voltaje cuando un voltaje de entrada de un inversor es idéntico a un voltaje de salida del inversor. El valor del umbral lógico se puede medir utilizando un voltaje cuando un terminal de salida de un inversor es corrientemente operado y un terminal de entrada del inversor se acorta.

Los inversores elaborados mediante procesos equivalentes se pueden diseñar para tener valores umbrales lógicos idénticos. Sin embargo, ya que puede existir una variación en el proceso semiconductor en un proceso de elaboración real como se describió anteriormente, puede ser posible que dos inversores elaborados no tengan valores umbrales lógicos perfectamente idénticos.

De acuerdo con una realización de ejemplo, el primer inversor 510 y el segundo inversor 540 se pueden elaborar mediante un proceso de elaboración equivalente, y puede existir diferencia entre los valores umbrales lógicos que resultan de la variación del proceso semiconductor.

La diferencia entre los valores umbrales lógicos puede depender de los procesos, y puede corresponder a, por ejemplo, un tamaño de aproximadamente pocos milivoltios a decenas de milivoltios. De acuerdo con esto, el valor umbral lógico del primer inversor 510 y el valor umbral lógico del segundo inversor 540 puede no ser comparado de manera precisa utilizando un circuito comparador separado, debido a un error en la medición.

De acuerdo con esto, se describirá un método para comparar los valores umbrales lógicos del primer inversor 510 y el segundo inversor 540, sin utilizar un circuito comparador separado, con base en el circuito 500 de la Figura 5.

A través del uso del circuito 500, se puede determinar cuál del primer inversor 510 y el segundo inversor 540 tiene mayor valor umbral lógico, al comparar los valores umbrales lógicos relativos del primer inversor 510 y el segundo inversor 540.

Cuando el segundo inversor 540 está ausente, un voltaje de salida del primer inversor 510 es igual que el valor umbral lógico del primer inversor 510 cuando un terminal de entrada y un terminal de salida del primer inversor 510 se acortan.

También, cuando el primer inversor 510 está ausente, un voltaje de salida del segundo inversor 540 es igual que el valor umbral lógico del segundo inversor 540 cuando el terminal de entrada y el terminal de salida del segundo inversor 540 se acortan.

Sin embargo, como se mostró en la Figura 5, cuando el terminal de entrada del primer inversor 510 y el terminal de salida de segundo inversor se acortan con el fin de ser conectados al primer nodo 501, y el terminal de salida del primer inversor 510 y el terminal de entrada del segundo inversor 540 se acortan con el fin de ser conectados a un segundo nodo 502, se pueden producir diferentes resultados.

Cuando el primer nodo 501 y el segundo nodo 502 se acortan al cerrar un interruptor 530, los valores de voltaje del primer nodo 501 y el segundo nodo 502 que se acortan pueden corresponder a un valor entre el valor umbral lógico del primer inversor 510 y el valor umbral lógico del segundo inversor 540. En lo sucesivo, el valor puede no corresponder a un valor promedio de los valores umbrales lógicos del primer inversor 510 y el valor umbral lógico del segundo inversor 540.

Sin importar cual del primer inversor 510 y el segundo inversor 540 tengan un mayor valor umbral, un voltaje del primer nodo 501 y un voltaje del segundo nodo 502 pueden corresponder a un valor entre el valor umbral lógico del primer inversor 510 y el valor umbral lógico del segundo inversor 540 aunque el interruptor 530 esté cerrado.

Cuando el primer nodo 501 y el segundo nodo 502 se abren al abrir el interruptor 530, el nivel lógico del voltaje de uno del primer nodo 501 y el segundo nodo 502 pueden corresponder a “0”, y un nivel lógico de un voltaje del otro del primer nodo 501 y el segundo nodo 502 puede corresponder a “1”.

Por ejemplo, en el caso del valor umbral lógico del primer inversor 510 que es inferior que el valor umbral lógico del segundo inversor 540, el voltaje del primer nodo 501 puede ser mayor que el valor umbral lógico del primer inversor 510 mientras que el primer nodo 501 y el segundo nodo 502 se acortan al cerrar el interruptor 530.

De acuerdo con esto, cuando el primer nodo 501 y el segundo nodo 502 se abren al reabrir el interruptor 530, el primer inversor 510 puede reconocer el voltaje del primer nodo 501 que corresponde al terminal de entrada del primer inversor 510 como un nivel lógico HIGH y puede controlar un voltaje del segundo nodo 502 que corresponde al terminal de salida del primer inversor 510 por ser un nivel lógico LOW.

En este caso, el segundo inversor 540 puede reconocer el voltaje del segundo nodo 502 que corresponde al terminal de entrada del segundo inversor 540 como un nivel lógico LOW y puede controlar el voltaje del primer nodo 501 que corresponde al terminal de salida del segundo inversor 540 por ser un nivel lógico HIGH.

Consecuentemente, el nivel lógico del voltaje del segundo nodo 502 que corresponde a una salida OUT del circuito 500 puede ser HIGH.

Por el contrario, cuando el valor umbral lógico del primer inversor 510 se asume como mayor que el valor umbral lógico del segundo inversor 540, el voltaje del primer nodo 501 puede ser inferior que el valor umbral lógico del primer inversor 510 mientras que el primer nodo 501 y el segundo nodo 502 se acortan al cerrar el interruptor 530.

De acuerdo con esto, cuando el primer nodo 501 y el segundo nodo 502 se abren al abrir el interruptor 530 de nuevo, el primer inversor 510 puede reconocer el voltaje del primer nodo 501 que corresponde al terminal de entrada del primer inversor 510 como un nivel lógico LOW, y pueden controlar el voltaje del segundo nodo 502 que corresponde al terminal de salida del primer inversor 510 para ser un nivel lógico HIGH.

En este caso, el segundo inversor 540 puede reconocer el voltaje del segundo nodo 502 que corresponde al terminal de entrada del segundo inversor 540 como un nivel lógico HIGH, y puede controlar el voltaje del primer nodo 501 que corresponde al terminal de salida del segundo inversor 540 por ser un nivel lógico LOW.

Consecuentemente, el nivel lógico del voltaje del segundo nodo 502 que corresponde a la salida OUT del circuito 500 puede ser LOW.

Como se mencionó anteriormente, el nivel lógico de la salida OUT después del interruptor 530 se acorta y abre puede corresponder a HIGH, esto es, un valor digital de “1” o LOW, esto es, un valor digital de “0”, con base en el cual el primer inversor 510 y el segundo inversor 540 tienen un mayor umbral lógico.

Aquí, el inversor que tiene un mayor valor umbral lógico entre el primer inversor 510 y el segundo inversor 540 que se fabrican mediante un proceso de elaboración equivalente se pueden determinar aleatoriamente. También, una vez fabricado, el inversor que tiene el valor umbral lógico mayor entre el primer inversor 510 y el segundo inversor 540 puede no cambiar fácilmente. Sin embargo, cuando una diferencia entre los valores umbrales lógicos es diminuta, o se incrementa un cambio ambiental, por ejemplo, ruido, temperatura externa y similares, el inversor que tiene el valor umbral lógico mayor entre el primer inversor 510 y el segundo inversor 540 se puede cambiar. Aunque tal situación puede no ocurrir frecuentemente, se puede requerir garantizar la invariancia de tiempo para la ejecución de una cable de autenticación de seguridad, autenticación, y similares.

De acuerdo con esto, cuando se genera un valor digital mediante el circuito 500, el valor digital generado se puede congelar mediante la unidad 120 de congelamiento de valor digital de la Figura 1 o se puede almacenar en la unidad 420 de almacenamiento de valor digital de la Figura 4, con el fin de garantizar la invariancia de tiempo.

Como se sugiere frecuentemente, el circuito 500 se puede construir como una celda unitaria que puede generar un valor digital de 1- bit. Cuando se suministran N celdas unitarias, se puede suministrar un valor digital de N-bits. En lo sucesivo, a menos que se mencione otra cosa, tal escalabilidad se puede entender para ser implicada en una configuración del generador 110 o 410 de valor digital.

La diferencia entre los valores umbrales lógicos del primer inversor 510 y el segundo inversor 540 se describirá en detalle con referencia a la gráfica de la Figura 6.

La Figura 6 ilustra curvas características de voltaje en un caso en el cual el valor umbral lógico del primer inversor 510 es menor que el valor umbral lógico del segundo inversor 540, entre las realizaciones de ejemplo divulgadas de la Figura 5.

Una curva 610 indica una curva característica de voltaje del primer inversor 510, y una cuerva 620 indica una curva característica de voltaje del segundo inversor 540. En ciertas realizaciones, cuando el primer inversor 510 y el segundo inversor 540 se elaboran mediante un proceso de elaboración equivalente, la curva 610 y la curva 620 pueden ser casi idénticas la una a la otra. Sin embargo, una diferencia diminuta puede existir entre la curva 610 y la curva 620 debido a la variación del proceso, como se muestra en la Figura 6.

Cuando se encuentra un punto de intersección de la curva 610 y una línea 630 recta con una pendiente 1, se puede determinar un valor V_1 de umbral lógico del primer inversor 510. También, cuando se encuentra un punto de intersección de la curva 620 y la línea 630 recta, se puede determinar el valor V_2 umbral lógico del segundo inversor 540.

En este ejemplo, V_1 es menor que V_2. De acuerdo con esto, cuando el primer nodo 501 y el segundo nodo 502 se acortan, también denominado como un “restablecer”, al cerrar el interruptor 530 de la Figura 5, un voltaje $V_{Restablecer}$ del primer nodo 501y un voltaje $V_{Restablecer}$ del segundo nodo 502 pueden corresponder a un valor entre V_1 y V_2.

Cuando el primer nodo 501 y el segundo nodo 502 se abren al abrir el interruptor 530 de nuevo, el primer inversor 510 puede reconocer el voltaje del primer nodo 501 ($V_{Restablecer}$) como un nivel lógico HIGH, y pueden controlar el voltaje del segundo nodo 502 que corresponde a un terminal de salida del primer inversor 510 por ser un nivel lógico LOW.

