(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 685 758**

(51) Int. CI.:

G06F 21/72 (2013.01)
H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.02.2011 PCT/KR2011/001376**

(87) Fecha y número de publicación internacional: **23.08.2012 WO12111872**

(96) Fecha de presentación y número de la solicitud europea: **28.02.2011 E 11858891 (2)**

(97) Fecha y número de publicación de la concesión europea: **22.08.2018 EP 2677452**

(54) Título: **Dispositivo de encriptación y método para la defensa contra un ataque físico**

(30) Prioridad:

15.02.2011 KR 20110013269

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.10.2018

(73) Titular/es:

ICTK CO., LTD. (100.0%)
2, 3rd Floor, Jawon Building 18, Samseong-ro 71-gil, Gangnam-gu
Seoul 135-997, KR

(72) Inventor/es:

KIM, DONG KYUE y
CHOI, BYOUNG DEOK

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Dispositivo de encriptación y método para la defensa contra un ataque físico

Campo técnico

La presente invención se refiere a la seguridad digital, y de forma más particular, a un dispositivo de encriptación y a un método para gestionar una clave de encriptación para la defensa contra ataques físicos en un módulo de seguridad de circuito integrado (CI), por ejemplo, una tarjeta inteligente, y similares.

Antecedentes de la técnica

Una tarjeta inteligente se refiere a una tarjeta de plástico del tamaño de una tarjeta de crédito, y puede incluir un circuito integrado (CI) para procesar datos. Dicha tarjeta inteligente tiene ventajas, cuando se compara con una tarjeta magnética convencional, ya que la tarjeta inteligente tiene una capacidad de almacenamiento de datos interna, e incluye una unidad de procesamiento, por ejemplo, un coprocesador, un microprocesador y similares.

Por consiguiente, la tarjeta inteligente puede realizar una operación de encriptación de forma autónoma utilizando un algoritmo de encriptación, con el fin de manejar información de pago financiero, información personal para identificación, y similares.

Mientras tanto, con el desarrollo de varias tecnologías de información, las tarjetas inteligentes se utilizan ampliamente, y están aumentando diversas amenazas de seguridad contra las tarjetas inteligentes.

Por ejemplo, los ataques físicos de lectura de información de un chip de CI que utilizan tecnologías de ingeniería inversa que se refieren a chips de CI pueden ser un gran problema en términos de seguridad.

Varios ataques físicos conocidos pueden emplear esquemas de ataque, por ejemplo, sondeo de bus, sondeo en modo de prueba, sobre escritura con respecto a una memoria de sólo lectura (ROM) o una memoria de sólo lectura programable y borrable eléctricamente (EEPROM), y similares, dependiendo de un esquema de almacenamiento de datos y una característica de memoria de una ROM y una EEPROM utilizadas en un módulo de seguridad de hardware.

El documento US 2008/0044010 se refiere a un sistema de encriptación para encriptar datos de entrada basándose en claves secretas. El sistema incluye un calculador de tabla configurado para calcular valores de tabla compuestos de valores de multiplicación escalar es mediante una operación de curva elíptica.

El documento US 2008/285745 se refiere a un procesador para ejecutar un algoritmo de tipo AES. El procesador ejecuta un algoritmo de Rijndeal que aplica una pluralidad de rondas de encriptación a una matriz de bloque de datos con el fin de tener una matriz de tamaño idéntico, a la ronda que incluye una matriz de bloque de clave y una tabla de sustitución de bloque de datos.

El documento EP 2650813 se refiera un dispositivo y método para generar una clave de identificación. La clave de identificación se identificará mediante una determinación probabilística de un corto que sucede entre nodos que constituyen un circuito, violando una regla de diseño prevista durante el proceso de fabricación de un semiconductor.

El documento US 2006/0061795 se refiere a un método de almacenamiento de un bi-patrón en cada uno de una pluralidad de dispositivos. El bi-patrón es almacenado en ubicaciones de memoria diferentes en cada dispositivo, y la ubicación de memoria puede ser seleccionada de forma aleatoria.

Resumen de la invención

De acuerdo con la invención, se proporciona un circuito integrado tal y como se cita por la reivindicación 1, y un método de encriptación tal y como se cita por la reivindicación 13.

Objetivos técnicos

Un aspecto de la presente divulgación proporciona un dispositivo de encriptación y un método robusto contra ataques físicos en una tarjeta inteligente.

En particular, otro aspecto de la presente invención proporciona un dispositivo de encriptación y un método que puede evitar que una clave de encriptación generada o almacenada sea extraída directamente de una memoria. Adicionalmente, otro aspecto más de la presente divulgación proporciona un dispositivo de encriptación y un método que puede evitar la fuga a través de un bus en un chip de circuito integrado (CI) de una tarjeta inteligente.

Soluciones técnicas

De acuerdo con un aspecto de la presente divulgación, se proporciona un dispositivo de encriptación para ejecutar una algoritmo de encriptación que utiliza una clave de encriptación cuando recibe unos datos de entrada que se van a encriptar, el dispositivo de encriptación que incluye un módulo de encriptación, que incluye un módulo de clave de

encriptación para proporcionar una clave de encriptación, para ejecutar el algoritmo de encriptación utilizando la clave de encriptación proporcionada por el módulo de clave de encriptación.

El módulo de encriptación puede incluir una pluralidad de módulos de clave de encriptación para proporcionar diferentes claves de encriptación. En este ejemplo, el modo de encriptación puede incluir un selector de módulo de clave de encriptación para seleccionar uno de la pluralidad de módulos de clave de encriptación, y una unidad de encriptación para ejecutar el algoritmo de encriptación utilizando una clave de encriptación proporcionada por el módulo de clave de encriptación seleccionado.

El selector de módulo de clave de encriptación puede seleccionar un módulo de clave de encriptación correspondiente a un índice de identificación pre asignado de entre la pluralidad de módulos de clave de encriptación.

El modo de encriptación puede incluir una pluralidad de celdas estándar, y la pluralidad de módulos de clave de encriptación puede estar dispuesta en posiciones aleatorias entre disposiciones de la pluralidad de celdas estándar incluidas en el modo de encriptación. Las celdas estándar pueden incluir dispositivos estandarizados o bloques de dispositivos que se van a utilizar para la implementación del módulo de encriptación.

El módulo de encriptación puede ejecutar el algoritmo de encriptación utilizando la clave de encriptación proporcionada por el módulo de clave de encriptación incluida en el módulo de encriptación, y la clave de encriptación proporcionada por el módulo de clave de encriptación puede que no tenga fugas en el modo de encriptación, y una clave de encriptación adicional para ejecutar el al algoritmo de encriptación puede que no fluya en el módulo de encriptación.

El módulo de clave de encriptación puede incluir un módulo de memoria no volátil para almacenar una clave de encriptación generada previamente.

El módulo de clave de encriptación puede incluir un módulo diferente de una memoria para generar y proporcionar la clave de encriptación.

En este caso, puede determinarse si los nodos en el módulo de clave de encriptación son cortocircuitados de forma probabilística mediante una violación de forma intencional de una regla de diseño prevista en un proceso de fabricación de un semiconductor, y el módulo de clave de encriptación puede generar y proporcionar la clave de encriptación basándose en un resultado de lectura si los nodos son cortocircuitados.

En este caso, los nodos en el módulo de clave de encriptación pueden ser capas conductoras de un semiconductor, la regla de diseño puede estar asociada con un tamaño de una vía o un contacto formado entre las capas conductoras del semiconductor, y el módulo de clave de encriptación puede generar y proporcionar la clave de encriptación basándose en si la vía o el contacto cortocircuita las capas conductoras.

La vía o el contacto puede tener un tamaño mediante el cual una diferencia entre una probabilidad de que la vía o el contacto cortocircuite las capas conductoras y la probabilidad de que la vía o el contacto no cortocircuite las capas conductoras está dentro de un rango de error predeterminado por la violación de forma intencionada de la regla de diseño.

El modo de clave de encriptación puede incluir N estructuras unitarias, cada una de las cuales genera un valor digital de 1 bit utilizando un único par de capas conductoras y una vía o contacto únicos que conectan las capas conductoras, y generar un valor digital de N bits generado a través de N estructuras unitarias como la clave de encriptación. En este caso, N se refiere a un número natural.

En este caso, el módulo de clave de encriptación puede generar un valor digital de N/k bits como clave de encriptación, dividiendo el valor digital de N bits generado en k unidades, comparando un primer grupo con un segundo grupo, entre la pluralidad de grupos, determinando valores que representan el primer grupo y el segundo grupo para ser “1” cuando un valor que incluye k bits digitales incluidos en el primer grupo es mayor que un valor que incluye k bits digitales incluidos en el segundo grupo, y determinar los valores digitales que representan el primer grupo y el segundo grupo para ser “0” cuando el valor que incluye k vis digitales incluidos del primer grupo es menor que o igual al valor que incluye k bits digitales incluidos en el segundo grupo. En este caso, k se refiere a un número natural.

