(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 707 862**

(51) Int. CI.:

H04L 9/14 (2006.01)
G06F 7/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.01.2011 PCT/KR2011/000605**

(87) Fecha y número de publicación internacional: **14.06.2012 WO12077856**

(96) Fecha de presentación y número de la solicitud europea: **28.01.2011 E 11847167 (1)**

(97) Fecha y número de publicación de la concesión europea: **21.11.2018 EP 2650813**

(54) Título: **Dispositivo y método para generar una clave de identificación**

(30) Prioridad:

09.12.2010 KR 20100125633

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.04.2019

(73) Titular/es:

ICTK HOLDINGS CO., LTD. (100.0%)
5F, 323, Pangyo-ro Bundang-gu, Seongnam-si Gyeonggi-do 13488, KR

(72) Inventor/es:

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

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Dispositivo y método para generar una clave de identificación.

Antecedentes

1. Campo de la invención

Las realizaciones de ejemplo se refieren a un campo de seguridad digital, y más particularmente, a un aparato y a un método para generar una clave de identificación utilizada para un método de codificación y decodificación, una firma digital, y similares que pueden ser necesarios para la seguridad de un aparato electrónico, seguridad del sistema integrado, seguridad del sistema en chip (SoC), seguridad de la tarjeta inteligente, seguridad del módulo de identidad del suscriptor universal (USIM) y similares.

2. Descripción de la técnica relacionada

A medida que una sociedad orientada a la información ha avanzado, la necesidad de proteger la privacidad individual ha aumentado. Por lo tanto, una tecnología para construir un sistema de seguridad que pueda transmitir información de manera segura mediante el cifrado y descifrado de la información es una tecnología esencialmente necesaria y destacada.

En la sociedad orientada a la información avanzada, junto con un ordenador de alto rendimiento, el uso de un dispositivo informático en forma de un sistema integrado o un sistema en chip (SoC) ha aumentado rápidamente. Por ejemplo, los dispositivos informáticos, como la identificación por radiofrecuencia (RFID), una tarjeta inteligente, un módulo de identidad de suscriptor universal (USIM), una contraseña de un solo uso (OTP) y similares, se han utilizado ampliamente.

Para construir un sistema de seguridad en el dispositivo informático, se puede usar una clave criptográfica que se usa para algoritmos de cifrado y descifrado, o una identificación única. La clave criptográfica o la identificación única serán referidas de aquí en adelante como una clave de identificación. La clave de identificación depende principalmente de un método para generar externamente un número pseudoaleatorio (PRN) que puede ser criptográficamente seguro, y almacenar el PRN en una memoria no volátil como una memoria flash, una memoria de solo lectura programable y borrable eléctricamente (EEPROM), y similares.

Con respecto a una clave de identificación almacenada en un dispositivo informático, recientemente se han llevado a cabo diversos ataques, como un ataque de canal lateral, un ataque de ingeniería inversa y similares. En respuesta a estos ataques, la tecnología de Función Física Inclonable (PUF) se está desarrollando como un método para generar y almacenar de manera segura una clave de identificación.

La PUF es una tecnología para generar una clave de identificación utilizando las sutiles diferencias de características físicas que existen en un sistema electrónico, y mantener o almacenar la clave de identificación como se genera, lo que también se conoce como una huella digital de hardware.

Para utilizar la PUF como clave de identificación, primero debe ser suficiente la aleatoriedad de una clave de identificación generada y, en segundo lugar, el valor de la clave de identificación generada debe ser invariante con respecto al flujo de tiempo o los cambios en el entorno de uso.

El documento US 2006/0131575 A1 divulga un dispositivo electrónico que incluye un grupo de elementos que genera un número de identificación específico y que está compuesto por una pluralidad de elementos, en donde el número de identificación específico se establece en función de una desviación irregular en la característica eléctrica de los elementos que se produce debido a un fallo aleatorio en un proceso de fabricación.

Sin embargo, existen problemas con las tecnologías convencionales, como la dificultad suficiente para obtener aleatoriedad, y una clave de identificación generada que se modifica debido a cambios en las características físicas de acuerdo con el flujo de tiempo o debido a cambios en el entorno de uso, que aún no se han resuelto.

Sumario

De acuerdo con los aspectos de la invención, se proporcionan un aparato y un método para generar una clave de identificación como se establece en las reivindicaciones 1 y 7, respectivamente, y un chip semiconductor identificable por la clave de identificación como se establece en la reivindicación 13.

En un aspecto general, se proporciona un aparato y un método para generar una clave de identificación con el fin de generar un valor de número aleatorio a través de un proceso de fabricación de semiconductores, y luego desarrollar una tecnología de Función Física Inclonable (PUF) que proporciona el valor que, una vez generado, puede ser invariante en el tiempo y usar la tecnología PUF como clave de identificación.

Un aspecto de la presente invención también proporciona un aparato y un método para generar una clave de identificación que puede garantizar probabilísticamente un equilibrio entre un valor digital de 0 y un valor digital de 1 en una clave de identificación en forma de un valor digital.

Un aspecto de la presente invención también proporciona un aparato y un método para generar una clave de identificación para configurar una PUF que puede fabricarse a un coste relativamente bajo y de una manera simple, puede ser físicamente inclonable y, por consiguiente, puede ser inmune a un ataque externo.

De acuerdo con un aspecto, se proporciona un aparato para generar una clave de identificación mediante una determinación probabilística de si ocurre un cortocircuito entre los nodos que constituyen un circuito al violar una regla de diseño provista durante un proceso de fabricación de semiconductores.

De acuerdo con un aspecto, se proporciona un aparato para generar una clave de identificación que incluye un generador de claves de identificación para generar una clave de identificación basada en si un contacto o una vía, utilizada para conectar eléctricamente capas conductoras en un chip semiconductor, genera cortocircuito en las capas conductoras, y un lector de clave de identificación para leer la clave de identificación leyendo si el contacto o la vía generan cortocircuito en las capas conductoras.

El generador de claves de identificación puede incluir un circuito que incluye un contacto o una vía que puede diseñarse para que sea igual o más pequeño que un tamaño determinado por la regla de diseño proporcionada durante el proceso de fabricación de semiconductores. El contacto o la vía que está diseñado para ser diminuto puede determinar de forma probabilística un cortocircuito entre las capas conductoras.

Después de determinar si el contacto o la vía hace cortocircuito las capas conductoras se establecen, se puede generar una vez un valor de un resultado determinado con una característica invariable según el flujo de tiempo y el entorno de uso, y puede permanecer sin cambios.

El generador de claves de identificación puede establecer un tamaño del contacto o un tamaño de la vía, de modo que la probabilidad de que el contacto o la vía generen cortocircuito en las capas conductoras, y la probabilidad de que el contacto o la vía falle para generar cortocircuito en las capas conductoras, puede ser igual. Aquí, una probabilidad de que un valor digital generado por el generador de claves de identificación correspondiente a 0, y una probabilidad de que un valor digital generado por el generador de claves de identificación correspondiente a 1 pueda corresponder igualmente a 1/2, en donde una probabilidad de 1/2 es equivalente al 50% en adelante.

El generador de claves de identificación puede incluir un circuito para generar un valor digital de 1 bit que usa un solo contacto o una sola vía a través de la conexión de un solo par de capas conductoras, y puede generar una clave de identificación de N bits usando N circuitos.

Cuando una probabilidad de que un valor digital que constituye la clave de identificación de N bits generada por el generador de claves de identificación corresponda a 0 y una probabilidad de que un valor digital que constituye la clave de identificación de N bits generada por el generador de claves de identificación corresponda a 1, no son cercanas a 1/2, la aleatoriedad de la clave de identificación generada puede disminuir.

De acuerdo con un aspecto de la presente invención, puede incluirse adicionalmente una unidad de procesamiento de clave de identificación para procesar la clave de identificación con el fin de asegurar la aleatoriedad de la clave de identificación generada.