En este caso, el segundo inversor 540 puede reconocer el voltaje ($V_{Restablecer}$) del segundo nodo 502 como un nivel lógico LOW, y puede controlar el voltaje del primer nodo 501 que corresponde al terminal de salida del segundo inversor 540 para ser un nivel lógico HIGH.

De acuerdo con esto, el nivel lógico del voltaje $V_{Restablecer}$ del segundo nodo 502 que corresponde a la salida OUT del circuito 500 de la Figura 5, puede ser HIGH.

Entre las varias realizaciones para describir un valor digital aleatorio generado con base en una diferencia en las características entre los dispositivos que utilizan la variación del proceso semiconductor, se ha descrito una realización que utiliza un inversor con referencia a las Figuras 4 y 5.

Sin embargo, una configuración del inversor no está limitada al circuito 500 de la Figura 5, y la presente divulgación incluye varias realizaciones que pueden generar un valor digital aleatorio que utiliza una diferencia en características entre dispositivos que utilizan la variación del proceso semiconductor, sin aparatarse de los principios dela invención.

El generador 110 o 410 de valor digital se puede configurar utilizando varios circuitos electrónicos, por ejemplo, un amplificador diferencial, un circuito de cerrojo, y similar, y además de un inversor. En lo sucesivo, se describirán ejemplos de tales realizaciones con referencia a las Figuras 7 a 9.

La Figura 7 es un diagrama que describe una configuración del generador 110 o 410 de valor digital de acuerdo con otra realización de ejemplo.

En referencia a la Figura 7, un circuito 700 de amplificador diferencial se utiliza para configurar el generador 110 o 410 de valor digital.

Cuando el primer terminal 711 de entrada y el segundo terminal 712 de entrada de un amplificador diferencial se acortan, diferentes valores digitales, por ejemplo, un valor de “1” y un valor de “0”, pueden salir del primer nodo 721 de salida y un segundo nodo 722 debido a la variación del proceso semiconductor.

El circuito 700 amplificador diferencial puede inicialmente amplificar una diferencia entre un voltaje del primer terminal 711 de entrada y un voltaje del segundo terminal 712 de entrada, y pueden suministrar una diferencia amplificada como una diferencia entre un valor de voltaje del primer nodo 721 de salida y un voltaje del segundo nodo 722 de salida.

De acuerdo con esto, cuando el primer nodo 711 de entrada y el segundo nodo 712 de entrada se acortan, la diferencia entre el voltaje del primer nodo 721 de salida y el segundo voltaje del segundo nodo 722 de salida, puede teóricamente ser cero.

Sin embargo, debido a la diferencia en las características eléctricas de los dispositivos incluidos en el circuito 700 amplificador diferencial, por ejemplo, los transistores, generados por la variación del proceso semiconductor, la diferencia entre el voltaje del primer nodo 721 de salida y el voltaje del segundo nodo 722 de salida puede no corresponder a cero cuando el primer nodo 711 de entrada y el segundo nodo de entrada 712 se acortan.

También, además de la diferencia en las características eléctricas de los dispositivos, esto es, los transistores, se puede incluir una diferencia en las características eléctricas de los dispositivos pasivos (no mostrados) por ejemplo, un resistor, un capacitor, un inductor, y similares, en el circuito 700 amplificador diferencial también puede originar una diferencia en el voltaje.

Esto es, el proceso de variación en un proceso de fabricación de chip puede producir una diferencia en las formas y estructuras de los dispositivos pasivos y, así, los dispositivos pasivos pueden tener diferentes valores característicos.

De acuerdo con esto, al comparar cual del primer nodo 721 de salida y el segundo nodo 722 de salida tiene mayor voltaje cuando el primer nodo 711 de entrada y el segundo nodo 712 de entrada se acortan, se puede generar una clave de identificación de 1 bit.

Por ejemplo, en un caso en el cual el voltaje del primer nodo 721 de salida es mayor que el voltaje del segundo nodo 722 de salida cuando el primer nodo 711 de entrada y el segundo nodo 712 de entrada se acortan, se puede determinar un valor digital generado para ser “1”. De otra manera, un valor digital generado se puede determinar como “0”.

También, cuando se suministran N celdas unitarias como se mencionó anteriormente, se puede generar un valor digital de N bit.

Las Figuras 8A y 8B son diagramas que describen una configuración del generador 110 o 410 de valor digital de acuerdo con otra realización de ejemplo.

En referencia a las Figuras 8A y 8B, el cerrojo de establecer – reestablecer (SR) se utiliza para configurar el generador 110 o 410 de valor digital. Las Figuras 8A y 8B ilustran dos (de muchos) ejemplos de configurar el cerrojo SR.

En la figura 8A, se utilizan las compuertas NOR. En la Figura 8B, se utilizan las compuertas NAND.

Con el fin de tener las mismas entradas y salidas lógicas en las configuraciones de compuertas NOR y NAND, dos entradas Sb y Rb en las compuertas NAND de la Figura 8B pueden corresponder a señales inversas de dos entradas S y R en las compuertas NOR de la Figura 8A.

Con el fin de configurar el generador 110 o 410 de valor digital utilizando el circuito ilustrado en las Figuras 8A y 8B, un valor de “1” puede primero ser la entrada a ambas de las dos entradas S y R.

De acuerdo con la tabla lógica teórica de un cerrojo SR, cuando el nivel lógico de “0” es entrada a ambas, las entradas S y R, la salida Q y la salida Qb que corresponden a un nivel inverso de la salida Q puede ser no definida. Cuando el nivel lógico de “1” es entrado a ambas, las entradas S y R, cada una de las salidas Q y la salida Qb pueden corresponder a un nivel lógico de “0”. Aquí, cuando la entrada del nivel lógico de ambas de las entradas S y R se cambia a un nivel lógico de “0”, la salida Q y la salida Qb se puede determinar para ser complementaria la una a la otra debido a una diferencia entre valores característicos de dispositivos que constituyen las dos compuertas

NOR. Esto es, la salida Q puede corresponder a “1” y la salida Qb puede corresponder a “0” o al contrario, el nodo Q de salida puede corresponder a “0” y el nodo Qb de salida puede corresponder a “1”.

Un resultado real de estos dos casos puede ser obtenido de manera aleatoria. Esto es porque aunque los dispositivos incluidos en las compuertas NOR de circuito de la Figura 8A y las compuertas NAND del circuito de la Figura 8B pueden tener diferentes características una de la otra, por ejemplo, voltaje umbral, movilidad, y similares, el resultado puede ser impredecible.

De acuerdo con esto, el generador 110 o 410 del valor digital configurado por el circuito de la Figura 8A u 8B puede generar un valor digital aleatorio.

La Figura 9 es un diagrama que describe una configuración de un generador de valor digital de acuerdo con otra realización de ejemplo.

Aunque un circuito de la Figura 9 es similar al circuito de la Figura 8A u 8B al utilizar el cerrojo CR, se agrega un interruptor 910 entre las salidas Q y Qb.

Un nivel lógico de “0” puede ser entrado a ambas entradas S y R, y el interruptor 910 puede ser cerrado. Un voltaje de la salida Q y un voltaje de la salida Qb pueden volverse idénticos el uno al otro, y el voltaje de la salida Q y el voltaje de la salida Qb pueden corresponder a un valor entre un voltaje que corresponde a un nivel lógico de “1” y un voltaje que corresponde a un nivel lógico de “0”.

Cuando el interruptor 910 se abre de nuevo, la salida Q puede corresponder a “1” y la salida Qb puede corresponder a “0”, o al contrario, la salida Q puede corresponder a “0” y la salida Qb puede corresponder a “1” dependiendo del valor umbral lógico de cada compuerta NOR. En este caso, un resultado real de estos dos casos puede ser obtenido de manera aleatoria.

Como se describió anteriormente en relación con la Figura 8, tal aleatoriedad se puede materializar ya que se puede determinar un resultado, que puede ser impredecible mediante los dispositivos incluidos en las compuertas NOR que tienen diferentes características una de la otra, por ejemplo, un voltaje umbral una movilidad, y similar.

De acuerdo con esto, el generador 110 o 410 de valor digital configurado por el circuito Figura 9 puede generar un valor digital aleatorio.

En lo sucesivo, ejemplos de circuitos de aparatos 100 para generar un valor digital en el cual la unidad 120 de congelamiento de valor digital se combina con el generador 110 de valor digital se puede describir con referencia a las Figuras 10 a 17D.

La Figura 10 es un diagrama que ilustra una configuración de un aparato para generar un valor digital en el cual una unidad 120 de congelamiento de valor digital de acuerdo con la realización de la Figura 2 se combina con un generador de valor digital que utiliza un cerrojo SR de acuerdo con una realización de la Figura 8A u 8B.

Una configuración de un generador 1010 de valor digital se puede entender por el circuito del cerrojo SR que se ha descrito con referencia a la Figura 8A y 8B.

Cuando los valores digitales diferentes, por ejemplo, un valor de “1” y un valor de “0” se generan a los dos terminales de salida, OUT y OUT_BAR, mediante el generador 1010 de valor digital, se puede aplicar una sobrecorriente a uno de los fusibles 1021 en una unidad 1020 de congelamiento de valor digital con base en los resultados correspondientes, y uno de los fusibles 1021 puede saltar.

De acuerdo con esto, cuando un fusible salta, un valor digital generado por el generador 1010 de valor digital se puede congelar mediante la unidad 1020 de congelamiento de valor digital.

Un proceso de salto de un fusible se describirá adicionalmente al referirse a la gráfica de la Figura 11.

La Figura 11 es una gráfica (gráfica de tiempo de señal) que describe un proceso de congelar un valor digital mediante la unidad 1020 de congelamiento de valor digital de acuerdo con la realización de la Figura 10.