Los nodos en el módulo de clave de encriptación pueden ser capas conductoras de un semiconductor, y la regla de diseño puede estar asociada con un espacio entre las capas conductoras del semiconductor, y el módulo de clave de encriptación puede generar y proporcionar la clave de encriptación basándose en si las capas conductoras del semiconductor son cortocircuitadas.

El módulo de clave de encriptación puede incluir N celdas unitarias, cada una para emitir un valor digital de 1 bit, cada una de las N celdas unitarias puede generar un valor digital de 1 bit basándose en la variación del proceso de fabricación del semiconductor y el módulo de clave de encriptación puede generar y proporcionar una clave de encriptación de N bits. En este caso, N se refiere a un número natural.

En este caso, una primera celda unitaria entre las N celdas unitarias puede incluir un primer inversor que tiene un primer umbral lógico, y un segundo inversor que tiene un segundo umbral lógico. El primer inversor y el segundo

inversor pueden formar una estructura de realimentación en la cual un terminal de entrada del primer inversor y un terminal de salida del segundo inversor son conectados a un primer nodo, y un terminal de salida del primer inversor y un terminal de entrada del segundo inversor son conectados a un segundo nodo. El primer umbral lógico puede ser diferente del segundo umbral lógico basándose en la variación del proceso de fabricación del semiconductor y un valor digital de 1 bit correspondiente a la primera celda unitaria puede determinarse basándose en un nivel lógico del primer nodo y un nivel lógico del segundo nodo.

El módulo de clave de encriptación puede incluir N amplificadores diferenciales. Cuando dos terminales de entrada de un amplificador diferencial, entre los N amplificadores diferenciales, son cortocircuitados, los niveles lógicos de dos terminales de salida del primer amplificador diferencial pueden diferir entre si basándose en la variación del proceso de fabricación de semiconductor, y un valor digital de 1 bit correspondiente al primer amplificador diferencial puede determinarse basándose en los niveles lógicos de los dos terminales de salida, y el módulo de clave de encriptación puede generar y proporcionar una clave de encriptación de N bits. En este caso, N se refiere a un número natural.

De acuerdo con otro aspecto de la presente divulgación, se proporciona un método de encriptación que incluye recibir unos datos de entrada que se van a encriptar en un módulo de encriptación que incluye un módulo de clave de encriptación para proporcionar una clave de encriptación, y encriptar los datos ejecutando un algoritmo de encriptación utilizando la clave de encriptación proporcionada por el módulo de clave de encriptación.

De acuerdo con otro aspecto más de la presente divulgación, se proporciona un chip de circuito integrado (CI) para ejecutar un algoritmo de encriptación que utiliza una clave de encriptación recibiendo datos que se van a encriptar, el chip de CI que incluye un módulo de encriptación, que incluye un módulo de clave de encriptación para proporcionar una clave de encriptación, para ejecutar un algoritmo de encriptación utilizando la clave de encriptación proporcionada por el módulo de clave de encriptación.

En este caso, el chip de CI puede estar dispuesto en una tarjeta inteligente para ejecutar el algoritmo encriptación en aplicaciones de la tarjeta inteligente.

Efectos ventajosos

Un aspecto de la presente divulgación proporciona un dispositivo y un método que puede ser seguro para un ataque físico, por ejemplo, un sondeo de bus, o un ataque sobre una memoria no volátil, dado que no se puede generar una clave fuera de un módulo de encriptación, y no se puede almacenar en una memoria o trasmitirse a través de un bus, y similares.

Otro aspecto de la presente divulgación proporciona un dispositivo y un método que pueden ser seguros para un ataque físico para extraer contenidos en una memoria, dado que se pueden disponer módulos de clave de encriptación para ser dispersados de forma aleatoria en un módulo, similar a otras celdas estándar, y por tanto, los módulos de clave de encriptación pueden ser difíciles de encontrar directamente.

Otro aspecto más de la presente divulgación proporciona un dispositivo y un método que puede lograr mejoras en términos de un espacio y una cantidad de energía que se va utilizar, dado que puede que no sea necesaria una memoria no volátil separada para almacenar una clave de encriptación.

Breve descripción de los dibujos

La figura 1 ilustra un dispositivo de encriptación de acuerdo con un modo de realización de la invención.

La figura 2 ilustra un modo de encriptación de acuerdo con un modo de realización de la presente invención.

La figura 3 es un diagrama de bloques que ilustra una configuración de ejemplo de un modo de encriptación de acuerdo con un modo de realización de la presente invención.

La figura 4 es un diagrama de circuito de ejemplo que ilustra un concepto de una celda unitaria que constituye un módulo de clave de encriptación de una forma de una función físicamente no clonable (PUF) para generar una clave de encriptación que utiliza una variación del proceso de acuerdo con un modo de realización de la presente invención.

La figura 5 es un gráfico de referencia para la comprensión del modo de realización de la figura 4.

La figura 6 es un diagrama de bloques que ilustra una implementación de ejemplo de un módulo de clave de encriptación de acuerdo con un modo de realización de la presente invención.

La figura 7 ilustra una celda unitaria de un módulo de claves de encriptación para generar un valor digital utilizando una variación de un proceso de un amplificador diferencial de acuerdo con un modo de realización de la presente invención.

La figura 8 ilustra un diagrama de circuito de ejemplo en el cual se implementa un módulo de clave de encriptación de acuerdo con un modo de realización de la presente invención.

La figura 9 es un diagrama conceptual que ilustra un principio de generación de un modo de clave de encriptación violando de forma intencional una regla de diseño de semiconductor de acuerdo con un modo de realización de la presente invención.

La figura 10 es un gráfico que ilustra una configuración de un módulo de clave de encriptación implementado violando intencionalmente una regla de diseño de semiconductor de acuerdo con un modo de realización de la presente invención.

La figura 11 es un diagrama conceptual que ilustra un proceso de generación de un módulo de clave de encriptación ajustando un espacio entre las capas conductoras de acuerdo con un modo de realización de la presente invención.

La figura 12 es un diagrama conceptual que ilustra una estructura de ejemplo de una matriz de vías o contactos formada en una capa de semiconductor para implementar un módulo de clave de encriptación de acuerdo con un modo de realización de la presente invención.

La figura 13 es un diagrama conceptual que ilustra un proceso de pos-procesamiento de valor digital generado en el modo de realización de la figura 12, para equilibrado de “0” y “1”, en lugar de utilizar el valor digital original como una clave de encriptación, de acuerdo con un modo de realización de la presente invención.

Mejor modo de llevar a cabo la invención.

Se hará ahora referencia en detalle a modos de realización de la presente invención, cuyos ejemplos son ilustrados en los dibujos que acompañan. Sin embargo, la presente invención no está limitada a los modos de realización descritos. En los dibujos, referencias numéricas similares se refieren a elementos similares a lo largo de toda la memoria.

La figura 1 ilustra un dispositivo 100 de encriptación de acuerdo con un modo de realización de la presente invención.

Como un ejemplo, el dispositivo 100 de encriptación puede ser incluido en un chip de circuito integrado (CI) de una tarjeta inteligente. El dispositivo 100 de encriptación puede incluir una memoria 120 de sólo lectura programable y borrable eléctricamente (EEPROM) para almacenar datos, una unidad 130 de procesamiento central (CPU), y de forma opcional, una memoria 140 de acceso aleatorio síncrona y dinámica (SDRAM). El dispositivo 100 de encriptación puede comunicarse con un entorno externo a través de una interfaz 101 de entrada/salida (I/O).

El dispositivo 100 de encriptación puede incluir un módulo 110 de encriptación, por ejemplo, un coprocesador criptográfico para encriptación.

De aquí en adelante, a menos que se mencione de otro modo, dependiendo de una aplicación del dispositivo 100 de encriptación incluida en una tarjeta inteligente o en un chip de CI de una tarjeta inteligente, al menos una porción de la SDRAM 140 opcional, la CPU 130, y la EEPROM 120 se pueden omitir, y se pueden realizar varios cambios y aplicaciones sin alejarse del alcance de las reivindicaciones.

Adicionalmente, de aquí en adelante, a menos que se mencione de otro modo, la interfaz 101 I/O puede ser una ruta de entrada y salida de entrada o salida de datos del dispositivo 100 de encriptación, independientemente de esquemas, por ejemplo, un esquema de tipo de contacto y/o un esquema sin contacto.

El módulo 110 de encriptación del dispositivo 100 de encriptación puede utilizar una clave de encriptación en un proceso de ejecución de un algoritmo de encriptación. La clave de encriptación puede incluir una clave pública, una clave secreta, y similares.

En un esquema convencional, una clave de encriptación para ejecutar un algoritmo de encriptación se puede almacenar fuera del módulo 110 de encriptación en forma de un valor digital, y el módulo 110 de encriptación puede recibir la clave de encriptación a través de un bus 102 en un proceso de encriptación y/o desencriptación de datos ejecutando el algoritmo de encriptación.