El aparato para generar la clave de identificación puede incluir la unidad de procesamiento de claves de identificación para procesar la clave de identificación al recibir una entrada de una clave de identificación leída por el lector de claves de identificación, agrupando los valores digitales que constituyen la clave de identificación en función de k bits y generando una pluralidad de grupos de valores digitales, comparando un primer grupo y un segundo grupo entre la pluralidad de los grupos de valores digitales, y determinando que un valor digital sea 1 cuando un valor que incluya k bits digitales incluidos en el primer grupo sea mayor que un valor que incluya k bits digitales incluidos en el segundo grupo, el valor digital representa el primer grupo y el segundo grupo.

Idealmente, cuando la probabilidad de que se genere 0 y la probabilidad de que se genere 1 corresponde exactamente a 1/2, la aleatoriedad de la clave de identificación generada se puede asegurar al máximo. Sin embargo, la probabilidad de generar un 0 y la probabilidad de generar un 1 pueden no corresponder exactamente a 1/2. Sin embargo, cuando se comparan dos grupos al agruparse en función de k bits, aunque la probabilidad de que se genere 0 y la probabilidad de que se genere 1 puede no corresponder exactamente a la 1/2, los dos grupos pueden estar en una condición igual y, en consecuencia, una probabilidad de que el primer grupo tenga un valor mayor que el segundo grupo y una probabilidad de que el primer grupo tenga un valor más bajo que el segundo grupo puede ser igual.

El primer grupo y el segundo grupo pueden tener un valor igual y, en este caso, un valor digital que representa el primer grupo y el segundo grupo puede determinarse como uno de 1 o 0, o no puede determinarse. Por lo tanto, incluso cuando en el aparato para generar la clave de identificación, la probabilidad de que se genere 0 y la probabilidad de que se genere 1 puede no corresponder exactamente a 1/2, la probabilidad de que se genere 0 y

la probabilidad de que se genere 1 puede ser igual a través de la unidad de procesamiento de identificación, y por lo tanto se puede asegurar la aleatoriedad

Con el fin de generar una clave de identificación de M bits en el aparato para generar la clave de identificación que incluye la unidad de procesamiento de claves de identificación, cuando se realiza una agrupación basada en k bits, puede ser necesario generar M x k bits. Sin embargo, cuando los valores del primer grupo y del segundo grupo son iguales, un valor representativo puede no determinarse en ocasiones y, por lo tanto, se puede configurar un circuito para generar un número de bits más suficiente que los bits M x k.

De acuerdo con un aspecto de la presente invención, se proporciona un aparato para generar una clave de identificación, el aparato incluye un generador de claves de identificación que tiene una separación entre las capas conductoras de un semiconductor, el generador de claves de identificación para generar una clave de identificación en función de si un se produce un cortocircuito entre las capas conductoras del semiconductor y un lector de clave de identificación para leer la clave de identificación mediante la lectura de si ocurre un cortocircuito entre las capas conductoras.

De acuerdo con un aspecto de la presente invención, se proporciona un aparato para generar una clave de identificación, el aparato incluye un generador de claves de identificación que tiene una separación entre las capas conductoras de un semiconductor, el generador de claves de identificación para generar una clave de identificación en función de si se produce un cortocircuito entre las capas conductoras del semiconductor, y un lector de claves de identificación para leer la clave de identificación mediante la lectura de si ocurre un cortocircuito entre las capas conductoras, en donde la separación entre las capas conductoras del semiconductor puede establecerse en un tamaño que viola una regla de diseño proporcionada durante un proceso de fabricación de semiconductores.

El generador de claves de identificación puede tener el espaciado entre las capas conductoras del semiconductor, de modo que una diferencia entre la probabilidad de que ocurra un cortocircuito entre las capas conductoras del semiconductor y la probabilidad de que ocurra una falla de cortocircuito entre las capas conductoras del semiconductor puede caer dentro de un rango de error predeterminado.

De acuerdo con un aspecto de la presente invención, también se proporciona un método para generar una clave de identificación, el método incluye generar una clave de identificación mediante una determinación probabilística de si ocurre un cortocircuito entre los nodos que constituyen un circuito al violar una regla de diseño provista durante un proceso de fabricación de semiconductores, y lectura de la clave de identificación mediante la lectura de si ocurre un cortocircuito entre los nodos que constituyen el circuito.

De acuerdo con un aspecto de la presente invención, también se proporciona un método para generar una clave de identificación, el método que incluye generar la clave de identificación tiene un espacio entre las capas conductoras de un semiconductor, y en función de si ocurre un cortocircuito entre las capas conductoras del semiconductor, y la lectura de la clave de identificación mediante la lectura de si ocurre un cortocircuito entre las capas conductoras, en donde la separación entre las capas conductoras del semiconductor se establece en un tamaño que viola la regla de diseño provista durante un proceso de fabricación de semiconductores.

Efecto de la invención

De acuerdo con realizaciones de ejemplo, se proporcionan un aparato y un método para generar una clave de identificación que puede ser altamente confiable ya que la clave de identificación puede generarse aleatoriamente a través de un proceso de fabricación de semiconductores, y un valor de la clave de identificación puede ser invariante una vez generado.

De acuerdo con realizaciones de ejemplo, se proporcionan un aparato y un método para generar una clave de identificación que puede garantizar probabilísticamente un equilibrio entre un valor digital de 0 y un valor digital de 1 en una clave de identificación en forma de un valor digital, y por lo tanto la aleatoriedad puede ser asegurada.

De acuerdo con realizaciones de ejemplo, se proporcionan un aparato y un método para generar una clave de identificación que puede fabricarse a un costo relativamente bajo y de una manera simple, puede ser físicamente inclonable y, por consiguiente, puede ser inmune a un ataque externo.

Breve descripción de los dibujos

Estos y/u otros aspectos, características y ventajas de la invención se harán evidentes y se apreciarán más fácilmente a partir de la siguiente descripción de realizaciones de ejemplo, tomadas junto con los dibujos adjuntos, en los que:

La figura 1 es un diagrama que ilustra un aparato para generar una clave de identificación de acuerdo con una realización de ejemplo;

La figura 2 es un diagrama que describe una configuración de un generador de claves de identificación de acuerdo con una realización de ejemplo;

La figura 3 es un gráfico que describe una configuración de un generador de claves de identificación de acuerdo con una realización de ejemplo;

La figura 4 es un diagrama que describe una configuración de un generador de claves de identificación de acuerdo con una realización de ejemplo;

La figura 5 es un diagrama que ilustra un arreglo de contactos o un arreglo de vías que puede permitir generar una clave de identificación mediante un generador de claves de identificación de acuerdo con una realización de ejemplo;

La figura 6 es un diagrama que ilustra una configuración de un generador de claves de identificación que puede generar una clave de identificación utilizando el arreglo de contactos o el arreglo de vías de la figura 5 de acuerdo con una realización de ejemplo;

La figura 7 es un diagrama que describe un proceso de procesamiento de una clave de identificación por una unidad de procesamiento de claves de identificación de acuerdo con una realización de ejemplo; y

La figura 8 es un diagrama que ilustra un método para generar una clave de identificación de acuerdo con una realización de ejemplo.

Descripción detallada

Ahora se hará referencia en detalle a realizaciones de ejemplo de la presente divulgación, cuyos ejemplos se ilustran en los dibujos adjuntos, en los que numerales de referencia similares se refieren a los elementos similares en todas partes. Las realizaciones de ejemplo se describen a continuación para explicar la presente invención haciendo referencia a las figuras.

La figura 1 es un diagrama que ilustra un aparato 100 para generar una clave de identificación de acuerdo con una realización de ejemplo.

Un generador 110 de claves de identificación puede generar, a través de un proceso semiconductor, una clave de identificación que puede ser invariante al flujo de tiempo y, aunque la clave de identificación generada puede ser aleatoria, puede ser invariante al flujo de tiempo.

La clave de identificación generada por el generador 110 de claves de identificación puede corresponder, por ejemplo, a un valor digital de N bits, siendo N un número natural.

Los factores de confiabilidad de una clave de identificación que se generará pueden incluir aleatoriedad de la clave de identificación generada e invariabilidad de la clave de identificación que puede ser invariante al flujo de tiempo.

El generador 110 de claves de identificación puede configurarse para tener aleatoriedad dependiendo de si ocurre un cortocircuito entre los nodos generados en un proceso de fabricación de semiconductores. Además, si el cortocircuito ocurre entre los nodos puede ser invariante al flujo de tiempo y al entorno de uso y, en consecuencia, la clave de identificación puede ser invariante una vez generada.