Por ejemplo, durante una primera operación del generador 1010 de valor digital de la FIGURA 10, se puede aplicar una sobrecorriente a un fusible 2 con base en la diferencia en las salidas OUT y OUT_BAR y el fusible 2 se puede saltar, y así, congelar un valor digital.

Una disposición de los fusibles 1021 de la Figura 10 puede ser solo una de varias realizaciones de ejemplo, de acuerdo con esto, otras varias disposiciones de fusibles se describirán adicionalmente con referencia a las Figuras 12A a 12D, además de la realización de la Figura 10.

Las Figuras 12A a 12D son diagramas en los cuales una unidad de congelamiento de valor digital se dispone en un aparato para generar un valor digital de acuerdo a varias realizaciones de ejemplo.

La Figura 12A ilustra una configuración de un valor digital generado configurado utilizando un cerrojo SR, y las Figuras 12B a 12D ilustran varias posiciones 1210, 1220, y 1230 de fusibles que se pueden disponer a lo largo de los cerrojos SR.

Las operaciones detalladas pueden ser suficientemente entendidas a través de las descripciones suministradas con referencia a las Figuras 8A a 11 y, así, se pueden omitir las descripciones detalladas.

Como se describió con referencia a la Figura 3, un valor digital puede ser congelado mediante los dispositivos OTP, en lugar de los fusibles, y tal realización se describirá con referencia a las Figuras 13A a 13D.

Las Figuras 13A a 13D son diagramas que ilustran varias configuraciones de una unidad de congelamiento de valor digital se configura utilizando un dispositivo OTP de acuerdo con realizaciones de ejemplo.

De manera similar a las Figuras 12A a 12D, la Figura 13A ilustra una configuración de un generador de valor digital configurada utilizando un cerrojo SR, y las Figuras 13B y 13D ilustran varias posiciones 1310, 1320 y 1330 de los dispositivos OTP que se pueden disponer junto con los cerrojos SR.

Un proceso de congelar un valor digital utilizando los dispositivos OTP puede ser suficientemente entendido a través de la Figura 3 y similares y, así, se pueden omitir descripciones detalladas.

Ejemplos de varias disposiciones de un circuito en el cual se pueden combinar la unidad de congelamiento de valor digital con un generador de valor digital de acuerdo con las realizaciones que utilizan los inversores tal como se describió con referencia a las Figuras 5 y 6 así como también con un cerrojo SR se suministran en lo que sigue.

Las Figuras 14A a 14E son diagramas en los cuales se dispone de una unidad de congelamiento de valor digital en un aparato para generar un valor digital cuando un generador de valor digital se configura de acuerdo a la realización de la Figura 5, de acuerdo a las realizaciones de ejemplo.

La Figura 14A ilustra una configuración del generador de valor digital configurado utilizando los inversores descritos con referencia a la Figura 5 y las Figuras 14B a 14E ilustran varía posiciones 1410, 1420, 1430, y 1440 de los fusibles que se pueden disponer junto con los inversores.

En este caso, un valor digital puede ser congelado mediante los dispositivos OTP, en lugar de los fusibles, y tal realización se describirá con referencia a las Figuras 15A a 15E.

Las Figuras 15A a 15E son diagramas que ilustran varias configuraciones de una unidad de congelamiento de valor digital cuando un generador de valor digital se configura de acuerdo a la realización de la Figura 5 y la unidad de congelamiento de valor digital se configura utilizando un dispositivo OTP, de acuerdo a realizaciones de ejemplo.

De manera similar a las Figuras 14A a 14B la Figura 15 ilustra una configuración de un generador de valor digital configurado utilizando los inversores, y las Figuras 15B a15E ilustran varias posiciones 1510, 1520, 1530 y 1540 de los dispositivos OTP que se han dispuesto junto con los inversores.

Las Figuras 16A a 16D son diagramas en los cuales se dispone de una unidad de congelamiento de valor digital en un aparato para generar un valor digital cuando un generador de valor digital se configura de acuerdo a la realización de la Figura 7, de acuerdo con las realizaciones de ejemplo.

La Figura 16A ilustra una configuración de un generador de valor digital configurado utilizando el amplificador diferencial descrito con referencia a la Figura 7, y las Figuras 16B a 16D ilustran varias posiciones 1610, 1620, 1630 de los fusibles que se pueden disponer en el aparato para generar un valor digital, junto con el amplificador diferencial.

En este caso, un valor digital se puede congelar mediante los dispositivos OTP, en lugar de los fusibles, y tal realización se describirá con referencia a las Figuras 17A a 17D.

Las Figuras 17A a 17D son diagramas que ilustran varias configuraciones de la unidad de congelamiento de valor digital cuando se configura un generador de valor digital de acuerdo a la realización de la Figura 7 y la unidad de congelamiento de valor digital se configura utilizando un dispositivo OTP, de acuerdo a otra realización.

De manera similar a las Figuras 16A a 16D, la Figura 17A ilustra una configuración de un generador de valor digital configurado utilizando un amplificador diferencial, y las Figuras 17B a 17D ilustran varias posiciones 1710, 1720, y 1730 de los dispositivos OTP que se pueden disponer junto con el amplificador diferencial.

La Figura 18 es un diagrama de flujo que ilustra un método para generar un valor digital de acuerdo con una realización de ejemplo.

En operación 1810, una señal de entrada se puede aplicar al generador 110 de valor digital del aparato 100 de la Figura 1 para generar un valor digital. La aplicación de la señal de entrada puede incluir una aplicación de voltaje, una operación corriente, una primera operación, y similares.

En la operación 1820, el generador 110 de valor digital puede generar un valor digital que utiliza una diferencia entre los valores característicos de los dispositivos semiconductores, que resultan de una variación del proceso semiconductor. Un proceso de operación 1820 mediante el cual el generador 110 de valor digital puede generar un valor digital aleatorio se ha descrito anteriormente con referencia a las Figuras 1 a 3, y 5 a 9.

En la operación 1830, la unidad 120 de congelamiento de valor digital puede congelar un valor digital aleatorio generado en la operación 1820 con el fin de garantizar la invariancia de tiempo.

El proceso de congelar el valor digital se ha descrito anteriormente con referencia a las Figuras 2 y 3, y 10 a 17.

La Figura 19 es un diagrama de flujo que ilustra un método para generar un valor digital de acuerdo con otra realización de ejemplo.

Un proceso para aplicar una señal de entrada en la operación 1910, y un proceso para generar un valor digital aleatorio mediante el generador 410 de valor digital en la operación 1920 son similares a las operaciones 1810 y 1820 de la Figura 18.

Sin embargo, el método de la Figura 19 difiere del método de la Figura 18 en que el valor digital aleatorio generado se puede almacenar en la unidad 420 de almacenamiento de valor digital de la Figura 4. La unidad 420 de almacenamiento de valor digital se ha descrito anteriormente con referencia a la Figura 4.

De acuerdo con varias realizaciones de ejemplo, se puede generar un valor digital aleatorio que utiliza variación del proceso semiconductor, y el valor digital se puede congelar o almacenar de tal manera que el valor digital puede no cambiar al envejecer un dispositivo durante el tiempo, un cambio en un ambiente periférico, por ejemplo, temperatura o ruido de tal manera que se puede garantizar la invariancia de tiempo.

De acuerdo con esto, se puede suministrar un valor digital aleatorio confiable que se puede utilizar como una clave de identificación y similar en varios campos de aplicación, que incluyen seguridad y autenticación.

Las realizaciones de ejemplo anteriormente descritas de la presente divulgación se pueden registrar en medios legibles por ordenador que incluyen instrucciones de programa para ejecutar varias operaciones realizadas por un ordenador. El medio también puede incluir, solo o en combinación con las instrucciones de programa, archivos de datos, estructuras de datos, y similares. Ejemplos de medios legibles por ordenador incluyen medios magnéticos tal como discos duros, floppy disc, y cinta magnética, medio óptico tal como discos de CD ROM y DVD; medios magnetoópticos tales como discos flopticos tal como dispositivos de hardware que son especialmente configurados para almacenar y efectuar instrucciones de programa, tales como la memoria de solo lectura (ROM), memoria de acceso aleatorio (RAM), memoria flash, y similares. Ejemplos de instrucciones de programa incluyen tanto código de máquina, tal como el producido por un compilador, y archivos que contienen código de nivel superior que se pueden ejecutar por un ordenador utilizando un interpretador. En los dispositivos de hardware descrito se pueden configurar para actuar como uno o más módulos de software con el fin de efectuar las operaciones de las realizaciones de ejemplo anteriormente descritas de la presente divulgación, o viceversa.

Aunque se han mostrado y descrito pocas realizaciones de ejemplo, la presente divulgación no se limita a las realizaciones de ejemplo descritas. En su lugar, se apreciará por aquellos expertos en la técnica que se pueden hacer cambios a estas realizaciones de ejemplo sin apartasen de los principios de la invención, cuyo alcance se define mediante las reivindicaciones y sus equivalentes.

REIVINDICACIONES

1. Un aparato para generar un valor digital, el aparato comprende:

un generador, donde el generador:

generar un valor digital con base en una variación de proceso en el proceso de fabricación de semiconductores;

caracterizado por que además comprende:

una unidad de congelamiento conectada al generador, en donde la unidad de congelamiento:

se fija a uno de un primer estado irreversible y un segundo estado irreversible con base en el valor digital generado; y

comprende una unidad de control configurada para congelar el valor digital.

2. El aparato de la reivindicación 1, en donde la unidad de congelamiento comprende un fusible y la unidad de control se configura para hacer saltar o no saltar el fusible para congelar el valor digital, en donde:

el fusible salta mediante una de una sobrecorriente o un sobrevoltaje;

si el fusible salta o no salta es invariante durante el tiempo; y

el primer estado corresponde al fusible que salta, el segundo estado corresponde al fusible que no salta, en donde:

el primer estado corresponde a un valor digital de 1, y el segundo estado corresponde a un valor digital de 0; o

el primer estado corresponde a un valor digital de 0, y el segundo estado corresponde a un valor digital de 1.