Sin embargo, dicho esquema es vulnerable a ataques físicos de averiguación de una clave de encriptación y/o un algoritmo de encriptación.

Dichos ataques físicos pueden atacar directamente a una región de una memoria, por ejemplo, la EEPROM 120, y similares, en la cual está presente la clave de encriptación, para extraer la clave de encriptación de la memoria utilizando un método, por ejemplo, sondeo, o un escaneado de la memoria. Adicionalmente, una ubicación del bus 102 en el chip de CI puede verificarse realizando ingeniería inversa. Por consiguiente, la clave de encriptación puede ser extraída realizando un sondeo de bus utilizando una micro-sonda cuando se ejecuta de forma artificial un comando predeterminado.

De acuerdo con el presente modo de realización, se puede generar una clave de encriptación directamente mediante un módulo 111 de clave de encriptación incluida en el módulo 110 de encriptación, y/o se puede almacenar una clave de encriptación generada previamente en el módulo 111 de clave de encriptación. Dicha clave de encriptación puede estar provista cuando el módulo 110 de encriptación ejecuta un algoritmo de encriptación.

Por consiguiente, la clave de encriptación que se va a utilizar por el módulo 110 de encriptación en el proceso de ejecución del algoritmo de encriptación puede que no se almacene fuera del módulo 110 de encriptación en forma de un valor digital y, puede que no se transfiera a través del bus 102 y por tanto, se pueden evitar ataques físicos en el algoritmo de encriptación del módulo 110 de encriptación.

El módulo 111 de clave de encriptación para generar y/o almacenar una clave de encriptación y para proporcionar la clave de encriptación cuando se ejecuta un algoritmo de encriptación por el módulo 110 de encriptación puede ser incluido físicamente o embebido en el módulo 110 de encriptación. Varios modos de realización de ejemplo de una configuración y un funcionamiento del módulo 110 de encriptación se describirán con referencia a la figura 2 y los dibujos posteriores.

La figura 2 ilustra el módulo 110 de encriptación de acuerdo con un modo de realización de la presente invención.

Tal y como se muestra en la figura 1, el módulo 110 de encriptación puede estar conectado a otros componentes a través del bus 102 en el dispositivo 100 de encriptación.

Con referencia la figura 2, el módulo 110 de encriptación puede incluir al menos un módulo 210, 220, 230, 240 y 250 de clave de encriptación.

Los módulos 210, 220, 230, 240 y 250 de clave de encriptación pueden generar y/o almacenar claves de encriptación para ser utilizadas para ejecutar un algoritmo de encriptación, individualmente o de forma conjunta, y proporcionar las claves de encriptación al módulo 110 de encriptación.

En un modo de realización, se puede incluir un módulo de clave de encriptación único en el módulo 110 de encriptación. En otro modo de realización, se puede incluir una pluralidad de módulos de clave de encriptación en el módulo 110 de excitación, tal y como se muestra en la figura 2.

Adicionalmente, cuando una pluralidad de módulos de clave de encriptación se incluye en el módulo 110 de encriptación, al menos una porción de la pluralidad de módulos 210, 220, 230, 240 y 250 de clave de encriptación puede corresponderse a simuladores que no proporcionan claves de encriptación en la realidad.

Un modo de realización en el cual se implementan módulos 210, 220, 230, 240 y 250 de clave de encriptación puede incluir un caso en el cual los módulos 210, 220, 230, 240 y 250 de clave de encriptación correspondan a dispositivos de memoria, y un caso en el cual los módulos 210, 220, 230, 240 y 250 de clave de encriptación correspondan a dispositivos distintos de una memoria.

Un modo de realización en el cual una porción de los módulos 210, 220, 230, 240 y 250 de clave de encriptación correspondan a dispositivos de memoria y otra porción de los módulos 210, 220, 230, 240 y 250 de clave de encriptación correspondan a dispositivos distintos de una memoria también puede ser posible. La presente invención no está constituida para estar limitada por una porción de los modos de realización.

Como un ejemplo, en el modo de realización en el cual los módulos 210, 220, 230, 240 y 250 de clave de encriptación incluyen dispositivos de memoria, se pueden almacenar simplemente claves de encriptación generadas previamente de una forma de un valor digital en los módulos 210, 220, 230, 240 y 250 de clave de encriptación correspondientes a los dispositivos de memoria, y se puede leer para el uso, cuando sea necesario, en un proceso de ejecución de un algoritmo de encriptación mediante el módulo 110 de encriptación.

En el otro modo de realización, cuando los módulos 210, 220, 230, 240 y 250 de clave de encriptación incluyen dispositivos distintos a una memoria, al menos una porción de los módulos 210, 220, 230, 240 y 250 de clave de encriptación puede incrementarse mediante funciones físicamente no clonables (PFU).

En el modo de realización en el cual los módulos 210, 220, 230, 240 y 250 de clave de encriptación incluyen dispositivos distintos de una memoria tales como PUF, hay varios modos de realización para implementar los PUF. Como un ejemplo, el PUF puede implementarse violando de forma intencionada una regla de diseño en un proceso de fabricación de un semiconductor, o utilizando una variación del proceso de fabricación de un semiconductor.

Dichos modos de realización serán descritos en detalle con referencia las figuras 4 a 13.

La figura 3 es un diagrama de bloques que ilustra una configuración de ejemplo del módulo 110 de encriptación de acuerdo con un modo de realización de la presente invención.

Cuando los datos que se van a encriptar son introducidos en una unidad 310 de entrada de datos a través del bus 102, y similares, se puede iniciar la ejecución del algoritmo de encriptación.

Tal y como se describe con referencia la figura 2, un módulo 320 de clave de encriptación único o una pluralidad de módulos 320 de clave de encriptación se pueden incluir físicamente en el módulo 110 de encriptación.

Como un ejemplo, cuando un módulo 01 321 de clave de encriptación hasta un módulo N 322 de clave de encriptación están presentes, un selector 330 de módulo de clave de encriptación puede seleccionar un módulo de clave de

encriptación para proporcionar una clave de encriptación que se va utilizar para un algoritmo de realización en la realidad. En este caso, N se refiere a un número natural.

Dicha selección puede corresponderse a una información de índice de un módulo de claves de encriptación que se va seleccionar en la realidad, entre indicios que identifican los módulos 320 de clave de encriptación o puede determinarse cableando, en un proceso de diseño y fabricación, los módulos 320 de clave de encriptación junto con el módulo 110 de encriptación.

Cuando una clave de encriptación está provista a lo largo del proceso, una unidad 340 de encriptación puede ejecutar un algoritmo de encriptación que utiliza la clave de encriptación para encriptar los datos de entrada, y los datos encriptado se pueden transferir a otros componentes a través de una unidad 350 de salida de datos a través del bus 102.

Aunque solo los procesos de datos de encriptación han sido descritos, un proceso de desencriptación que utiliza un algoritmo de encriptación puede ser similar. Los modos de realización de la presente invención deberían no considerarse como que se limitan a una de la encriptación y desencriptación.

Dado que la clave de encriptación es gestionada dentro del módulo 110 de encriptación de forma autónoma, la clave de encriptación puede que no se transfiera a un entorno externo del módulo 110 de encriptación o al módulo 110 de encriptación desde un entorno externo. Por consiguiente, una probabilidad de éxito de ataques físicos puede descender de forma remarcable. En particular, una probabilidad de éxito de un ataque físico de sondeo del bus 102 puede ser extremadamente baja.

Un caso en el que las claves de encriptación se corresponden a dispositivos de memoria sido descrito con referencia las figuras 1 y 2. De aquí en adelante, modos de realización en los cuales los módulos de clave de encriptación se implementen utilizando PUF correspondientes a dispositivos distintos de la memoria se describirán con referencia las figuras 4 a 13.

Para referencia, un PUF mencionado en el presente documento puede generar una clave de encriptación físicamente no clonable e inalterable una vez que se ha fabricado, al menos en teoría.

De aquí en adelante, se describirán varios modos de realización en los cuales los módulos de clave de encriptación son implementados por PUF correspondientes a dispositivos distintos de una memoria. Las figuras 4 a 8 pueden corresponderse a ejemplos en los cuales los módulos de clave de encriptación para generar claves de encriptación son implementados utilizando una variación del proceso de semiconductor.

Las figuras 9 a 13 se corresponderán a ejemplos en los cuales los módulos de clave de encriptación para generar claves de encriptación se implementan violando de forma intencionada una regla de diseño para diseñar un circuito.

La figura 4 es un diagrama de circuito de ejemplo que ilustra un concepto de una celda unitaria que constituye un módulo de clave de encriptación de una forma de un PUF para generar una clave de encriptación utilizando una variación de proceso de acuerdo con un modo de realización de la presente invención.

En la figura 4, se muestra un primer inversor 410 y un segundo inversor 420.

Una variación de proceso de semiconductor se puede provocar mediante varias razones. Por ejemplo, cuando se fabrica un transistor, una variación de proceso se puede provocar mediante un parámetro, por ejemplo, una tensión umbral, un índice asociado con un espesor de óxido, un índice asociado con una concentración de dopado, una longitud de puerta válida, o similares.