El generador 110 de claves de identificación puede generar una clave de identificación en función de si las capas conductoras, por ejemplo, las capas metálicas, tienen cortocircuito por un contacto o una vía que puede formarse entre las capas conductoras generadas durante un proceso de fabricación de semiconductores.

El contacto o la vía pueden estar diseñados para conectar las capas conductoras, y un tamaño del contacto o un tamaño de la vía puede determinarse comúnmente para generar cortocircuito en las capas conductoras. Una regla de diseño común puede determinar un tamaño mínimo del contacto o la vía para garantizar un cortocircuito entre las capas conductoras.

Sin embargo, en la configuración del generador 110 de claves de identificación de acuerdo con una realización de ejemplo, se puede determinar que el tamaño del contacto o el tamaño de la vía es más pequeño que el tamaño determinado por la regla de diseño, y por lo tanto una parte de los contactos o una parte de las vías puede generar cortocircuito en las capas conductoras, y la otra parte de los contactos o la otra parte de las vías pueden no generar cortocircuito en las capas conductoras. Aquí, si el cortocircuito ocurre puede ser determinado probabilísticamente.

En un proceso semiconductor convencional, cuando un contacto o una vía falla en generar cortocircuitos en capas conductoras, aunque se puede considerar que el proceso ha fallado, se puede usar para generar una clave de identificación que tenga aleatoriedad.

La configuración del tamaño del contacto o el tamaño de la vía de acuerdo con la realización descrita anteriormente se describirá adicionalmente con referencia a la figura 2 y la figura 3.

De acuerdo con otra realización de la presente invención, el generador 110 de clave de identificación puede generar una clave de identificación que tiene aleatoriedad por una determinación probabilística de si ocurre un cortocircuito entre líneas conductoras, determinando que el espaciado entre las líneas conductoras es menor que un tamaño determinado por una regla de diseño, durante un proceso de fabricación de semiconductores.

La realización descrita anteriormente se puede usar para generar una clave de identificación aleatoria al violar las reglas de diseño, lo que puede garantizar una abertura entre las líneas conductoras, es decir, una separación mayor que un nivel predeterminado, durante un proceso de fabricación de semiconductor convencional.

La configuración del espaciado entre las líneas conductoras se describirá adicionalmente con referencia a la figura 4.

El generador 110 de clave de identificación puede generar eléctricamente la clave de identificación generada de acuerdo con la realización descrita anteriormente de la presente invención. Se puede identificar si un contacto o una vía hace cortocircuito de capas conductoras o si ocurre un cortocircuito entre líneas conductoras utilizando un transistor de lectura, una configuración de la cual se describirá con más detalle con referencia a la figura 6.

En una realización que utiliza un ajuste de tamaño del contacto o la vía, incluso cuando una relación del contacto o la vía que genera cortocircuito en las capas conductoras ajustando el tamaño del contacto o la vía y la relación del contacto o la vía que falla en generar cortocircuitos en capas conductoras se puede ajustar para que tenga una probabilidad igual a 1/2, puede ser posible que exista una relación exactamente igual entre el caso en que ocurre el cortocircuito (por ejemplo, un valor digital de 0) y el caso opuesto (por ejemplo, un valor digital de 1) no se puede garantizar probabilísticamente.

Es decir, a medida que el tamaño del contacto o la vía se acerca a un valor determinado por una regla de diseño, la probabilidad de que ocurra un cortocircuito puede ser mayor y, a la inversa, a medida que el tamaño del contacto o la vía se hace más pequeño que el valor determinado por la regla de diseño, la probabilidad de que ocurra una falla de cortocircuito puede ser mayor. Cuando una de las probabilidades de que ocurra un cortocircuito y la probabilidad de que ocurra un cortocircuito no sea mayor, la aleatoriedad de una clave de identificación generada puede disminuir.

El mismo problema puede surgir en una realización de ejemplo de ajuste de la separación entre las líneas conductoras como se describió anteriormente.

Por lo tanto, el aparato 100 para generar la clave de identificación puede incluir además una unidad 130 de procesamiento de clave de identificación para procesar la clave de identificación generada por el generador 110 de clave de identificación, que puede aumentar o garantizar la aleatoriedad. Aunque el término unidad de procesamiento de clave de identificación se puede usar para referirse al numeral 130 de referencia en esta divulgación, la presente divulgación no se limita a esta realización de ejemplo específica.

Una operación de la unidad 130 de procesamiento de clave de identificación se describirá adicionalmente con referencia a la figura 7.

La figura 2 es un diagrama que describe una configuración de un generador de claves de identificación de acuerdo con una realización de ejemplo.

En la figura 2, se ilustra una configuración de vías que pueden formarse entre una capa 202 de metal 1 y una capa 201 de metal 2 durante un proceso de fabricación de semiconductores.

En un grupo 210 en donde las vías se pueden establecer en un tamaño suficiente según lo determinado por una regla de diseño, todas las vías pueden generar cortocircuito en la capa 202 de metal 1 y la capa 201 de metal 2, y si se produce un cortocircuito se puede indicar con un valor digital de 0.

En un grupo 230 en donde las vías pueden establecerse en un tamaño pequeño, es posible que todas las vías no hagan cortocircuito para la capa 202 de metal 1 y para la capa 201 de metal 2. Aquí, si se produce un cortocircuito se puede indicar con un valor digital de 1.

En un grupo 220 donde las vías se establecen en un tamaño mediano entre el tamaño del grupo 210 y el tamaño del grupo 230, parte de las vías pueden generar cortocircuito en la capa 202 de metal 1 y la capa 201 de metal 2, y la otra parte de las vías pueden no generar cortocircuito en la capa 202 de metal 1 y la capa 201 de metal 2.

Al igual que en el grupo 220, el generador 110 de claves de identificación puede configurarse estableciendo un tamaño de vías de modo que parte de las vías puedan generar cortocircuito en la capa 202 de metal 1 y la capa 201 de metal 2, y la otra parte de las vías no puedan generar cortocircuito en la capa 202 de metal 1 y la capa 201 de metal 2.

Una regla de diseño con respecto a un tamaño de una vía puede ser diferente dependiendo del proceso de fabricación de un semiconductor. Por ejemplo, cuando una regla de diseño de una vía se establece en 0.25 μm durante un proceso complementario de óxido de metal semiconductor (CMOS) de 0.18 μm, el generador 110 de clave de identificación puede establecer un tamaño de una vía como 0.19 μm, y permitiendo así una distribución probabilística de si ocurre un cortocircuito entre las capas metálicas.

Una probabilidad ideal de que ocurra un cortocircuito con respecto a la distribución de probabilidad de si el cortocircuito ocurre puede corresponder a una probabilidad del 50%. El generador 110 de claves de identificación puede configurarse estableciendo un tamaño de vía para que se corresponda con la distribución de probabilidad ideal o lo más cerca posible de la distribución de probabilidad del 50%. En ciertas realizaciones, el tamaño de la vía se puede determinar de acuerdo con un experimento basado en el proceso.

La figura 3 es un gráfico que describe una configuración de un generador de claves de identificación de acuerdo con una realización de ejemplo.

Como se confirma en el gráfico, a medida que el tamaño de una vía se hace mayor, la probabilidad de que ocurra un cortocircuito entre las capas metálicas puede ser cercana a 1. El tamaño de una vía determinado por una regla de diseño puede corresponder a Sd, que puede ser un valor para garantizar suficientemente un cortocircuito entre las capas metálicas.

Sm puede ser un tamaño de una vía en la que la probabilidad de que ocurra un cortocircuito entre las capas metálicas puede corresponder teóricamente a 0.5. Sm puede tener un valor diferente basado en un proceso, y en ciertas realizaciones, un valor aproximado, aunque no exacto, se puede encontrar de acuerdo con un experimento basado en el proceso.

En el generador 110 de claves de identificación, si se produce un cortocircuito entre las capas metálicas se puede establecer en 0.5, dentro de un rango de Sx1 (no mostrado) y Sx2 (no mostrado) que puede tener un error permisible predeterminado. Aquí, Sx1 y Sx2 pueden estar cerca del Sx mostrado, y pueden corresponder a un tamaño que tiene un margen predeterminado.