3. El aparato de la reivindicación 1 o 2, en donde la unidad de congelamiento comprende un dispositivo programable por una vez (OTP) y la unidad de control se configura para programar el dispositivo OTP para congelar el valor digital, y en donde:

El valor digital programado en el dispositivo OTP es invariante durante el tiempo.

4. El aparato de la reivindicación 3, en donde:

La unidad de control se configura para programar el dispositivo OTP para congelar el valor digital con base en la señal de control de la unidad de control.

5. El aparato de la reivindicación 1, en donde el generador comprende una función físicamente no clonable (PUF).

6. El aparato de una cualquiera de las reivindicaciones 1-5, en donde el generador comprende:

un primer inversor y un segundo inversor;

el primer inversor y el segundo inversor fabricado con base en un proceso equivalente y que tiene valores característicos eléctricos diferentes con base en la variación del proceso en el proceso de fabricación de semiconductores.

7. El aparato de la reivindicación 6, el generador comprende además:

un terminal de entrada del primer inversor;

un terminal de salida del primer inversor;

un terminal de entrada del segundo inversor;

un terminal de salida del segundo inversor;

un primer nodo; y

un segundo nodo,

en donde:

el terminal de salida del primer inversor y el terminal de entrada del segundo inversor se conectan al primer nodo, y el terminal de entrada del primer inversor y el terminal de salida del segundo inversor se conectan al segundo nodo, y

cuando el primer nodo y el segundo nodo se acortan y luego se abren, el generador genera el valor digital con base en un nivel lógico de al menos uno del primer nodo y el segundo nodo.

8. El aparato de una cualquiera de las reivindicaciones 1-7, en donde el generador comprende un amplificador diferencial, y en donde el generador:

Genera el valor digital con base en una comparación de valores de voltaje de dos nodos de salida del amplificador diferencial cuando dos nodos de entrada del amplificador diferencial se acortan.

9. El aparato de cualquiera de las reivindicaciones 1-8, en donde el generador comprende un cerrojo de establecer-reestablecer (SR), y en donde el generador genera el valor digital con base en el nivel lógico de al menos uno de dos nodos de salida del cerrojo SR, en donde el nivel lógico se determina con base en una diferencia en los valores umbrales lógicos de las compuertas lógicas utilizadas para configurar el cerrojo SR cuando:

Un nivel lógico de “1” es entrado a dos nodos de entrada del cerrojo SR, y luego el nivel lógico de “0” es entrado a los dos nodos de entrada del cerrojo SR;

un nivel lógico de “0” es entrado a los dos nodos de entrada del cerrojo SR, y luego el nivel lógico de “1” es entrado a los dos nodos de entrada del cerrojo SR;

dos nodos de salida del cerrojo SR se acortan, y luego se abren mientras un nivel lógico de “0” se entra a dos nodos de entrada del cerrojo SR; o

dos nodos de salida del cerrojo SR se acortan, y luego se abren mientras que el nivel lógico de “1” es entrado a dos nodos de entrada en el cerrojo SR.

10. Un chip semiconductor que comprende el aparato de una cualquiera de las reivindicaciones 1-9.

11. Un método para generar un valor digital, el método comprende:

generar, en un aparato, un valor digital con base en la variación del proceso en un proceso de fabricación semiconductor.

caracterizado por las etapas adicionales de:

proporcionar el valor digital a una unidad de congelamiento que comprende una unidad de control para congelar el valor digital, estando la unidad de congelamiento fijada a uno de un primer estado irreversible y a un segundo estado irreversible con base en el valor digital generado; y

congela el valor digital

12. El método de la reivindicación 11, en donde congelar el valor digital comprende además la unidad de control que hace saltar un fusible para congelar el valor digital, en donde:

el fusible salta por uno de una sobrecorriente o un sobrevoltaje;

si el fusible salta o no salta es invariante durante el tiempo; y

un primer estado corresponde al fusible que salta, y un segundo estado corresponde al fusible que no salta, en donde:

el primer estado corresponde a un valor digital de 1, y el segundo estado corresponde a un valor digital de 0; o

el primer estado corresponde a un valor digital de 0, y el segundo estado corresponde a un valor digital de 1.

13. El método de la reivindicación 11, en donde congelar el valor digital comprende:

La unidad de control que programa un dispositivo programable por una vez (OTP) para congelar el valor digital, en donde el valor digital programado en el dispositivo OTP es invariante durante el tiempo.

14. El método de la reivindicación 13, en donde la unidad de control programa el dispositivo OTP para congelar el valor digital que utiliza una señal de control.

15. El método de una cualquiera de las reivindicaciones 11-14, en donde generar el valor digital comprende además:

acortar un primer nodo de un circuito eléctrico y un segundo nodo del circuito eléctrico;

abrir el primer nodo del circuito eléctrico y el segundo nodo del circuito eléctrico; y

generar un valor digital con base en el nivel lógico de al menos uno del primer nodo y el segundo nodo.

16. El método de la reivindicación 15, en donde:

El primer nodo está conectado a un terminal de salida de un primer inversor y un terminal de entrada de un segundo inversor; y

El segundo nodo está conectado a un terminal de entrada del primer inversor y un terminal de salida del segundo inversor, en donde:

El primer inversor y el segundo inversor se elaboran con base en un proceso equivalente y tienen valores característicos eléctricos diferentes con base en la variación del proceso en el proceso de elaboración semiconductor.

17. El método de una cualquiera de las reivindicaciones 11-16 en donde generar el valor digital comprende además:

acortar dos nodos de entrada de un amplificador diferencial; y

generar un valor digital con base en una comparación de los valores de voltaje de dos nodos de salida del amplificador diferencial.

18. El método de la reivindicación 11, en donde generar el valor digital comprende además:

Determinar un nivel lógico de al menos uno de dos nodos de salida de un cerrojo SR, con base en una diferencia en los valores umbrales lógicos de la compuerta lógica utilizada para configurar el cerrojo SR cuando:

Un nivel lógico de “1” es entrado a dos nodos de entrada del cerrojo SR y un nivel lógico de “0” es entrado a los dos nodos de entrada del cerrojo SR;

Un nivel lógico de “0” es entrado a dos nodos de entrada del cerrojo SR y un nivel lógico de “1” es entrado a los dos nodos de entrada del cerrojo SR;

Dos nodos de salida del cerrojo SR se acortan y los dos nodos de salida del cerrojo SR se abren mientras un nivel lógico de “0” es entrado a dos nodos de entrada del cerrojo SR; o

dos nodos de salida del cerrojo SR son acortados y los dos nodos de salida del cerrojo SR son abiertos mientras un nivel lógico de “1” es entrado a los dos nodos de entrada del cerrojo SR; y

generar un valor digital con base en el nivel lógico determinado.

19. Un dispositivo programado con un valor digital generado por el método de una cualquiera de las reivindicaciones 11-18.

20. El dispositivo de la reivindicación 19 que comprende al menos 1 de un dispositivo programable por una vez (OTP) y un dispositivo programable multitiempo o programable muchas veces (MTP).