En general, un proceso de fabricación de semiconductor con una variación del proceso mínima puede contemplarse como excelente. Sin embargo, debido a una característica física, la variación del proceso puede ser reducible, pero no eliminable de forma completa.

En el presente modo de realización, el primer inversor 410 puede tener un primer umbral lógico, y el segundo inversor 420 puede tener un segundo umbral lógico. Un umbral lógico se refiere a un valor de una tensión cuando una tensión de entrada de un inversor es idéntica a una tensión de salida del inversor. Una descripción adicional detallada se proporcionará con referencia a la figura 5.

Un umbral lógico de un dispositivo inversor puede medirse utilizando un valor de una tensión cuando un terminal de salida y un terminal de entrada de un inversor se hacen funcionar o se cortocircuitan.

Los inversores fabricados mediante un proceso idéntico pueden diseñarse para tener un umbral lógico idéntico en teoría. Sin embargo, tal y como se describió anteriormente, debido a una variación de proceso en un proceso de fabricación en la realidad, cualquiera de los inversores puede que no tenga un umbral lógico perfectamente idéntico en la realidad.

De acuerdo con el presente modo de realización, el primer inversor 410 y el segundo inversor 420 pueden ser fabricados mediante un proceso idéntico, y puede que tengan una diferencia entre umbrales lógicos resultantes de una variación del proceso.

La diferencia entre los umbrales lógicos puede variar dependiendo de un proceso, sin embargo, por ejemplo, correspondiente al tamaño de aproximadamente unas pocas decenas de milivoltios. Por consiguiente, el umbral lógico del primer inversor 410 y el umbral lógico del segundo inversor 420 medidos utilizando un circuito comparador separado pueden ser imprecisos debido a un error en la medida.

Por consiguiente, hay una demanda de un método de comparación de umbrales lógicos de dos inversores relativamente, en particular, un método de medida de umbrales lógicos de dos inversores sin un circuito comparador separado. En un modo de realización de la presente invención, se puede determinar un umbral lógico mayor comparando los umbrales lógicos de dos inversores relativamente (de forma autónoma sin el uso de un circuito comparador separado).

En el caso en el que el segundo inversor 420 esté ausente, la tensión de salida del primer inversor 410 puede ser idéntica a un umbral lógico del primer inversor 410 cuando un terminal de entrada y un terminal de salida del primer inversor 410 son cortocircuitados.

Adicionalmente en un caso en el que el primer inversor 410 esté ausente, la tensión de salida del segundo inversor 420 puede ser idéntica a un umbral lógico del segundo inversor 420 cuando un terminal de entrada y un terminal de salida del segundo inversor 420 son cortocircuitados.

Sin embargo, tal y como se muestra en la figura 4, cuando el terminal de entrada del primer inversor 410 y el terminal de salida del segundo inversor 420 son cortocircuitados para ser conectados a un primer nodo, y el terminal de salida del primer inversor 410 y el terminal de entrada del segundo inversor 420 son cortocircuitados para ser conectados a un segundo nodo, se pueden obtener diferentes resultados.

Cuando el primer nodo y el segundo nodo son cortocircuitados utilizando un interruptor 430, los valores de las tensiones de los dos nodos cortocircuitados pueden ser valores entre el umbral lógico del primer inversor 410 y el umbral lógico del segundo inversor 420 (puede que no sea un valor promedio, de aquí en adelante, aplicará lo mismo).

Independientemente de un valor más grande de los umbrales lógicos de los dos inversores, un valor de una tensión de salida puede ser un valor entre los umbrales lógicos de los dos inversores mientras el interruptor 430 está cerrado.

Cuando el interruptor 430 está abierto para abrir el primer nodo y el segundo nodo, el nivel lógico de un valor de una tensión de uno de, el primer nodo y el segundo nodo, puede ser “0” y el nivel lógico de un valor de una tensión del otro puede ser “1”.

Por ejemplo, cuando el umbral de lógica del primer inversor 410 es menor que el umbral de lógica del segundo inversor 420, una tensión del primer nodo puede ser más alta que la del umbral lógico del primer inversor 410 mientras que el interruptor 430 está cerrado de manera que el primer nodo (un nodo opuesto a un nodo de salida) y el segundo nodo (el nodo de salida) son cortocircuitados.

Por consiguiente, cuando el interruptor 430 es reorientado de tal manera que el primer nodo y el segundo nodo son abiertos, el primer inversor 410 puede reconocer una tensión del primer nodo (correspondiente al terminal de entrada del primer inversor 410) como un nivel lógico alto, y hacer que una tensión del segundo modo correspondiente al terminal de salida del primer inversor 410 sea un nivel lógico bajo.

En este caso, el segundo inversor 420 puede reconocer una tensión del segundo nodo (correspondiente al terminal de entrada del segundo inversor (420) como un nivel lógico bajo, y hacer una tensión del primer nodo correspondiente al terminal de salida del segundo inversor 420 un nivel lógico alto.

Por consiguiente, el nivel lógico de la tensión del segundo terminal correspondiente al terminal de salida (“salida”) de la figura 4 puede ser alto.

Por el contrario, cuando el umbral lógico del primer inversor 410 es más alto que el umbral lógico del segundo inversor 420, una tensión del primer nodo, mientras el interruptor 430 está cerrado de manera que el primer nodo y el segundo nodo son cortocircuitados, puede ser inferior que el umbral lógico del primer inversor 410.

Por consiguiente, cuando el interruptor 430 se vuelve a abrir de manera que el primer nodo y el segundo nodo están abiertos, el primer inversor 410 puede reconocer una tensión del primer nodo (correspondiente al terminal de entrada del primer inversor 410) como un nivel lógico bajo, y hacer que una tensión del segundo nodo correspondiente al terminal de salida del primer inversor 410 sea un nivel lógico alto

En este caso, el segundo inversor 420 puede reconocer una tensión del segundo nodo (correspondiente al terminal de entrada del segundo inversor 420) como un nivel lógico alto, y hacer que una tensión del primer modo correspondiente al terminal de salida del segundo inversor 420 sea un nivel lógico bajo.

Por consiguiente, el nivel lógico de la tensión del segundo terminal correspondiente al terminal de salida (“salida”) de la figura 4 puede ser bajo.

Tal y como se describió anteriormente, dependiendo de un valor más alto del umbral lógico del primer inversor 410 y del umbral lógico del segundo inversor 420, el nivel lógico del terminal de salida (“salida”) después de que el interruptor 430 sea cortocircuitado-abierto puede ser alto (o “1”) o bajo (o “0”).

Un valor más grande de umbrales lógicos del primer inversor 410 y el segundo inversor 420 fabricados mediante un proceso de fabricación idéntico pueden ser determinados de forma aleatoria. De forma probabilística, una probabilidad de que uno de los dos inversores tenga un umbral lógico más alto que un umbral lógico del otro puede ser de aproximadamente un 50%.

Adicionalmente, una vez que se ha fabricado, un cambio del valor más grande puede ser difícil.

A través del modo de realización de la figura 4, se puede generar un valor digital de 1 bit (un valor que tiene una probabilidad idéntica de ser “1” o de ser “0”, sin embargo, difícil de cambiar una vez que se ha fabricado).

El proceso descrito anteriormente puede entenderse de forma más clara a través del gráfico de la figura 5.

La figura 5 es un gráfico de referencia para la comprensión del modo de realización de la figura 4.

El gráfico de referencia de ejemplo ilustra una característica de tensión para un caso en el cual el umbral lógico del primer inversor 410 es inferior que el umbral lógico del segundo inversor 420 de la figura 4.

Una curva 510 indica una característica de tensión del primer inversor 410, y una curva 520 indica una característica de tensión del segundo inversor 420. Cuando el primer inversor 410 y el segundo inversor 420 son fabricados mediante un proceso de fabricación idéntico de acuerdo con un modo de realización de la presente invención, la curva 510 y la curva 520 pueden ser casi idénticas, sin embargo, tienen una diferencia modesta debido a una variación del proceso.

Cuando se encuentra un punto de intersección de la curva 510 y una línea 530 recta con un gradiente de “1”, puede ser determinado el umbral V_1 lógico del primer inversor 410. Adicionalmente, cuando se encuentra un punto de intersección de la curva 520 y la línea 530 recta, puede ser determinado el umbral V_2 lógico del segundo inversor 420.

En el presente modo de realización, V_1 es menor que V_2. Por consiguiente, cuando el interruptor 430 de la figura 4 está cerrado tal que el primer nodo y el segundo nodo están cortocircuitados (también referido como “reinicio”, las tensiones $V_{REINICIO}$ del primer nodo y el segundo nodo pueden corresponderse con los valores entre V_1 y V_2.