La figura 4 es un diagrama que describe una configuración de un generador de claves de identificación de acuerdo con una realización de la presente invención.

De acuerdo con otra realización de la presente invención, si un cortocircuito ocurre entre líneas de metal puede determinarse probabilísticamente ajustando un espacio entre las líneas de metal.

En un grupo 410 donde el espacio entre líneas de metal se puede establecer para que sea relativamente estrecho para garantizar o aumentar la probabilidad de un cortocircuito entre las líneas de metal, en todos los casos puede ocurrir un cortocircuito entre las líneas de metal.

En un grupo 430 donde el espaciado entre las líneas de metal se puede establecer para que sea relativamente grande, puede que no ocurra un cortocircuito entre las líneas de metal en todos los casos.

Al igual que en un grupo 420, el generador 110 de claves de identificación puede establecer un espaciado donde la probabilidad de que ocurra un cortocircuito entre las líneas de metal es tal que parte de las líneas de metal puede generar cortocircuito y la otra parte de las líneas de metal puede no generar cortocircuito.

La figura 5 es un diagrama que ilustra un arreglo de contactos o un arreglo de vías que puede formarse en una capa semiconductora para generar una clave de identificación mediante el generador 110 de claves de identificación de acuerdo con una realización de ejemplo.

En la figura 5, se ilustra una configuración de vías formadas entre capas metálicas que pueden estar en capas sobre un sustrato semiconductor, incluidas vías M en anchura (o una alineación horizontal) y vías N en longitud (o una alineación vertical), es decir, vías M x N en total, M y N son números naturales.

El generador 110 de clave de identificación puede generar una clave de identificación de M x N-bit basada en si cada una de las vías de M x N genera cortocircuito en las capas metálicas (un valor digital de 0), o falla en generar cortocircuitos en las capas metálicas (un valor digital de 1).

La clave de identificación de M x N-bit generada puede ser leída por el lector 120 de claves de identificación.

La figura 6 es un diagrama que ilustra una configuración de un circuito del generador 120 de clave de identificación de acuerdo con una realización de ejemplo.

El generador 120 de clave de identificación puede identificar valores lógicos digitales utilizando un transistor de lectura entre un voltaje VDD de referencia y una conexión a tierra.

En un ejemplo de la figura 6, que incluye un circuito de descenso, cuando una vía individual en el generador 110 de claves de identificación genera cortocircuito en capas metálicas, un valor de salida puede corresponder a 0, y

cuando una vía individual falla en generar cortocircuitos en capas metálicas, un valor de salida puede corresponder a 1, y por lo tanto, el generador 110 de clave de identificación puede generar una clave de identificación. Aunque no se describe con mayor detalle, una descripción con respecto al circuito de descenso se extiende a un ejemplo de una configuración que incluye un circuito de ascenso.

Se puede generar una clave de identificación de una manera similar en una realización de ejemplo usando un cortocircuito entre líneas de metal.

Aunque una única realización de ejemplo de una configuración del generador 120 de clave de identificación de la figura 6 se describe, la presente divulgación no se limita a la realización de ejemplo específica.

Por lo tanto, en el caso de una configuración que puede generar un valor digital al determinar si se produce un cortocircuito entre capas metálicas o entre líneas de metal en el generador 110 de claves de identificación, se pueden realizar varias modificaciones y variaciones sin apartarse del alcance de la divulgación.

La clave de identificación generada por el generador 110 de claves de identificación puede transmitirse y almacenarse en el lector 120 de claves de identificación. El lector 120 de claves de identificación puede corresponder a un registro o un biestable (no mostrado) que puede recibir una entrada de la clave de identificación generada, y puede almacenar la clave de identificación generada.

En ciertas realizaciones, el lector 120 de claves de identificación puede corresponder al registro o al biestable así como a otras configuraciones análogas al registro o al biestable que pueden leer y almacenar la clave de identificación generada.

La figura 7 es un diagrama que describe un proceso de procesamiento de una clave de identificación por una unidad de procesamiento de claves de identificación de acuerdo con una realización de ejemplo.

La unidad 130 de procesamiento de clave de identificación puede agrupar valores digitales de M x N-bit generados por el generador 110 de clave de identificación basado en un número predeterminado.

Aunque la agrupación conceptual de los valores digitales se ha descrito con referencia a la figura 7, la presente invención no está limitada a la realización de ejemplo descrita. Los expertos en la técnica pueden apreciar que en ciertas realizaciones, el lector 120 de clave de identificación que incluye registros o biestables puede agrupar los registros o los biestables.

En la figura 7, se pueden agrupar cuatro valores digitales en un solo grupo.

La unidad 130 de procesamiento de identificación puede comparar valores digitales de 4 bits generados por cada uno de un grupo 710 y un grupo 720. Cuando el valor digital de 4 bits del grupo 710 puede ser mayor que el valor digital de 4 bits del grupo 720, un valor digital que representa el grupo 710 y el grupo 720 puede determinarse como 1.

A la inversa, cuando el valor digital de 4 bits del grupo 710 puede ser menor que el valor digital de 4 bits del grupo 720, se puede determinar que el valor digital que representa el grupo 710 y el grupo 720 es 0.

En ciertas realizaciones, cuando el valor digital de 4 bits del grupo 720 puede ser mayor que el valor digital de 4 bits del grupo 710, se puede determinar que el valor digital representativo es 1.

Cuando el valor digital de 4 bits del grupo 710 y el valor digital de 4 bits del grupo 720 pueden ser iguales, se puede determinar que el valor digital representativo es uno de 1 y 0, o puede ser indeterminado.

Usando este esquema, se puede determinar una clave de identificación usando la clave de identificación generada al generar el valor digital representativo usando la comparación de un grupo 730 y un grupo 740, y similares.

La descripción anterior se puede describir como un proceso de procesamiento de la clave de identificación para aumentar la aleatoriedad de la clave de identificación.

En el generador 110 de claves de identificación, cuando una relación de un cortocircuito que se produce (un valor digital de 0) y una relación de un cortocircuito que no se produce (un valor digital de 1) son diferentes, un equilibrio entre 0 y 1 puede no ser realizado a veces. Aquí, la probabilidad de que se genere 1 y la probabilidad de que se genere 0 con respecto a cada bit puede ser diferente del 50%. Sin embargo, dado que dos grupos pueden ser equivalentes, la probabilidad de que uno de los dos grupos tenga un valor digital mayor que el otro de los dos grupos puede corresponder al 50%. Por lo tanto, un equilibrio probabilístico entre 0 y 1 se puede realizar a través del proceso descrito anteriormente.

Cuando la clave de identificación originalmente generada corresponde a M x N bits, la clave de identificación puede ser determinada por la unidad 130 de procesamiento de clave de identificación de la figura 7 y puede corresponder a M x N/8 bits ya que un nuevo valor digital de 1 bit se puede determinar utilizando un valor digital de 8 bits.

La descripción anterior con respecto a un proceso de agrupación o un proceso de procesamiento de la clave de identificación por la unidad 130 de procesamiento de claves de identificación no se limita a una realización de ejemplo, y las modificaciones y variaciones del proceso de procesamiento de la clave de identificación para mantener un equilibrio entre el valor digital de 0 y el valor digital de 1 se pueden hacer sin apartarse del espíritu de la divulgación o el alcance de la divulgación.

La nueva clave de identificación que puede ser generada por el generador 110 de claves de identificación y determinada por la unidad 130 de procesamiento de claves de identificación puede tener aleatoriedad y puede convertirse en un valor confiable que, en teoría, puede permanecer invariable una vez que se genera.

De acuerdo con realizaciones de la presente invención, una clave de identificación confiable que tiene una característica de un número aleatorio que puede ser invariable según el flujo de tiempo puede fabricarse fácilmente a costos de fabricación relativamente bajos.