FIG. 1

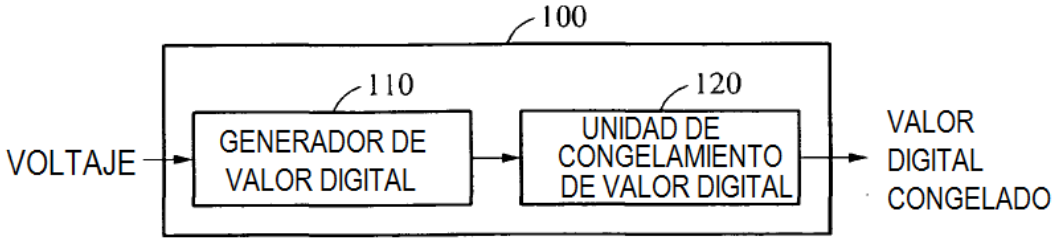

100
110
120
VOLTAJE
GENERADOR DE VALOR DIGITAL
UNIDAD DE CONGELAMIENTO DE VALOR DIGITAL
VALOR DIGITAL CONGELADO

FIG. 2

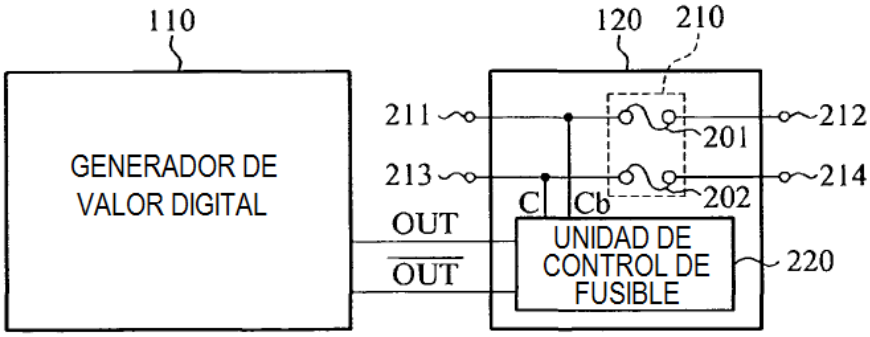

110
120
210
GENERADOR DE VALOR DIGITAL
211
213
201
202
212
214
C
Cb
OUT
OUT
UNIDAD DE CONTROL DE FUSIBLE
220

FIG. 3

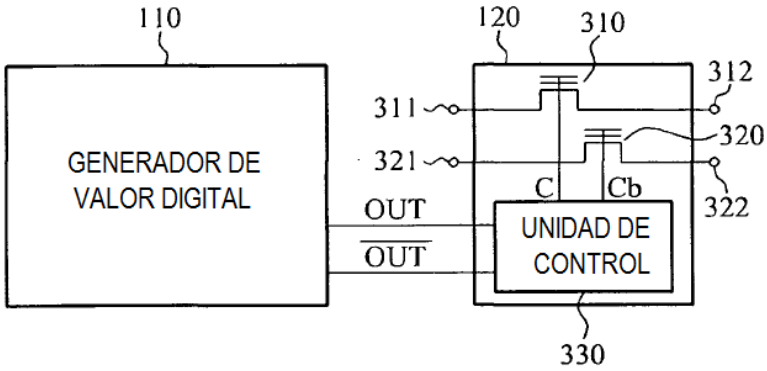

110
120
310
312
311
320
321
C
Cb
322
GENERADOR DE VALOR DIGITAL
OUT
$\overline{OUT}$
UNIDAD DE CONTROL
330

FIG. 4

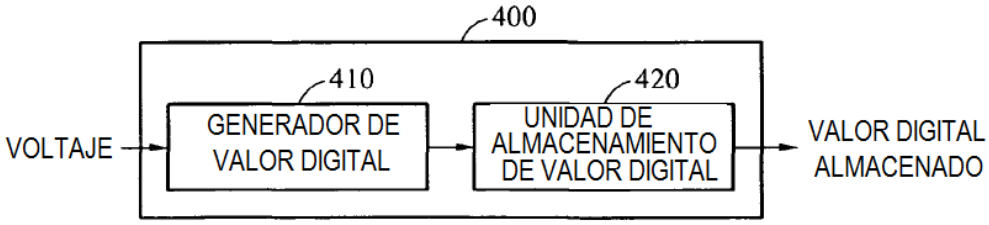

400
410
420
VOLTAJE
GENERADOR DE VALOR DIGITAL
UNIDAD DE ALMACENAMIENTO DE VALOR DIGITAL
VALOR DIGITAL ALMACENADO

FIG. 5

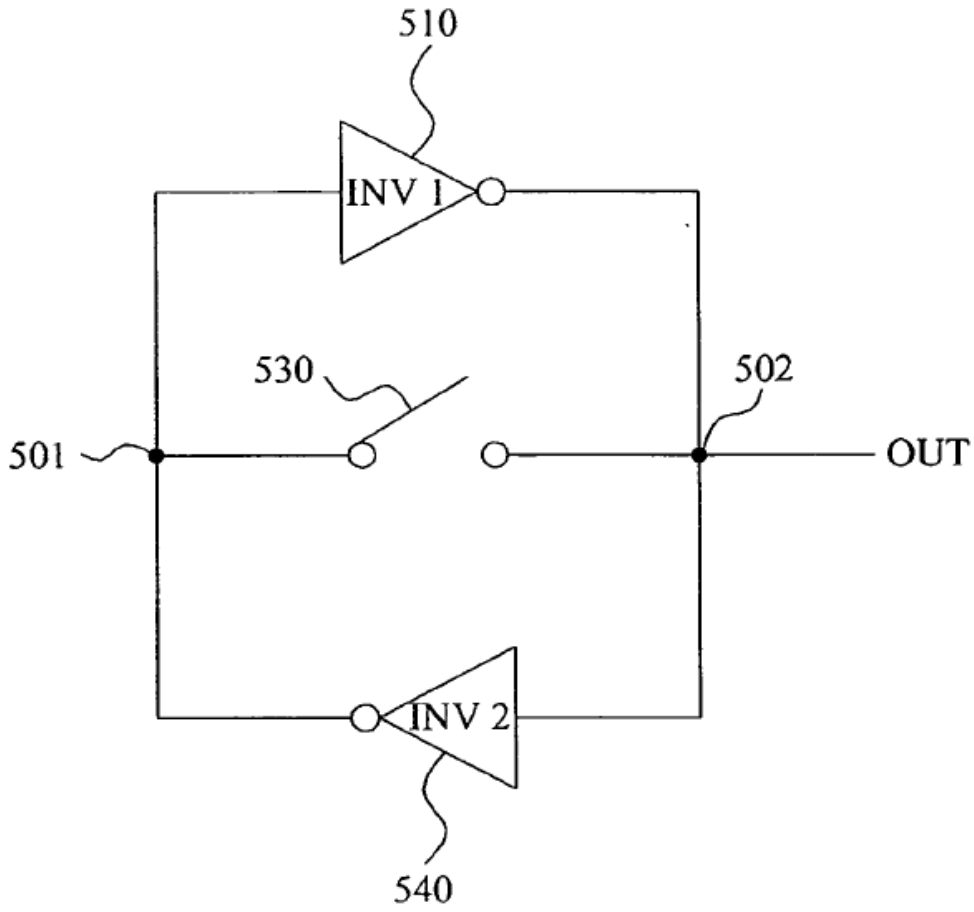


FIG. 6