Cuando el interruptor 430 se vuelve abrir de manera que el primer nodo y el segundo nodo están abiertos, el primer inversor 410 puede reconocer la tensión $V_{REINICIO}$ del primer nodo como un nivel lógico alto, y puede hacer que la tensión del segundo nodo correspondiente al terminal de salida del primer inversor 410 sea un nivel lógico bajo.

En este caso, el segundo inversor 420 puede reconocer la tensión $V_{REINICIO}$ del segundo nodo como un nivel lógico bajo, y puede hacer que la tensión del primer nodo correspondiente al terminal de salida del segundo inversor 420 sea un nivel lógico alto.

Por consiguiente, el nivel lógico de la tensión del segundo terminal correspondiente al terminal de salida (“salida”) de la figura 4 puede ser alto.

En un caso en el que la celda unitaria ilustrada en la figura 4 genere un valor digital de 1 bit, se puede generar una clave de encriptación utilizando un valor digital de N bits integrando N celdas unitarias.

De acuerdo con un modo de realización de la presente invención, los módulos 320 de clave de encriptación se pueden implementar utilizando dicho esquema.

Un módulo de clave de encriptación para generar una clave de encriptación de una forma de un valor digital basándose en una diferencia entre umbrales lógicos de dispositivos inversores utilizando una variación del proceso de semiconductor se puede implementar mediante una configuración de la figura 6.

La figura 6 es un diagrama de bloques que ilustra una implementación de ejemplo de un módulo 600 de clave de encriptación de acuerdo con un modo de realización de la presente invención.

Con referencia la figura 6, el módulo 600 de clave de encriptación puede incluir cinco inversores 611 a 615, un selector 620, y un comparador 630.

El selector 620 puede seleccionar dos inversores de cinco inversores de la figura 6. Por ejemplo, se puede seleccionar el inversor 612 y el inversor 613.

En este ejemplo, el comparador 630 puede comparar un umbral lógico del inversor 612 con un umbral lógico del inversor 613, y proporcionar una tensión de salida a un terminal de salida basándose en un resultado de la

comparación. Un valor digital de 1 bit puede ser generado basándose en un nivel lógico de la tensión de salida del terminal de salida.

Cuando el selector 620 selecciona otros dos inversores, el comparador 630 puede generar un valor digital de 1 bit de nuevo.

Tal y como se describió anteriormente, cuando el selector 620 selecciona dos inversores de los cinco inversores 611 a 615, y el comparador 630 genera un valor digital comparando los umbrales lógicos de los dos inversores seleccionados, se puede obtener un valor digital de un máximo de 10 bits.

Aunque se incluyen cinco inversores en el presente modo de realización, la presente invención no está limitada a ello. Se pueden realizar varios cambios a la vista de un área del circuito, un número de bits en un valor digital que se va a generar, y similares.

En el presente modo de realización, considerando que el área del comparador 630 que se va a integrar en un chip de semiconductores considerablemente grande, cuando se compara con un área de los inversores 611 a 615, una pluralidad de inversores y un único comparador 630 se conectan a través del selector 620. Sin embargo, en otras aplicaciones, un único comparador puede hacer un par con dos inversores para generar un valor digital de N bits.

El módulo de clave de encriptación para generar una clave de encriptación de una forma de un valor digital basándose en una diferencia entre umbrales lógicos de dispositivos inversores utilizando una variación de proceso de semiconductor puede también implementarse mediante una configuración de la figura 7.

La figura 7 ilustra una celda 700 unitaria de un módulo de clave de encriptación para generar un valor digital utilizando una variación de proceso de un amplificador diferencial de acuerdo con un modo de realización de la presente invención.

La celda 700 unitaria puede corresponderse a un circuito de un amplificador diferencial. La celda unitaria correspondiente al circuito del amplificador diferencial que incluye al menos un dispositivo de un transistor y una resistencia puede amplificar una diferencia entre una tensión de un primer terminal 711 de entrada y una tensión de un segundo terminal 712 de entrada, y proporcionar la diferencia amplificada como una diferencia entre una tensión de un primer terminal 721 de salida y una tensión de un segundo terminal 722 de salida.

Por consiguiente, cuando el primer terminal 711 de entrada y el segundo terminal 712 de entrada son cortocircuitados, un valor de una tensión de salida correspondiente a la diferencia de la tensión del primer terminal 721 y la tensión del segundo terminal 722 puede ser “0” en teoría.

Sin embargo, debido a una diferencia en las características eléctricas entre dispositivos resultantes de una variación de proceso de semiconductor, la tensión del primer terminal 721 de salida puede que no sea completamente idéntica a la tensión del segundo terminal 722 de salida.

Por consiguiente, comparando las tensiones de dos terminales de salida para verificar una tensión más alta utilizando un método similar al método de comparar los umbrales lógicos de los inversores del modo de realización de la figura 6, se puede generar un valor digital de 1 bit.

Por ejemplo, en el caso en el que el primer terminal 711 de entrada y el segundo terminal 712 de entrada se han cortocircuitados, cuando un valor de la tensión del primer terminal 721 de salida es más alto que el valor de la tensión del segundo terminal 722 de salida, se puede reconocer un valor digital de “1”. Por el contrario, cuando el valor de la tensión del primer terminal 721 de salida es menor que el valor de tensión del segundo terminal 722 de salida, se puede reconocer un valor digital de “0”.

Por consiguiente, cuando se integran N celdas unitarias, cada una de las N celdas unitarias que puede corresponderse con el amplificador 700 diferencial, se puede proporcionar una clave de encriptación en forma de un valor digital de N bits, y se puede implementar un módulo de clave de encriptación de acuerdo con un modo de realización de la presente invención. Dicha implementación es ilustrada en la figura 8.

La figura 8 ilustra un diagrama de circuito de ejemplo en el cual se implementa un módulo 800 de clave de encriptación de acuerdo con un modo de realización de la presente invención.

Con referencia a la figura 8, el módulo 800 de clave de encriptación puede incluir seis amplificadores 811 a 816 diferenciales, un selector 820 para seleccionar uno de los seis amplificadores diferenciales, y un comparador 830 para comparar dos tensiones de salida de los amplificadores diferenciales seleccionados por el selector 820 para generar un valor digital de 1 bit.

En este ejemplo, todos los terminales de entrada de los seis amplificadores 811 a 816 diferenciales pueden ser cortocircuitados y pueden tener una tensión idéntica.

De acuerdo con un modo de realización de la presente invención, el selector 820 puede incluir un dispositivo multiplexor (MUX) 6:1. Sin embargo, el presente modo de realización puede ser un ejemplo para la implementación de la presente invención, y la presente invención no está limitada a un modo de realización específico.

Por consiguiente, se pueden cambiar varios puertos de entrada/salida del dispositivo MUX. Adicionalmente, el selector 820 puede incluir otro dispositivo, diferente del dispositivo MUX. El dispositivo MUX 6:1 puede emitir, a dos terminales de salida, tensiones de salida de los seis amplificadores diferenciales a través de doce terminales de entrada. Los dos terminales de entrada pueden estar conectados a dos terminales de entrada del comparador 830.

En el presente modo de realización, el módulo 800 de clave de encriptación puede generar una clave de encriptación correspondiente a un valor digital de 6 bits.

Los modos de realización en los cuales los módulos de clave de encriptación son implementados utilizando una variación de proceso de implementación han sido descritos con referencia las figuras 4 a 8.

De aquí en adelante, los modos de realización en los cuales los módulos de clave de encriptación son implementados violando de forma intencional una regla de diseño de semiconductor serán descritos con referencia a las figuras 9 a 13.

La figura 9 es un diagrama conceptual que ilustra un principio de generación de un modo de clave de encriptación violando de forma intencional una regla de diseño de semiconductor de acuerdo con un modo de realización de la presente invención.

En general, se puede diseñar un contacto o una vía para conectar capas conductoras, y puede determinarse un tamaño del contacto o de la vía para que las capas conductoras sean cortocircuitadas. En una regla de diseño general, se puede determinar un tamaño mínimo de un contacto o de una vía para garantizar que las capas conductoras sean cortocircuitadas.

Sin embargo, en una implementación de módulos de clave de encriptación de acuerdo con un modo de realización de la presente invención, reduciendo de forma intencional un tamaño de un contacto o una vía para ser más pequeño que un tamaño determinado en la regla de diseño, una porción de los contactos o vías pueden cortocircuitar capas conductoras, y otra porción de los contactos o las vías pueden no cortocircuitar las capas conductoras. Se puede determinar de forma probabilística si los contactos o las vías cortocircuitan las capas conductoras.

En un proceso de semiconductor convencional, cuando un contacto o una vía no es capaz de cortocircuitar las capas conductoras, el proceso puede ser considerado como que ha fallado. Sin embargo, en la presente invención, dicho fallo se puede utilizar para generar una clave de encriptación que tenga aleatoriedad.

Con referencia la figura 9, se pueden formar vías entre una primera capa 902 metálica y una segunda capa 901 metálica en un proceso de fabricación de semiconductor.