La clave de identificación aleatoria puede generarse durante un proceso de fabricación de semiconductores, y la clave de identificación puede ser invariante después de que se haya completado la fabricación, y por lo tanto, un proceso de entrada externa de la clave de identificación a una memoria no volátil, en un esquema convencional, puede ser innecesario. Por lo tanto, un proceso de entrada y salida externa de la clave de identificación puede estar ausente, e incluso cuando se filtra un dibujo de diseño para un chip semiconductor, porque la clave de identificación puede generarse en función de una diferencia de características físicas durante un proceso de fabricación, la clave de identificación puede ser inclonable y proporcionar una seguridad considerablemente excelente. Además, dado que el proceso de fabricación de la memoria no volátil puede ser innecesario, los costos de fabricación pueden reducirse.

La figura 8 es un diagrama que ilustra un método para generar una clave de identificación de acuerdo con una realización de ejemplo.

En la operación 810, el generador 110 de clave de identificación puede generar una clave de identificación.

El generador 110 de claves de identificación puede configurarse para tener aleatoriedad en cuanto a si ocurre un cortocircuito entre nodos generados durante un proceso de fabricación de semiconductores. Además, una característica de si el cortocircuito ocurre entre los nodos puede ser físicamente invariante y, en consecuencia, la clave de identificación puede ser invariante una vez generada.

El generador 110 de claves de identificación puede generar una clave de identificación en función de si ocurre un cortocircuito entre un contacto o una vía que puede formarse entre capas conductoras generadas durante un proceso de fabricación de semiconductores. La configuración de un tamaño del contacto o un tamaño de la vía es como se describe anteriormente con referencia a la figura 2 y la figura 3.

El generador 110 de clave de identificación puede ajustar el espaciado entre las líneas conductoras durante un proceso de fabricación de semiconductores, de modo que parte de las líneas conductoras generan cortocircuitos y la otra parte de las líneas conductoras fallan en generar cortocircuitos, generando así una clave de identificación que tiene aleatoriedad. La realización es como se describe anteriormente con referencia a las figuras 4 a 6.

En la operación 820, el lector 120 de claves de identificación puede almacenar la clave de identificación generada usando un registro o un biestable. En la generación de la clave de identificación y la lectura de la clave de identificación, se puede identificar si el contacto o la vía generan cortocircuito, ya sea capas conductoras o líneas conductoras, utilizando un transistor de lectura, que es como se describió anteriormente con referencia a la figura 6.

En la operación 830, la unidad 130 de procesamiento de clave de identificación puede procesar la clave de identificación generada por el generador 110 de clave de identificación, y por tanto puede garantizar la aleatoriedad.

El proceso de procesamiento de la clave de identificación es como se describe anteriormente con referencia a la figura 7.

Las realizaciones de ejemplo descritas anteriormente de la presente divulgación pueden grabarse en medios legibles por ordenador no transitorios que incluyen instrucciones de programa para implementar diversas operaciones incorporadas por un ordenador. Los medios también pueden incluir, solos o en combinación con las instrucciones del programa, archivos de datos, estructuras de datos y similares. Los ejemplos de medios legibles por ordenador no transitorios incluyen medios magnéticos como discos duros, disquetes y cintas magnéticas; medios ópticos, tales como discos CD ROM y DVD; medios magneto ópticos tales como discos ópticos; y dispositivos de hardware que están especialmente configurados para almacenar y ejecutar instrucciones de programas, como memoria de solo lectura (ROM), memoria de acceso aleatorio (RAM), memoria flash y similares. Los ejemplos de instrucciones del programa incluyen tanto el código de máquina, como el código producido por un compilador, y los archivos que contienen un código de nivel superior que puede ser ejecutado por el ordenador usando un intérprete. Los dispositivos de hardware descritos pueden configurarse para actuar como uno o más

módulos de software para realizar las operaciones de las realizaciones de ejemplo de la presente invención descritas anteriormente, o viceversa.

Aunque se han mostrado y descrito algunas realizaciones de ejemplo de la presente invención, la presente divulgación no se limita a las realizaciones de ejemplo descritas. En su lugar, los expertos en la técnica apreciarán que se pueden realizar cambios en estas realizaciones de ejemplo sin apartarse de los principios de la invención, cuyo alcance está definido por las reivindicaciones y sus equivalentes.

REIVINDICACIONES

1. Un aparato para generar una clave de identificación, el aparato comprende:

un generador (110) de claves configurado para generar un bit digital basado en si un contacto o una vía formada entre las capas (201, 202) conductoras de un circuito genera cortocircuito en las capas conductoras del circuito; y

un procesador (130) configurado para:

agrupar una pluralidad de bits digitales generados por el generador (110) de claves basado en a una pluralidad de contactos o vías en un primer grupo (710) con k bits digitales y un segundo grupo (720) con k bits digitales, en donde k es un número natural; y

comparar el primer grupo (710) y el segundo grupo (720) para determinar un valor digital para una clave de identificación.

2. El aparato de la reivindicación 1, en donde:

el valor digital para la clave de identificación es 1 cuando los k bits digitales del primer grupo son mayores que los k bits digitales del segundo grupo;

el valor digital para la clave de identificación es 0 cuando los k bits digitales del primer grupo son mayores que los k bits digitales del segundo grupo;

el valor digital para la clave de identificación es 1 cuando los k bits digitales del primer grupo son menores que los k bits digitales del segundo grupo;

el valor digital para la clave de identificación es 0 cuando los k bits digitales del primer grupo son menores que los k bits digitales del segundo grupo; o

el valor digital para la clave de identificación es 1, 0, o no determinado cuando los k bits digitales del primer grupo son iguales a los k bits digitales del segundo grupo.

3. El aparato de la reivindicación 1 o la reivindicación 2, que comprende además:

un lector (120) de claves configurado para leer la clave de identificación usando uno de un circuito de descenso y un circuito de ascenso.

4. El aparato de cualquiera de las reivindicaciones 1-3, en donde la clave de identificación comprende N valores digitales generados usando configuraciones N, en donde N es un número natural.

5. El aparato de cualquiera de las reivindicaciones 1-4, en donde el contacto o la vía está diseñado para ser diferente de un tamaño determinado por una regla de diseño durante un proceso de fabricación de semiconductores.

6. El aparato según cualquiera de las reivindicaciones 1 a 5, en donde el tamaño de la separación entre las capas (201, 202) conductoras del circuito está diseñado para ser diferente de un tamaño determinado por una regla de diseño durante un proceso de fabricación de semiconductores.

7. Un método para generar una clave de identificación, el método comprende:

generar bits digitales en función de si los contactos o las vías formadas entre las capas (201, 202) conductoras de un circuito, respectivamente, generan cortocircuito en las capas conductoras del circuito;

agrupar los bits digitales generados en un primer grupo (710) con k bits digitales y un segundo grupo (720) con k bits digitales, en donde k es un número natural; y

comparar el primer grupo (710) y el segundo grupo (720) para determinar un valor digital que forma la clave de identificación.

8. El método de la reivindicación 8, en donde si un contacto o una vía formada entre las capas (201, 202) conductoras del circuito generan cortocircuito las capas conductoras del circuito son invariantes con el tiempo.

9. El método de la reivindicación 7 u 8, en donde la probabilidad de que un contacto o una vía formada entre las capas (201, 202) conductoras del circuito genere cortocircuito en las capas conductoras del circuito está dentro de un rango permisible predeterminado.

10. El método de cualquiera de las reivindicaciones 7-9, que comprende además: leer (830) la clave de identificación, en donde leer la clave de identificación comprende además usar uno de un circuito de descenso y un circuito de ascenso.

11. El método de cualquiera de las reivindicaciones 7-10, en donde la clave de identificación comprende N valores digitales y se genera usando configuraciones N, en donde N es un número natural.

12. El método de cualquiera de las reivindicaciones 7-11, en donde:

el valor digital para la clave de identificación es 1 cuando los k bits digitales del primer grupo son mayores que los k bits digitales del segundo grupo;

el valor digital para la clave de identificación es 0 cuando los k bits digitales del primer grupo son mayores que los k bits digitales del segundo grupo;

el valor digital para la clave de identificación es 1 cuando los k bits digitales del primer grupo son menores que los k bits digitales del segundo grupo;

el valor digital para la clave de identificación es 0 cuando los k bits digitales del primer grupo son menores que los k bits digitales del segundo grupo; o

el valor digital para la clave de identificación es 1, 0, o no determinado cuando los k bits digitales del primer grupo son iguales a los k bits digitales del segundo grupo.