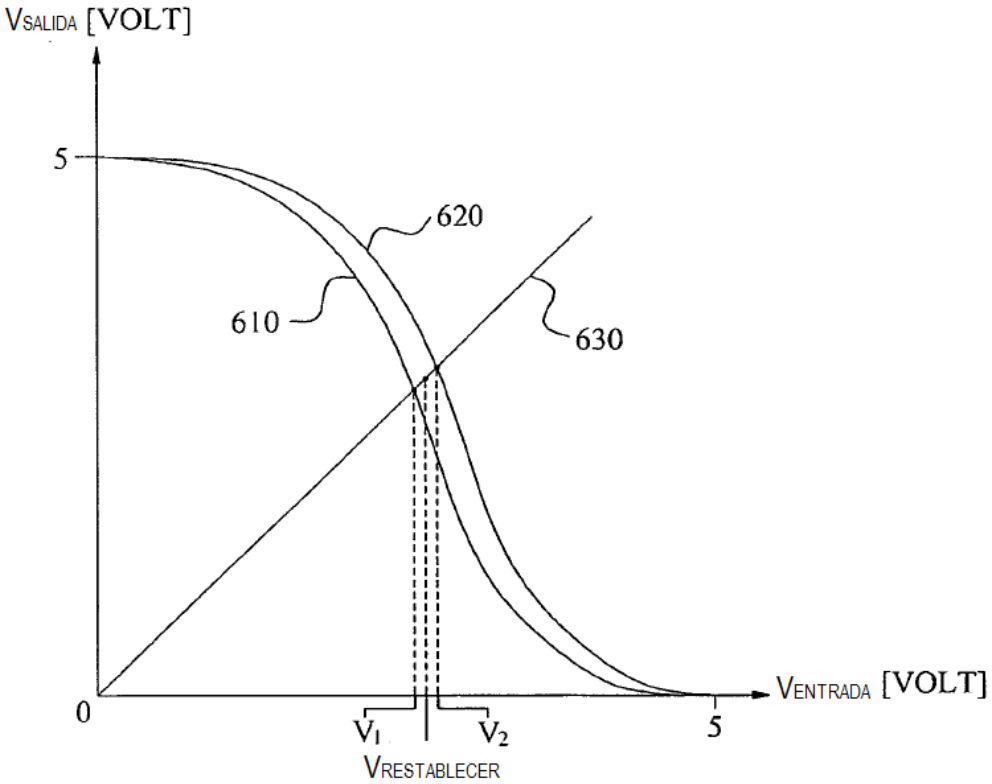

VSALIDA [VOLT]
5
620
610
630
0
V1
V2
5
VENTRADA [VOLT]
VRESTABLECER

FIG. 7

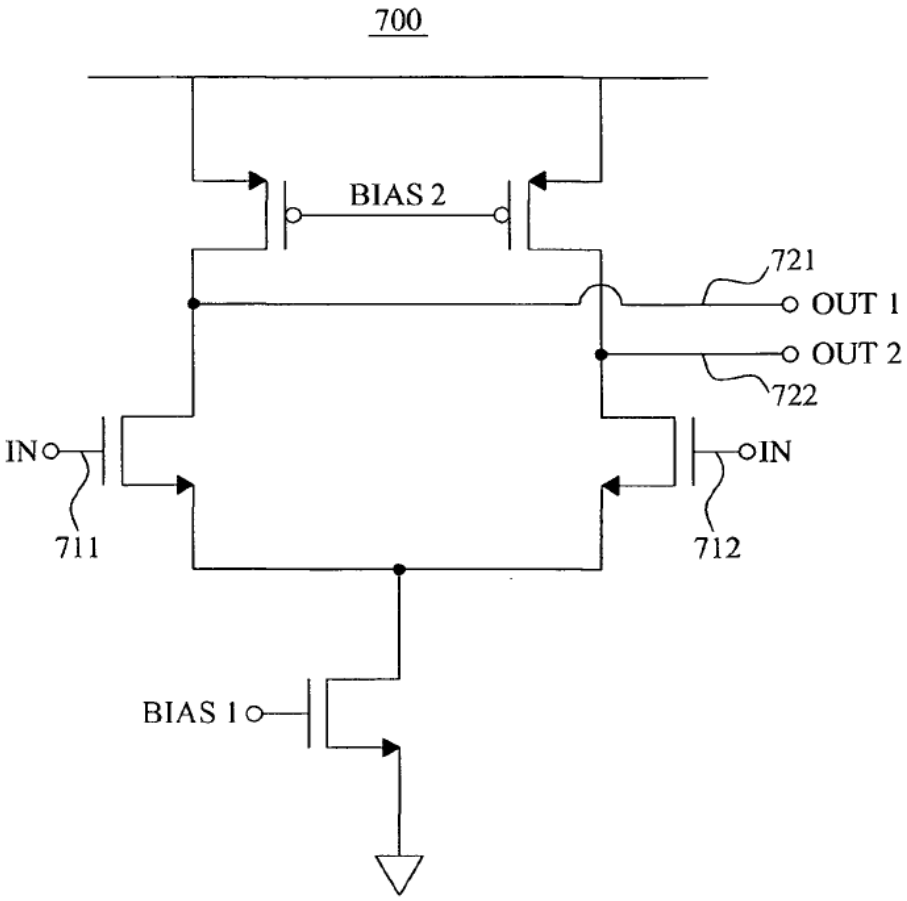


FIG. 8A

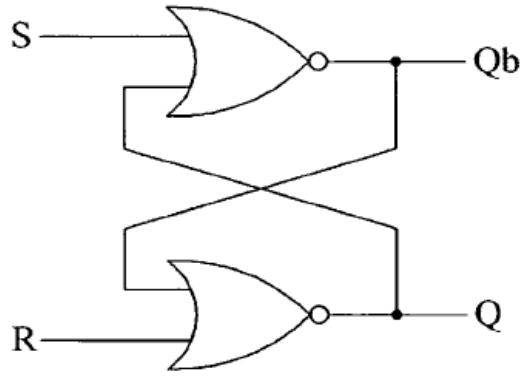


FIG. 8B

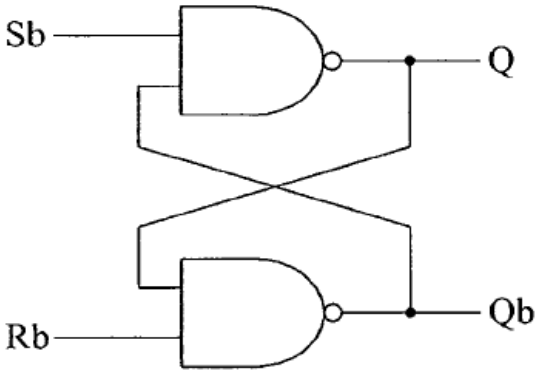


FIG. 9

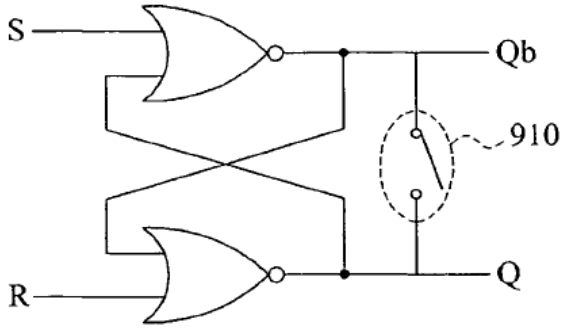

S
R
Qb
Q
910

FIG. 10

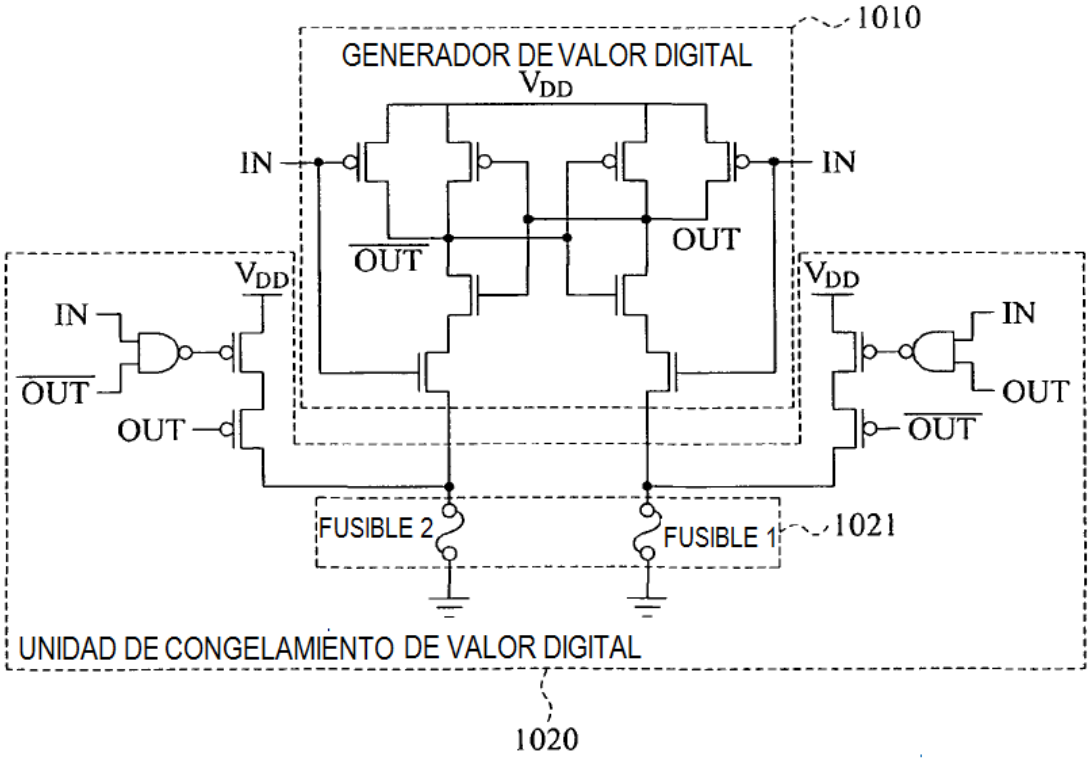
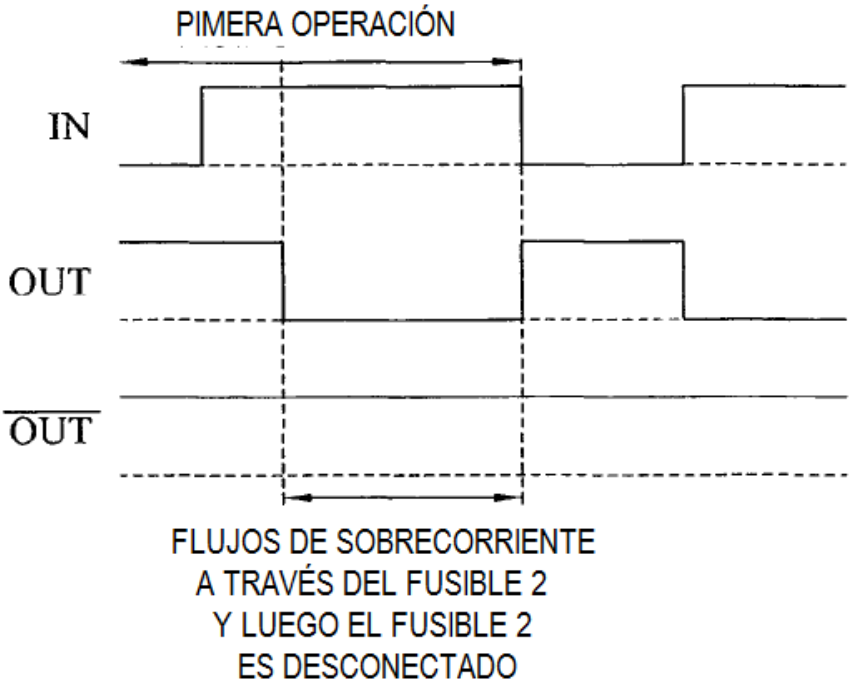

1010
GENERADOR DE VALOR DIGITAL
VDD
IN
IN
OUT
OUT
VDD
VDD
IN
OUT
IN
OUT
OUT
FUSIBLE 2
FUSIBLE 1
1021
UNIDAD DE CONGELAMIENTO DE VALOR DIGITAL
1020

FIG. 11


PIMERA OPERACIÓN
IN
OUT
$\overline{OUT}$
FLUJOS DE SOBRECORRIENTE
A TRAVÉS DEL FUSIBLE 2
Y LUEGO EL FUSIBLE 2
ES DESCONECTADO