En un grupo 910 en el cual los tamaños de las vías son suficientemente grandes de acuerdo con una regla de diseño, toda las vías cortocircuitan la primera capa 902 metálica y la segunda capa 901 metálica, y si las vías cortocircuiten la primera capa 902 metálica y la segunda capa 901 metálica se puede expresar mediante un valor digital de “0”.

En un grupo 930 en el cual los tamaños de las vías son demasiado pequeños, todas las vías no cortocircuitan la primera capa 902 metálica y la segunda capa 901 metálica. Por consiguiente, si las vías cortocircuitan la primera capa 902 metálica y la segunda capa 901 metálica se puede expresar mediante un valor digital de “1”.

En un grupo 920 en el cual los tamaños de las vías están entre los tamaños de las vías del grupo 910 y los tamaños de las vías del grupo 930, una porción de las vías cortocircuita la primera capa 902 metálica y la segunda capa 901 metálica y otra porción de las vías no cortocircuita la primera capa 902 metálica y la segunda capa 901 metálica.

De acuerdo con un modo de realización de la presente invención, con el fin de implementar un módulo de clave de encriptación, los tamaños de las vías pueden establecerse para una porción de las vías para cortocircuitar la primera capa 902 metálica y la segunda capa 901 metálica, y otra porción de las vías para no cortocircuitar la primera capa 902 metálica y la segunda capa 901 metálica, tal y como se muestra en el grupo 920.

Una regla de diseño asociada con un tamaño de una vía puede variar dependiendo de un proceso de fabricación de semiconductor. Por ejemplo, si un tamaño de una vía que cumple con una regla de diseños se establece a 0,25 micrómetros (μm) en un proceso de fabricación de un semiconductor de óxido-metal complementario (CMOS) de 0,18 μm, en una implementación de un módulo de clave de encriptación de acuerdo con el modo de realización de la presente invención, la regla de diseño puede violarse de forma intencionada para establecer el tamaño de la vía a 0,19 μm, por lo que se puede distribuir de forma probabilística si la vía cortocircuita las capas metálicas.

La distribución de la probabilidad con referencia a si la vía cortocircuita las capas metálicas puede establecerse para tener una probabilidad de cortocircuito de un 50%, para una eficiencia óptima. En la implementación de los módulos de clave de encriptación de acuerdo con un modo de realización de la presente invención, el tamaño de la vía puede

establecerse para la distribución de la probabilidad para estar cercana a un 50% del máximo. En el establecimiento del tamaño de la vía, el tamaño de la vía puede determinarse mediante un experimento de acuerdo con un proceso.

La figura 10 es un gráfico que ilustra una configuración de un módulo de clave de encriptación implementado violando de forma intencional una regla de diseño de semiconductor de acuerdo con un modo de realización de la invención.

En el gráfico, a medida que aumenta el tamaño de la vía, una probabilidad de que las capas metálicas sean cortocircuitadas se hace más próxima a “1”. Sd se refiere a un tamaño de la vía de acuerdo con la regla de diseño, y puede corresponderse a un valor que garantice de forma suficiente que las capas metálicas son cortocircuitadas.

Sm se refiere a un tamaño de una vía con el cual una probabilidad de que las capas metálicas sean cortocircuitadas puede corresponder a “0,5”, en teoría. Tal y como se describió anteriormente, el valor puede cambiarse dependiendo de un proceso, y un valor lo más similar se puede encontrar mediante un experimento. Sin embargo, un valor preciso de Sm puede ser difícil de encontrar.

Por consiguiente, en una implementación de módulos de clave de encriptación de acuerdo con un modo de realización de la presente invención, si las capas metálicas son cortocircuitadas puede establecerse dentro de un rango entre Sx1 y Sx2 (aunque no se muestran de forma separada, refiriéndose a una región que tiene un margen predeterminado basado en Sx) que tiene una tolerancia predeterminada basada en 0,5, mediante un experimento detallado.

Los modos de realización en los cuales el modo de clave de encriptación se implemente mediante una violación de forma intencionada de una regla de diseño asociada con un tamaño de una vía han sido descritos con referencia a las figuras 9 y 10. De acuerdo con otros modos de realización de la presente invención, los módulos de clave de encriptación se pueden implementar violando de forma intencionada una regla de diseño asociada con un espacio entre las capas conductoras.

La figura 11 es un diagrama conceptual que ilustra un proceso de generación de un módulo de clave de encriptación mediante el ajuste de un espacio entre las capas conductoras de acuerdo con un modo de realización de la presente invención.

Tal y como se describió anteriormente, de acuerdo con el presente modo de realización, ajustando un espacio entre las líneas metálicas, se puede determinar de forma probabilística si las líneas metálicas son cortocircuitadas.

En un grupo 1110 en el cual el espacio entre las líneas metálicas es suficientemente estrecho para garantizar que las líneas metálicas sean cortocircuitadas.

En un grupo 1130 en el cual el espacio entre las líneas metálicas es excesivamente grande, todas las líneas metálicas no son cortocircuitadas.

En el presente modo de realización, con el fin de implementar un módulo de clave de encriptación, se establecen espacios entre líneas metálicas para cortocircuitar las líneas metálicas de forma probabilística, para una porción de las líneas metálicas que se van a cortocircuitar y otra porción para líneas metálicas que no se van a cortocircuitar tal y como se muestra en el grupo 1120.

La figura 12 es un diagrama conceptual que ilustra una estructura de ejemplo de una matriz de vías o contactos formados en una capa semiconductora para implementar un módulo 1200 de clave de encriptación de acuerdo con un modo de realización de la presente invención.

Con referencia la figura 12, M vías en anchura y N vías en longitud, un total de M x N vías, se puede formar entre capas metálicas laminadas o un sustrato de semiconductor. En este caso, M y N se refieren a números naturales.

El módulo 1200 de clave de encriptación puede generar y proporcionar una clave de encriptación de M x N bits, basándose en si cada una de las M x N vías cortocircuita las capas metálicas (un valor digital de “0”) o no cortocircuita las capas metálicas (un valor digital de “1”).

La figura 13 es un diagrama conceptual que ilustra un proceso de pos-procesamiento de un valor digital generado en el modo de realización de la figura 12 para un equilibrio de “0” y “1” más bien que utilizar el valor digital original como clave de encriptación, de acuerdo con un modo de realización de la presente invención.

De acuerdo con el presente modo de realización, un valor digital de M x N bits generado por el módulo 1200 de clave de encriptación se puede dividir basándose en k unidades predeterminadas. En este caso, k se refiere a un número natural.

La división mostrada en la figura 13 puede ser proporcionada como un ejemplo para facilidad de descripción. En una implementación real, puede ser posible un método de división de flip-flops o registros en el módulo 1200 de clave de encriptación y similares.

Por consiguiente, varios cambios y aplicaciones se pueden realizar por los expertos en la técnica al proceso de realizar un equilibrado de “0” y “1” utilizando el método de dividir el valor digital, y dichos cambios y aplicaciones no deberían considerarse como que se alejan del alcance de la presente invención.

En el ejemplo de la figura 13, cuatro valores digitales se pueden clasificar como un grupo único.

El módulo 1200 de clave de encriptación puede comparar un tamaño de un valor digital de 4 bits generado por un grupo 1310 con un tamaño de un valor digital de 4 bits generado por un grupo 1320. Cuando el valor digital de 4 bits del grupo 1310 es mayor que el valor digital de 4 bits del grupo 1320, se pueden determinar los valores digitales que representan el grupo 1310 o el grupo1320 para ser “1”.

De forma inversa, cuando el valor digital de 4 bits del grupo 1310 es menor que el valor digital de 4 bits del grupo 1320, se pueden determinar los valores digitales que representan el grupo 1310 y el grupo 1320 para ser “0”.

En otro modo de realización, los valores digitales que representan grupos pueden determinarse acompañando números de valores digitales de 1 bit de los grupos.

El método de acuerdo con los modos de realización descritos anteriormente de la presente invención se puede grabar en medios legibles por ordenador que incluyen instrucciones de programa para implementar varias operaciones implementadas 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 tales como discos duros, discos flexibles, y cintas magnéticas; medios ópticos tales como discos de CD ROM y DVD; medios magneto-ópticos tales como discos flópticos; y dispositivos de hardware que están especialmente configurados para almacenar y realizar instrucciones de programa, tales como memoria de sólo lectura (ROM), memoria de acceso aleatorio (RAM), memoria flash y similares. Ejemplos de instrucciones de programa incluyen tanto código máquina, tal como el producido mediante un compilador, como archivos que contienen código de alto nivel que puede ser ejecutado mediante un ordenador usando un intérprete. Los dispositivos de hardware descritos pueden estar configurados para actuar como uno o más módulos de software con el fin de realizar las operaciones de los modos de realización de ejemplo descritos anteriormente de la presente invención, o viceversa.

Aunque se han mostrado y descrito unos pocos modos de realización de la presente invención, la presente invención no está limitada a los modos de realización descritos. Más bien, se podría apreciar por los expertos en la técnica que se pueden realizar cambios a esos modos de realización sin alejarse de los principios de la invención, cuyo alcance es definido por las reivindicaciones y sus equivalentes.