13. Un chip semiconductor adaptado para generar una clave de identificación por uno cualquiera de los métodos de las reivindicaciones 7-12.

FIG. 1

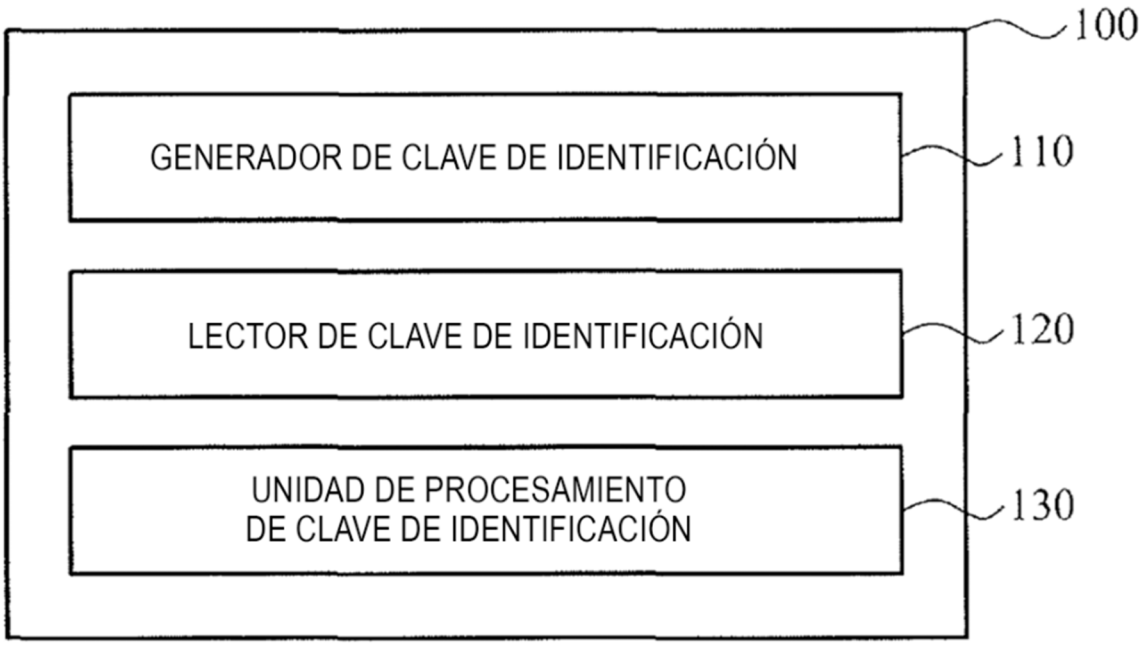

100
GENERADOR DE CLAVE DE IDENTIFICACIÓN
110
LECTOR DE CLAVE DE IDENTIFICACIÓN
120
UNIDAD DE PROCESAMIENTO
DE CLAVE DE IDENTIFICACIÓN
130