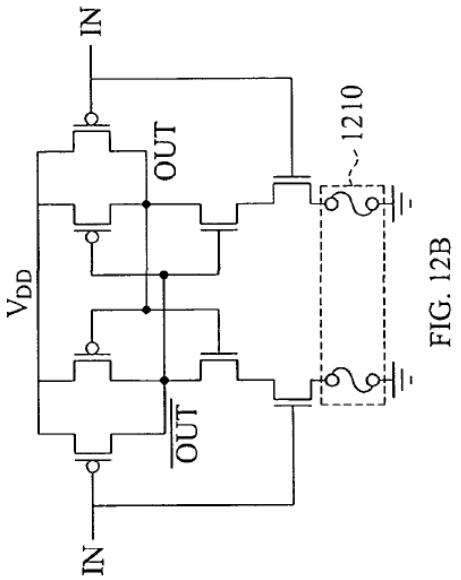


FIG. 12B

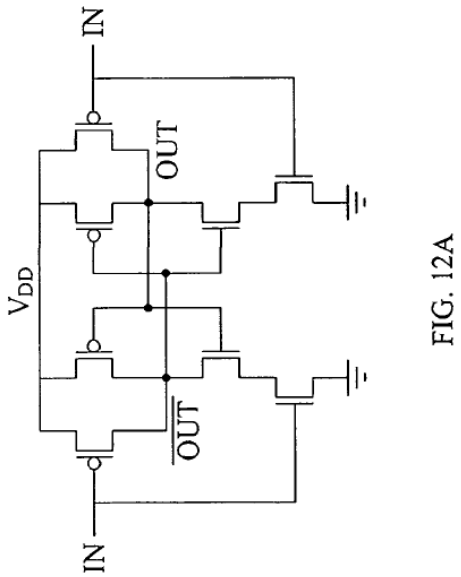


FIG. 12A

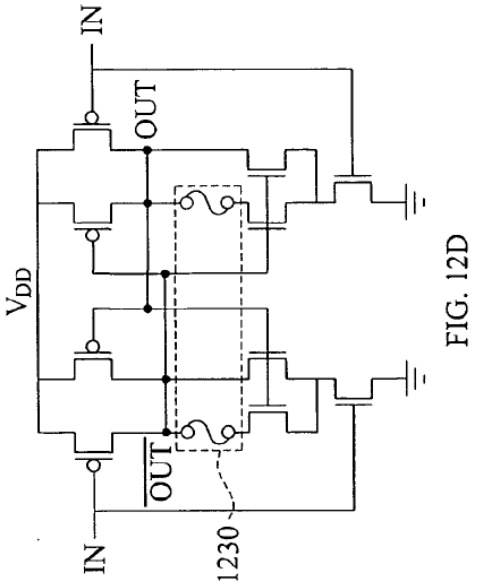


FIG. 12D

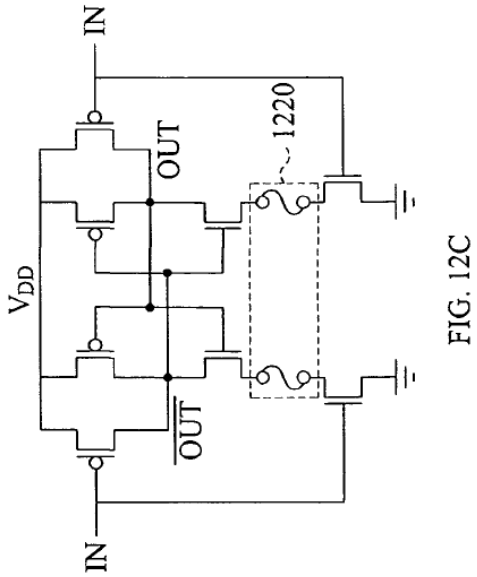


FIG. 12C

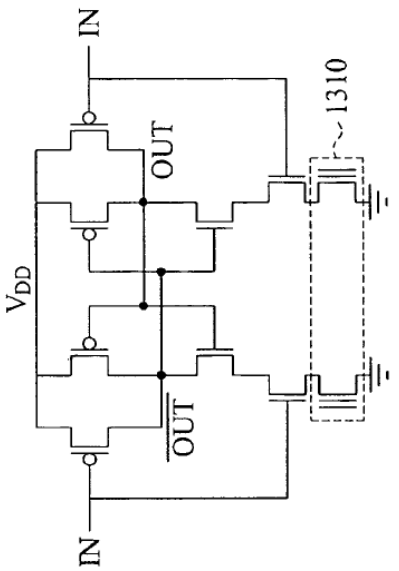


FIG. 13B

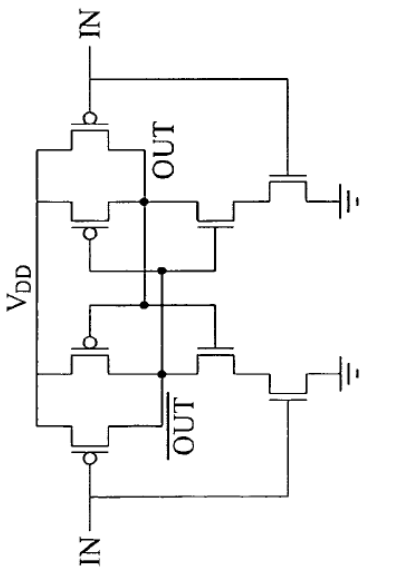


FIG. 13A

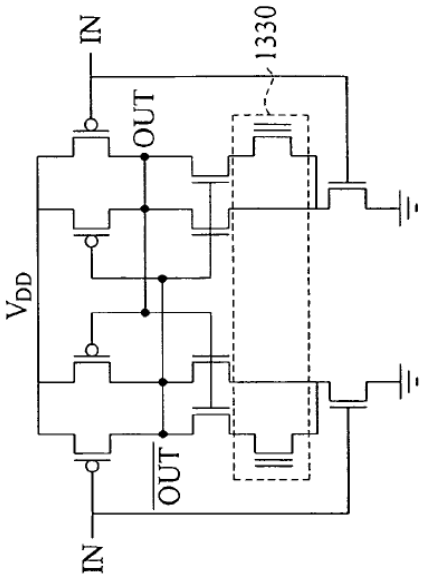


FIG. 13D

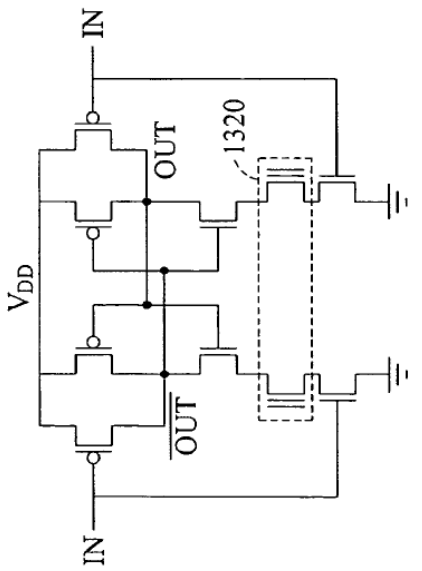


FIG. 13C

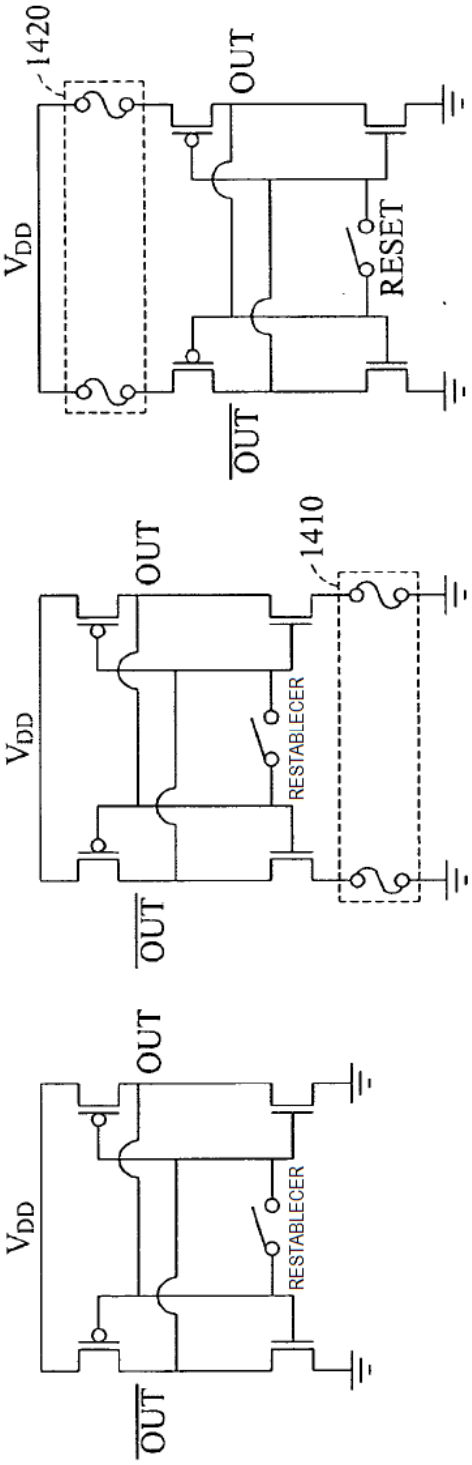


FIG. 14C

FIG. 14B

FIG. 14A

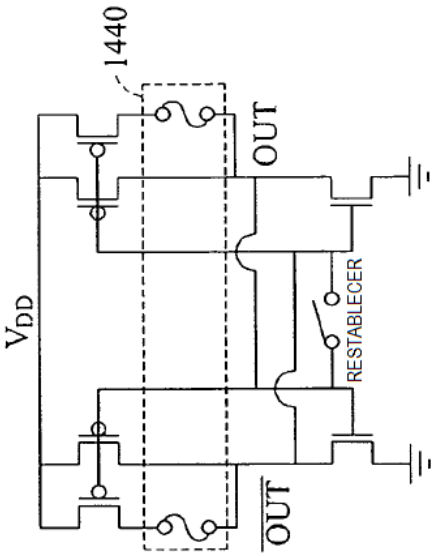


FIG. 14E

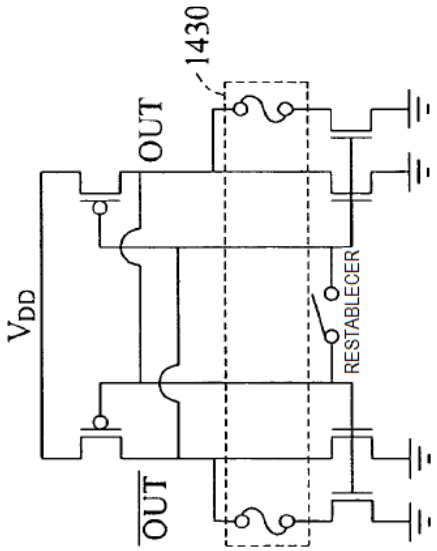


FIG. 14D

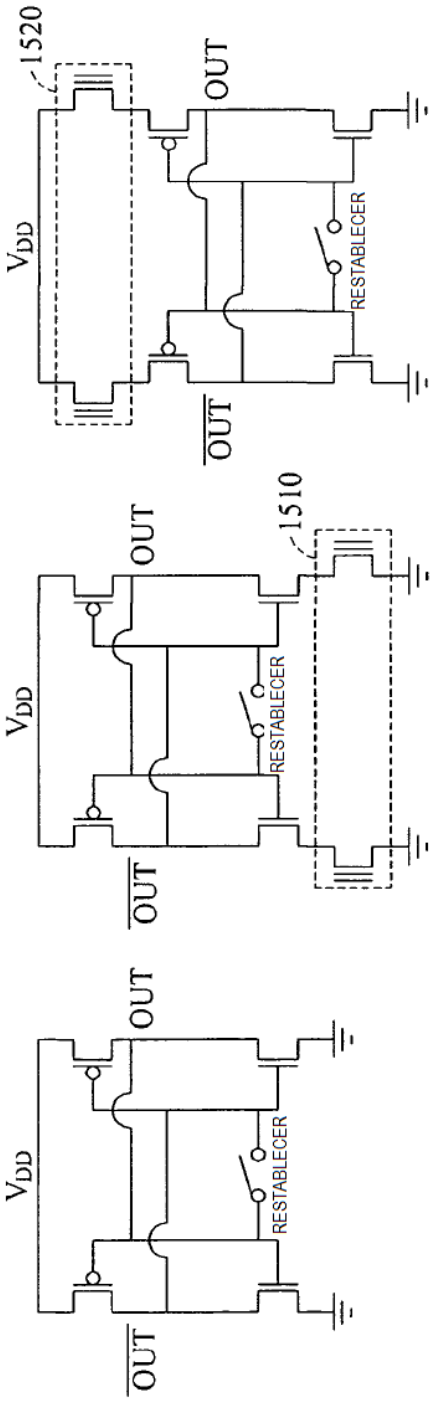


FIG. 15A

FIG. 15B

FIG. 15C

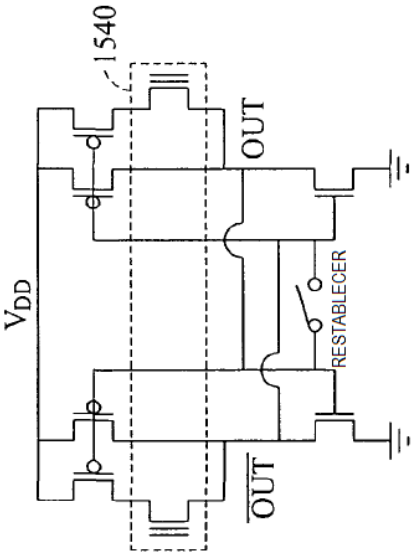


FIG. 15E