REIVINDICACIONES

1. Un circuito integrado para ejecutar el algoritmo de encriptación que utiliza una clave de encriptación recibiendo unos datos de entrada que se van a encriptar, el circuito integrado que comprende:

un módulo (110) de encriptación para ejecutar el algoritmo de encriptación que utiliza una clave de encriptación; y

una pluralidad de módulos (321, 322) de clave de encriptación para proporcionar diferentes claves de encriptación,

en donde el módulo (110) de encriptación comprende:

un selector (330) de módulo de clave de encriptación para seleccionar uno de una pluralidad de módulos (321, 322) de clave de encriptación, y

una unidad (340) de encriptación para ejecutar el algoritmo de encriptación utilizando una clave de encriptación proporcionada por el módulo (321, 322) de clave de encriptación seleccionado,

caracterizado porque el módulo (110) de encriptación además comprende una pluralidad de celdas estándar, en donde la pluralidad de módulos (321, 322) de clave de encriptación está dispuesta en posiciones aleatorias entre disposiciones de la pluralidad de celdas estándar incluidas en el módulo de encriptación, y en donde al menos una porción de la pluralidad de módulos de clave de encriptación son módulos de clave de encriptación de simulación que no proporcionan claves de encriptación.

2. El circuito integrado de la reivindicación 1, en donde el selector (330) de módulo de clave de encriptación está configurado para seleccionar un módulo (321, 322) de clave de encriptación correspondiente a un índice de identificación pre-asignado entre la pluralidad de módulos de clave de encriptación.

3. El circuito integrado de la reivindicación 1, en donde:

el circuito integrado además comprende un bus (102) y está configurado para no transferir la clave de encriptación proporcionada por un módulo (321, 322) de clave de encriptación fuera del módulo (110) de encriptación a través del bus (102).

4. El circuito integrado de la reivindicación 1, en donde un módulo (321, 322) de clave de encriptación comprende un módulo de memoria no volátil para almacenar la clave de encriptación generada previamente.

5. El circuito integrado de la reivindicación 1, en donde el módulo (321, 322) de clave de encriptación comprende un módulo distinto de una memoria para generar y proporcionar la clave de encriptación.

6. El circuito integrado de la reivindicación 5, en donde se determina de forma probabilística si los nodos en el módulo (321, 322) de clave de encriptación son cortocircuitados violando de forma intencionada una regla de diseño proporcionada en un proceso de fabricación de semiconductor, y el módulo de clave de encriptación está configurado para generar y proporcionar la clave de encriptación basada en un resultado de la lectura si los nodos fueron cortocircuitados.

7. El circuito integrado de la reivindicación 6, en donde:

los nodos en el módulo (321, 322) de clave de encriptación comprenden capas (901, 902) conductoras de un semiconductor, y

la regla de diseño está asociada con un tamaño de una vía o un contacto formado entre las capas conductoras del semiconductor y el módulo de clave de encriptación está configurado para generar y proporcionar la clave de encriptación basándose en sí la vía o el contacto cortocircuita las capas conductoras;

opcionalmente en donde la vía o el contacto tiene un tamaño por medio del cual una diferencia entre una probabilidad de que la vía o el contacto cortocircuite las capas conductoras y la probabilidad de que la vía o el contacto no cortocircuite las capas conductoras está dentro de un rango de error predeterminado mediante una violación de forma intencionada de la regla de diseño.

8. El circuito integrado de la reivindicación 6, en donde el módulo (321, 322) de clave de encriptación comprende N estructuras unitarias, cada una de las cuales está configurada para generar un valor digital de 1 bit utilizando un único par de capas conductoras y una única vía o un contacto que conecta las capas conductoras, y configurada para generar un valor digital de N bits generado a través de las N estructuras unitarias como la clave de encriptación,

en donde N se refiere a un número natural;

y opcionalmente en donde el módulo de clave de encriptación está configurado para generar valor digital de N/k bits como clave de encriptación, dividiendo el valor digital de N bits generado en k unidades, comparando un primer grupo con un segundo grupo, entre la pluralidad de grupos, que determina valores digitales que representan el primer grupo y el segundo grupo para ser “1” cuando un valor que comprende k bits digitales incluidos en el primer grupo es mayor

que un valor que comprenden k bits digitales incluidos en el segundo grupo, y que determina los valores digitales que representan el primer grupo y el segundo grupo para ser “0” cuando el valor que comprende k bits digitales incluidos del primer grupo es menor que o igual al valor que comprende k bits digitales incluidos en el segundo grupo,

en donde k se refiere a un número natural.

9. El circuito integrado de la reivindicación 6, en donde:

los nodos en el módulo (321, 322) de clave de encriptación comprenden capas conductoras de un semiconductor, y

la regla de diseño está asociada con un espacio entre las capas conductoras del semiconductor y el módulo de clave de encriptación está configurado para generar y proporcionar la clave de encriptación basándose en si se cortocircuitan las capas conductoras del semiconductor.

10. El circuito integrado de la reivindicación 5, en donde

el módulo (321, 322) de clave de encriptación comprende N celdas unitarias, cada una para emitir un valor digital de 1 bit, cada una de las N celdas unitarias está configurada para generar el valor digital de 1 bit basándose en una variación del proceso de fabricación de semiconductor, y

el módulo de clave de encriptación está configurado para generar y proporcionar una clave de encriptación de N bits, en donde N se refiere a un número natural;

y opcionalmente en donde la primera celda unitaria entre las N celdas unitarias comprende:

un primer inversor (410) que tiene un primer umbral lógico; y

un segundo inversor (420) que tiene un segundo umbral lógico,

en donde el primer inversor y el segundo inversor forman una estructura de realimentación en la cual un terminal de entrada del primer inversor y un terminal de salida del segundo inversor están conectados a un primer nodo, y un terminal de salida del primer inversor y un terminal de entrada del segundo inversor están conectados a un segundo nodo, y

el primer umbral lógico es diferente del segundo umbral lógico basado en la variación del proceso de fabricación de semiconductores, y un valor digital de 1 bit correspondiente a la primera celda unitaria es determinado basándose en un nivel lógico del primer nodo y en un nivel lógico del segundo nodo.

11. El circuito integrado de la reivindicación 4, en donde el módulo (321, 322) de clave de encriptación comprende N amplificadores (811, 812, 813, 814, 815, 816) diferenciales,

en donde, cuando dos terminales de entrada del primer amplificador, entre los N amplificadores diferenciales, son cortocircuitados, niveles lógicos de los dos terminales de salida del primer amplificador diferencial difieren entre sí basándose en una variación del proceso de fabricación de semiconductores, y un valor digital de 1 bit correspondiente al primer amplificador diferencial se determina basándose en los niveles lógicos de los dos terminales de salida, y

el modo de clave de encriptación está configurado para generar y proporcionar una clave de encriptación de N bits,

en donde N se refiere a un número natural.

12. El circuito integrado de la reivindicación 1, en donde circuito integrado está dispuesto en una tarjeta inteligente para ejecutar el algoritmo de encriptación en aplicaciones de la tarjeta inteligente.

13. Un método de encriptación que comprende:

recibir unos datos de entrada para ser encriptados en un módulo (110) de encriptación de un circuito integrado, el circuito integrado que comprende una pluralidad de módulos (321, 322) de clave de encriptación para proporcionar diferentes claves de encriptación;

seleccionar uno de la pluralidad de módulos (321, 322) de clave de encriptación; y

encriptar los datos ejecutando un algoritmo de encriptación utilizando una clave de encriptación proporcionada por el módulo (321, 322) de clave de encriptación seleccionado, caracterizado porque el módulo (110) de encriptación comprende una pluralidad de celdas estándar, en donde la pluralidad de módulos (321, 322) de clave de encriptación está dispuesta en posiciones aleatorias entre disposiciones de la pluralidad de celdas estándar incluidas en el módulo de algoritmo, y en donde al menos una porción de la pluralidad de módulos de clave de encriptación son módulos de clave de encriptación de simulación que no proporcionan claves de encriptación.