FIG. 2

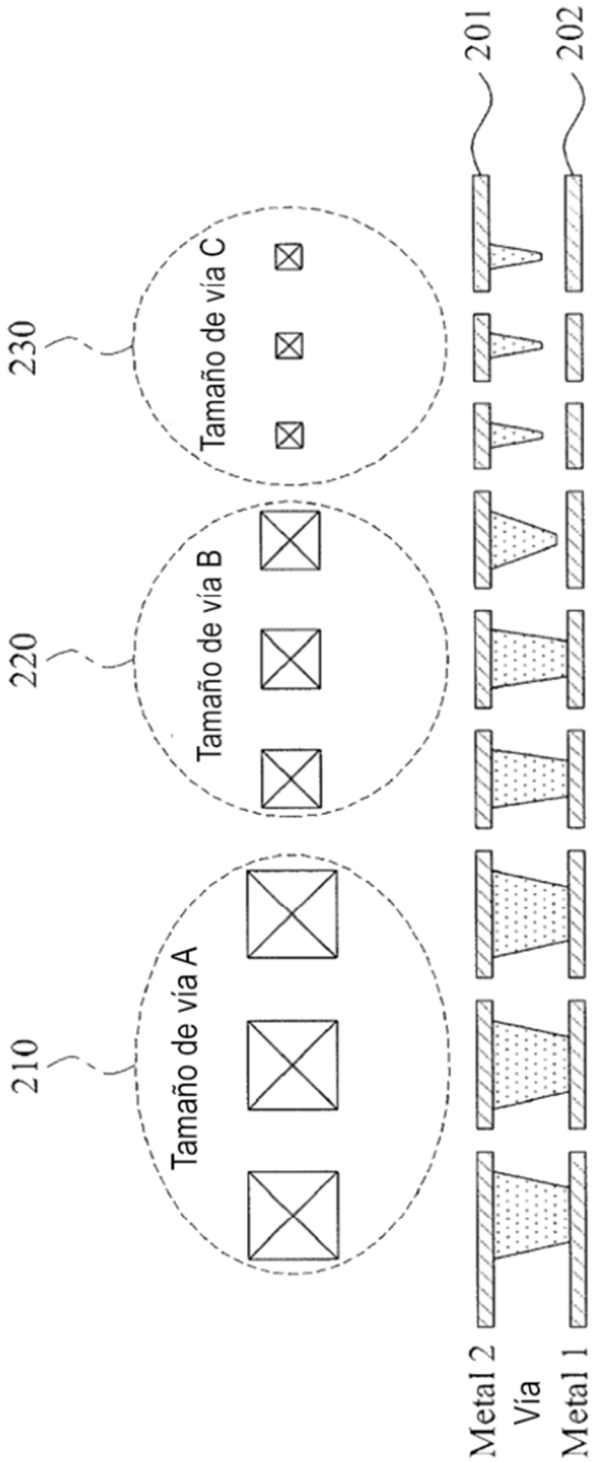

210
Tamaño de vía A
220
Tamaño de vía B
230
Tamaño de vía C
201
202
Metal 2
Vía
Metal 1
Valor
0
0
0
0
1
1
1
1

FIG. 3

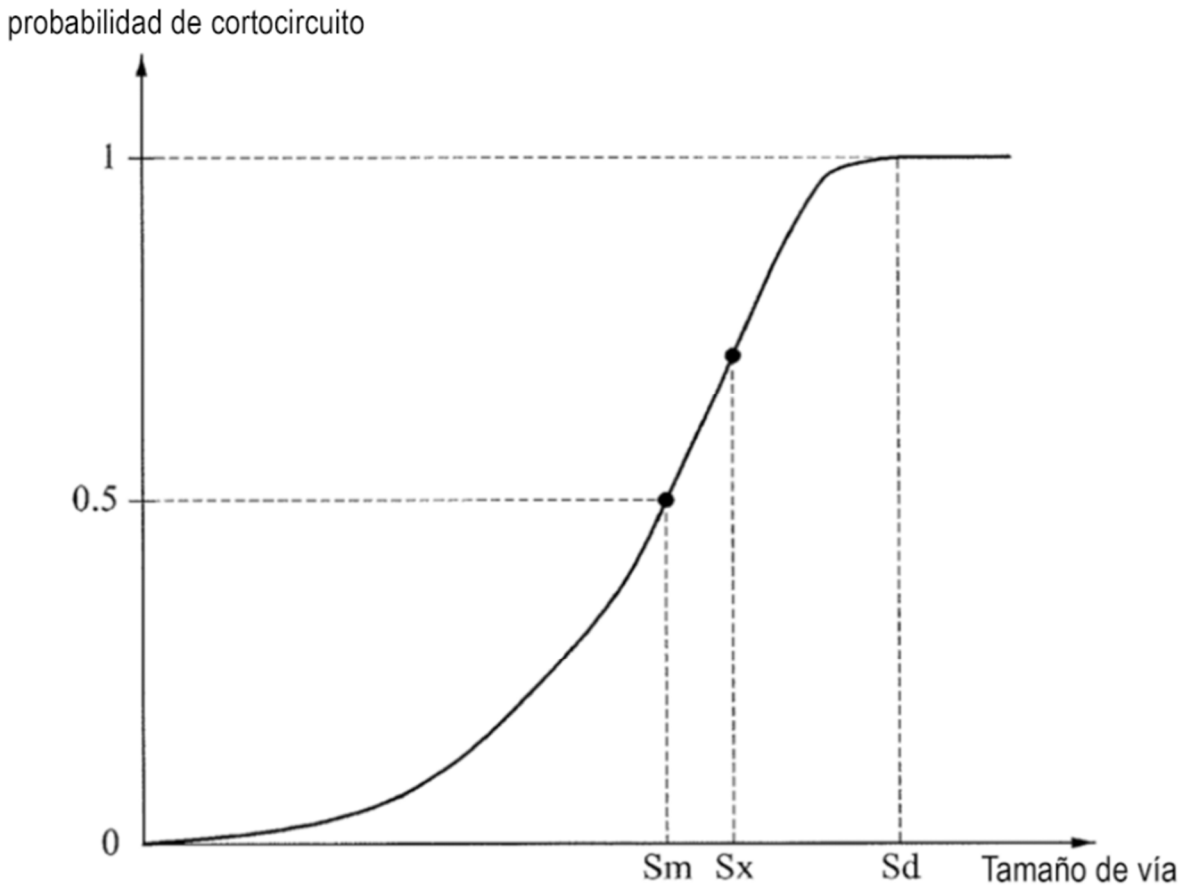


FIG. 4

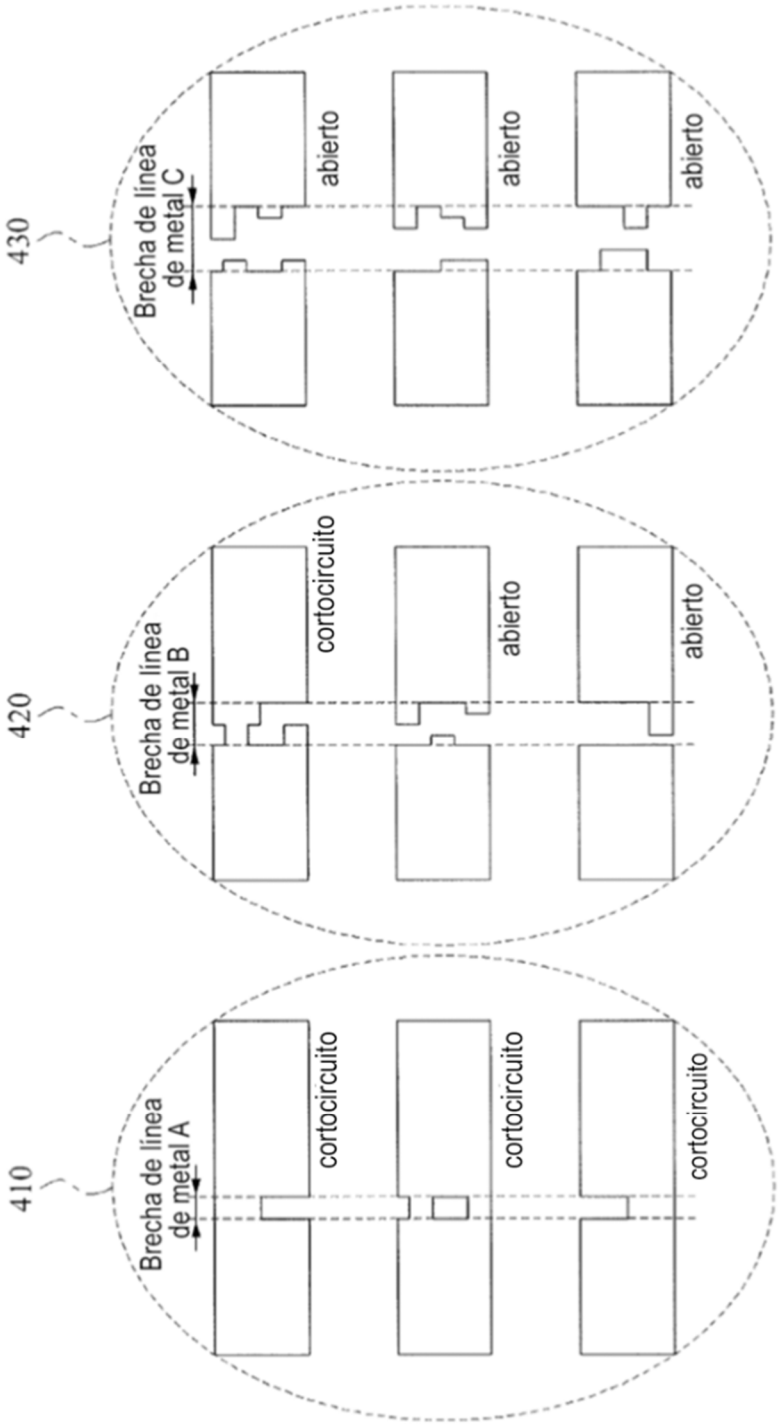

430
Brecha de línea de metal C
abierto
abierto
abierto
420
Brecha de línea de metal B
cortocircuito
abierto
abierto
410
Brecha de línea de metal A
cortocircuito
cortocircuito
cortocircuito