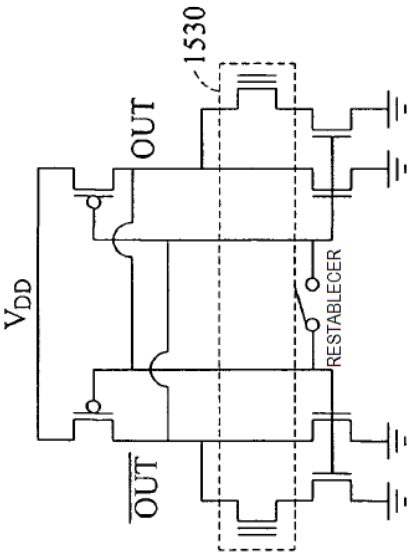


FIG. 15D

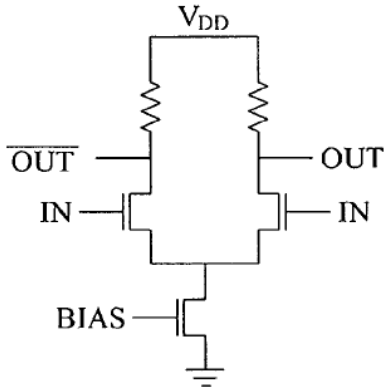


FIG. 16A

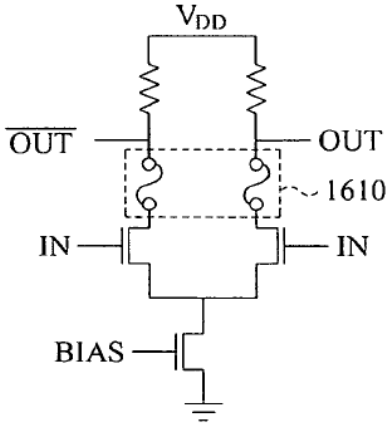


FIG. 16B

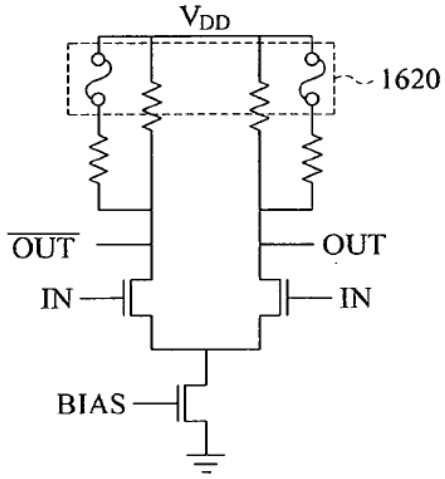


FIG. 16C

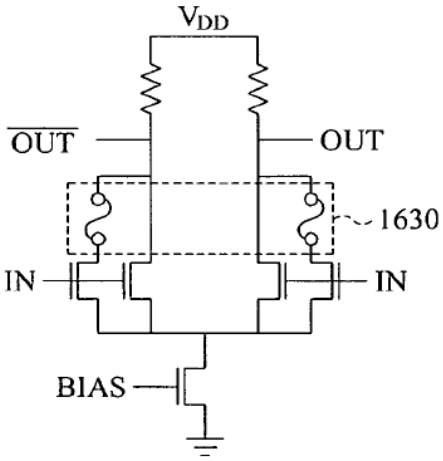


FIG. 16D

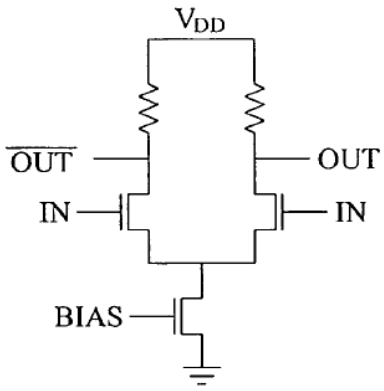


FIG. 17A

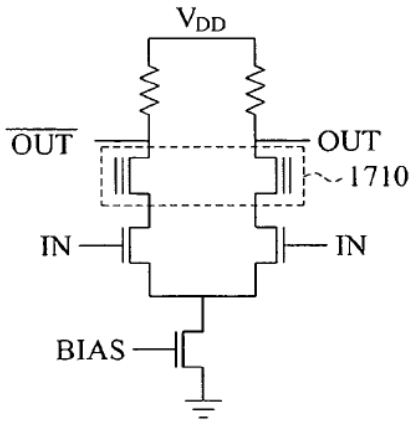


FIG. 17B

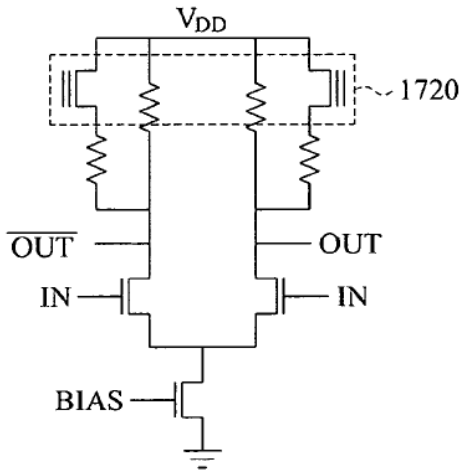


FIG. 17C

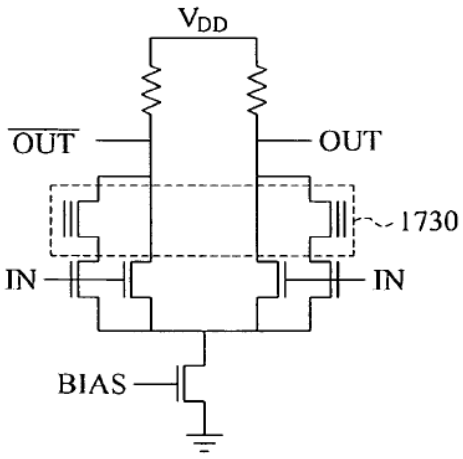


FIG. 17D

FIG. 18

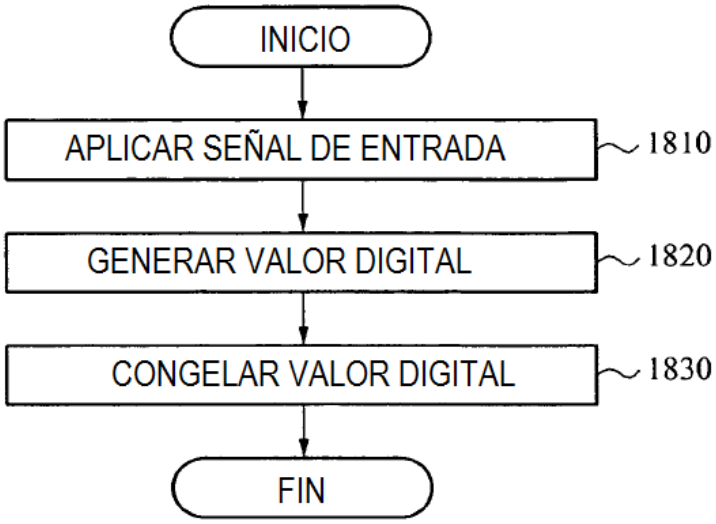
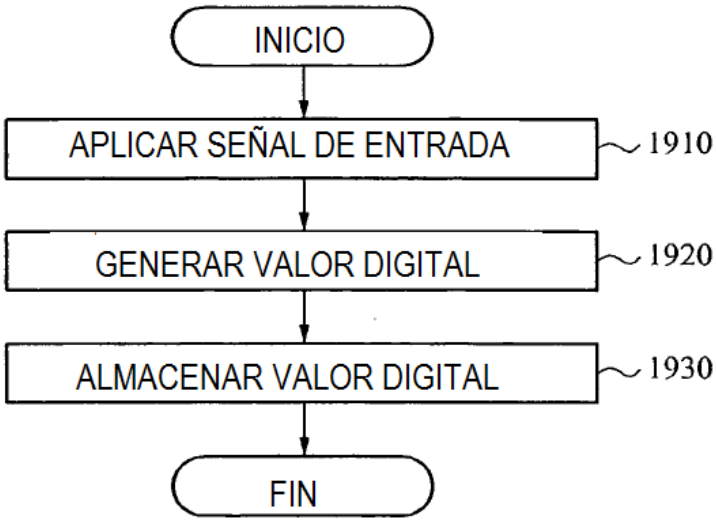

INICIO
APLICAR SEÑAL DE ENTRADA
1810
GENERAR VALOR DIGITAL
1820
CONGELAR VALOR DIGITAL
1830
FIN

FIG. 19


INICIO
APLICAR SEÑAL DE ENTRADA
1910
GENERAR VALOR DIGITAL
1920
ALMACENAR VALOR DIGITAL
1930
FIN