FIG. 5

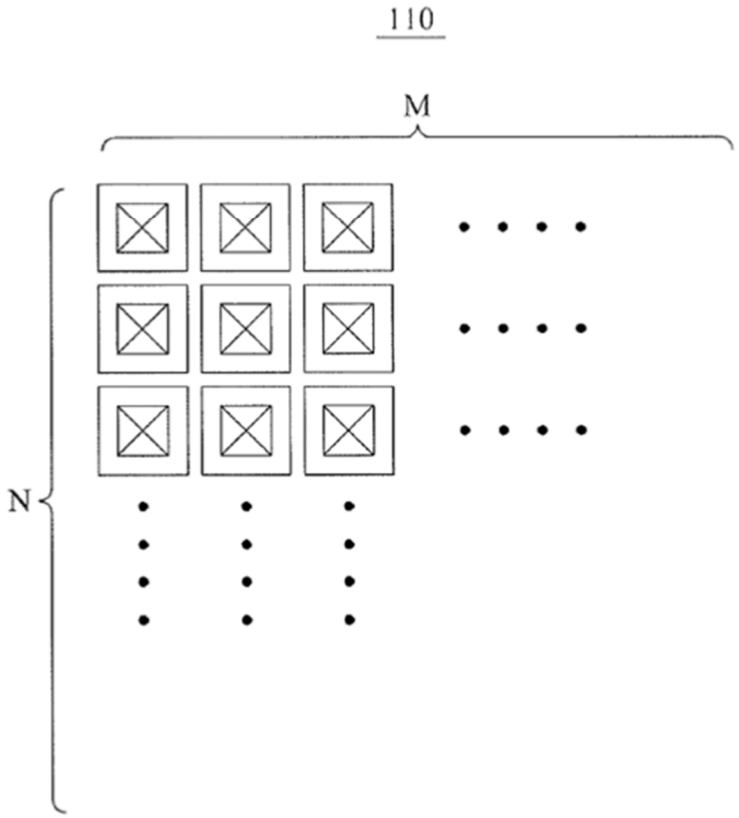


FIG. 6

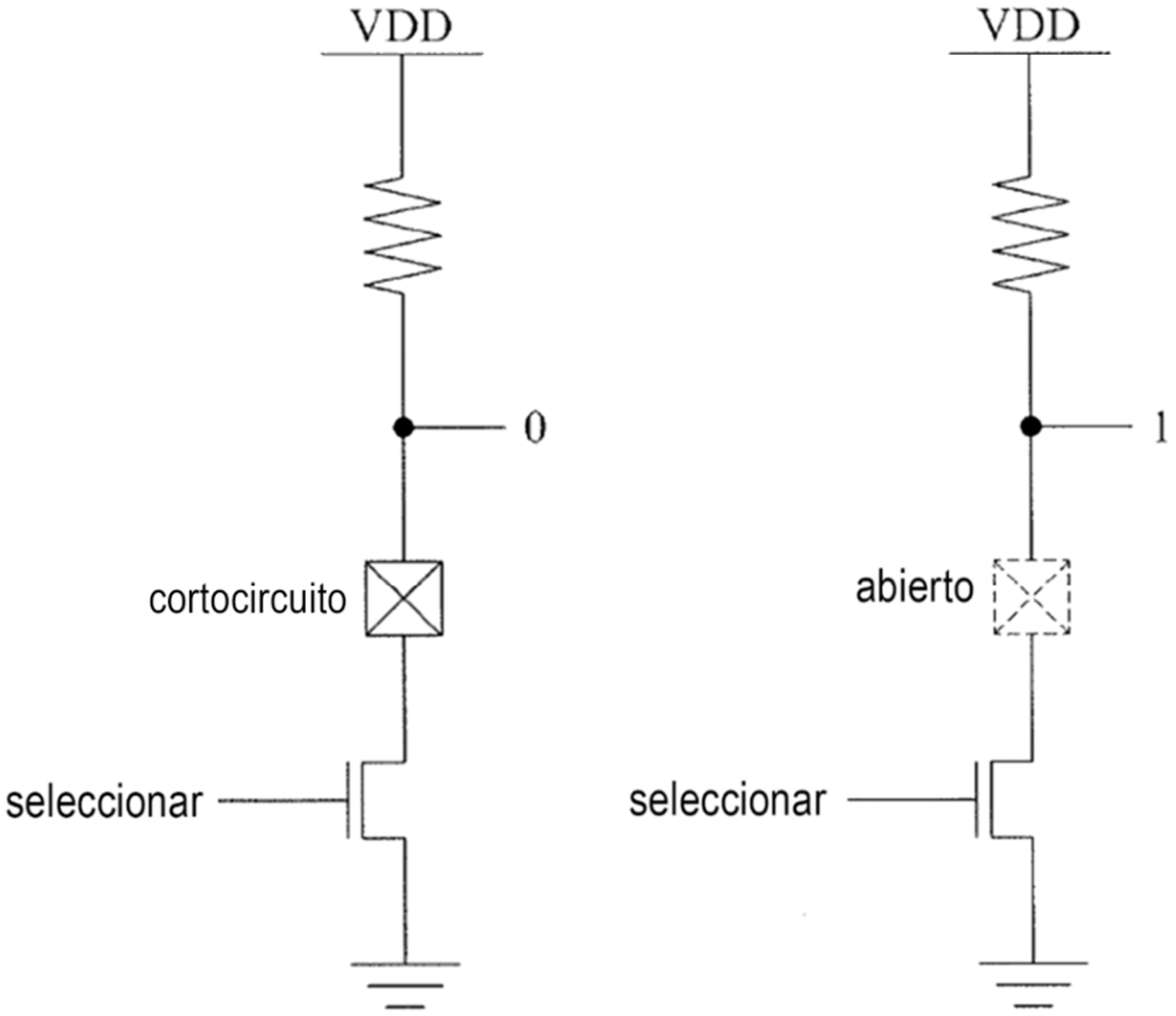

VDD
0
cortocircuito
seleccionar
VDD
1
abierto
seleccionar

FIG. 7

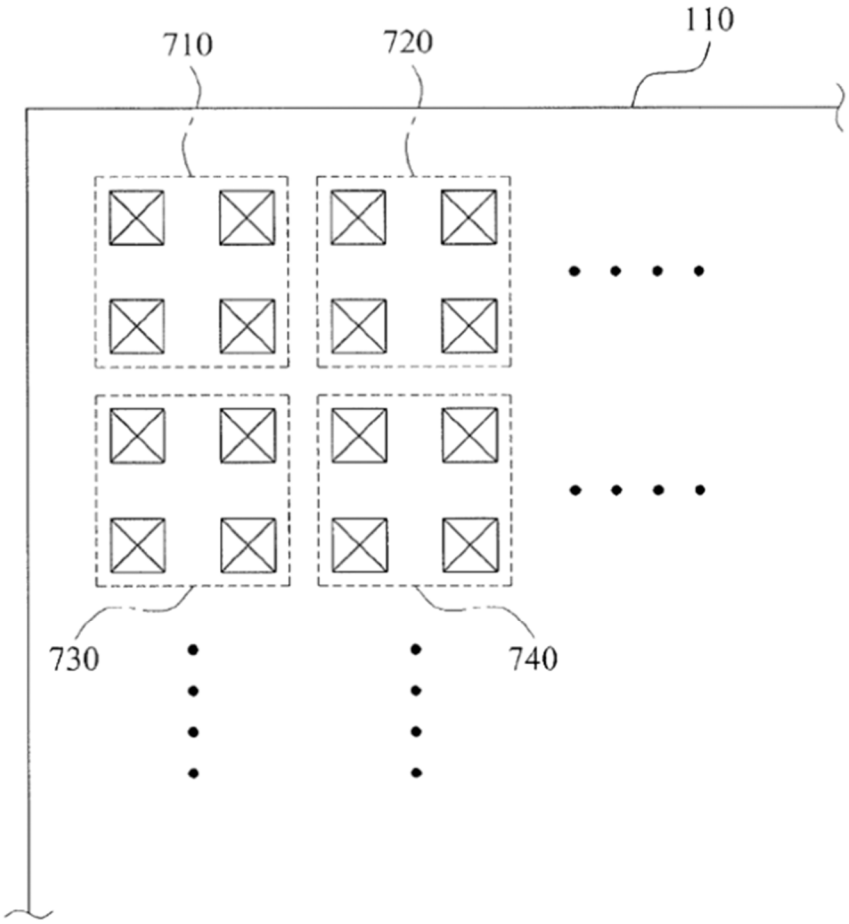
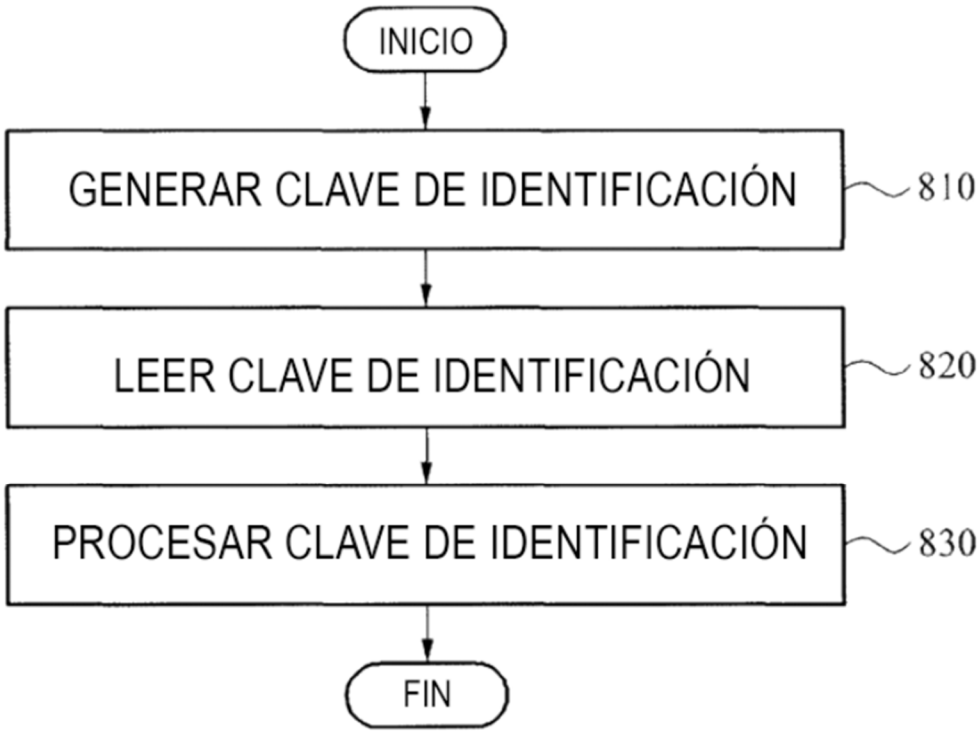


FIG. 8


INICIO
GENERAR CLAVE DE IDENTIFICACIÓN
810
LEER CLAVE DE IDENTIFICACIÓN
820
PROCESAR CLAVE DE IDENTIFICACIÓN
830
FIN