FIG. 1

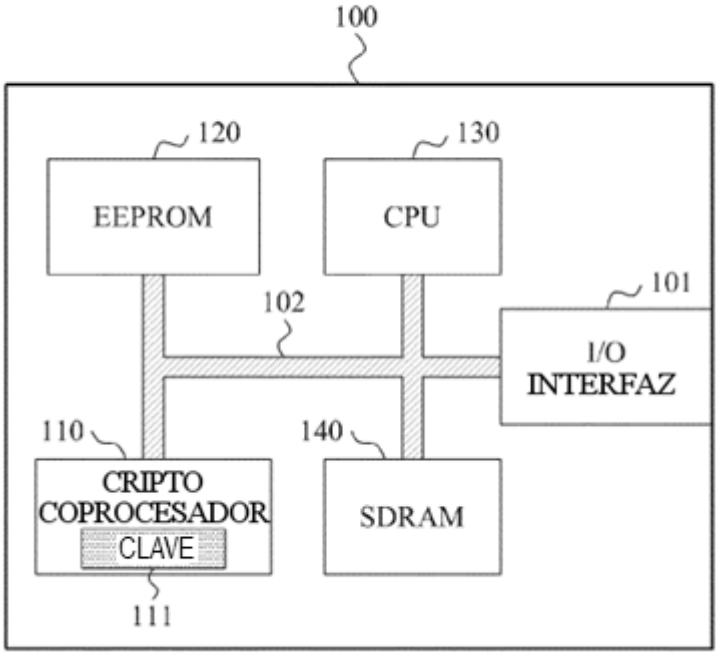
100
120
EEPROM
130
CPU
101
102
I/O
INTERFAZ
110
CRIPTO
COPROCESADOR
CLAVE
111
140
SDRAM

FIG. 2

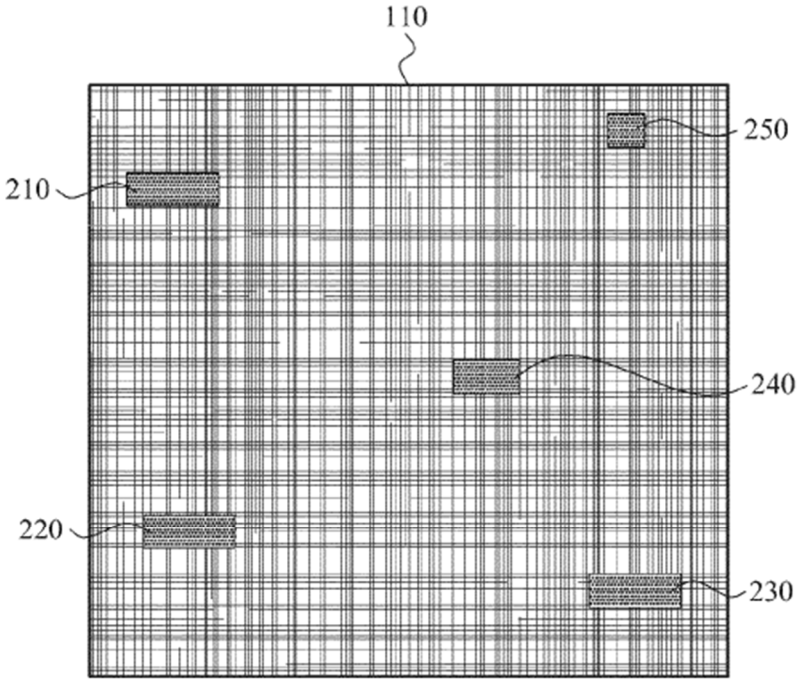

FIG. 3

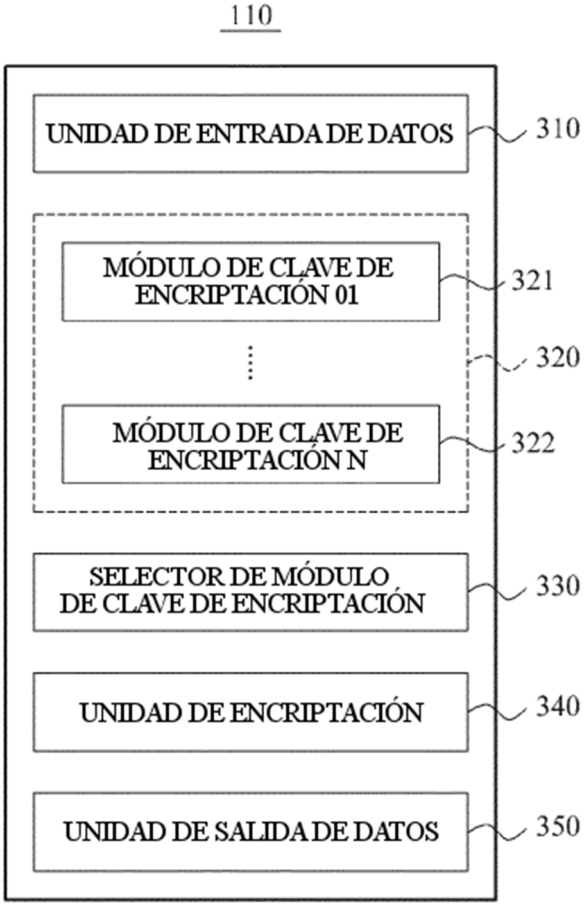
110
UNIDAD DE ENTRADA DE DATOS
310
MÓDULO DE CLAVE DE ENCRIPTACIÓN 01
321
320
MÓDULO DE CLAVE DE ENCRIPTACIÓN N
322
SELECTOR DE MÓDULO DE CLAVE DE ENCRIPTACIÓN
330
UNIDAD DE ENCRIPTACIÓN
340
UNIDAD DE SALIDA DE DATOS
350

FIG. 4

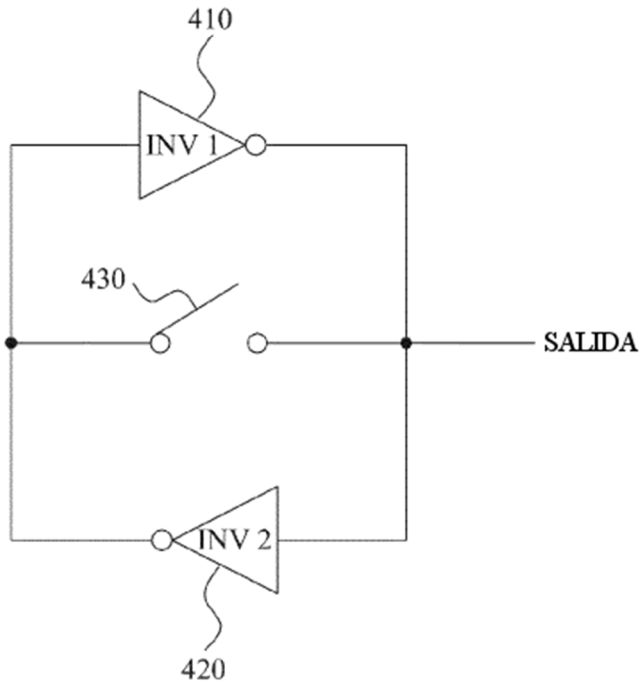

FIG. 5

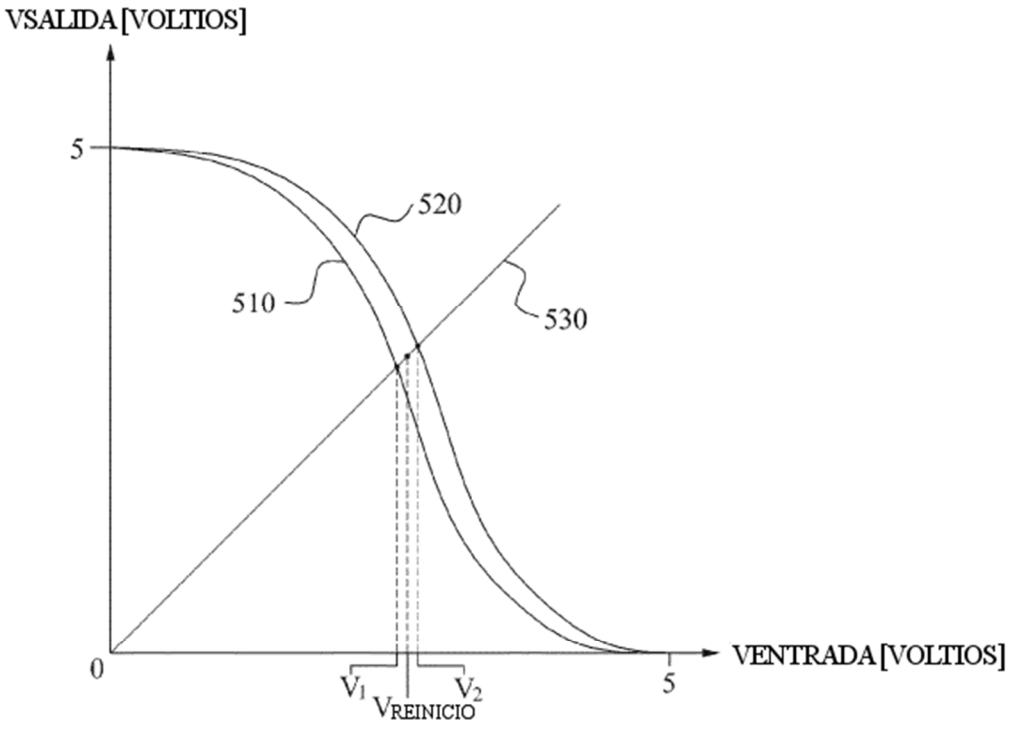
VSALIDA [VOLTIOS]
5
520
510
530
0
V1
VREINICIO
V2
5
VENTRADA [VOLTIOS]

FIG. 6

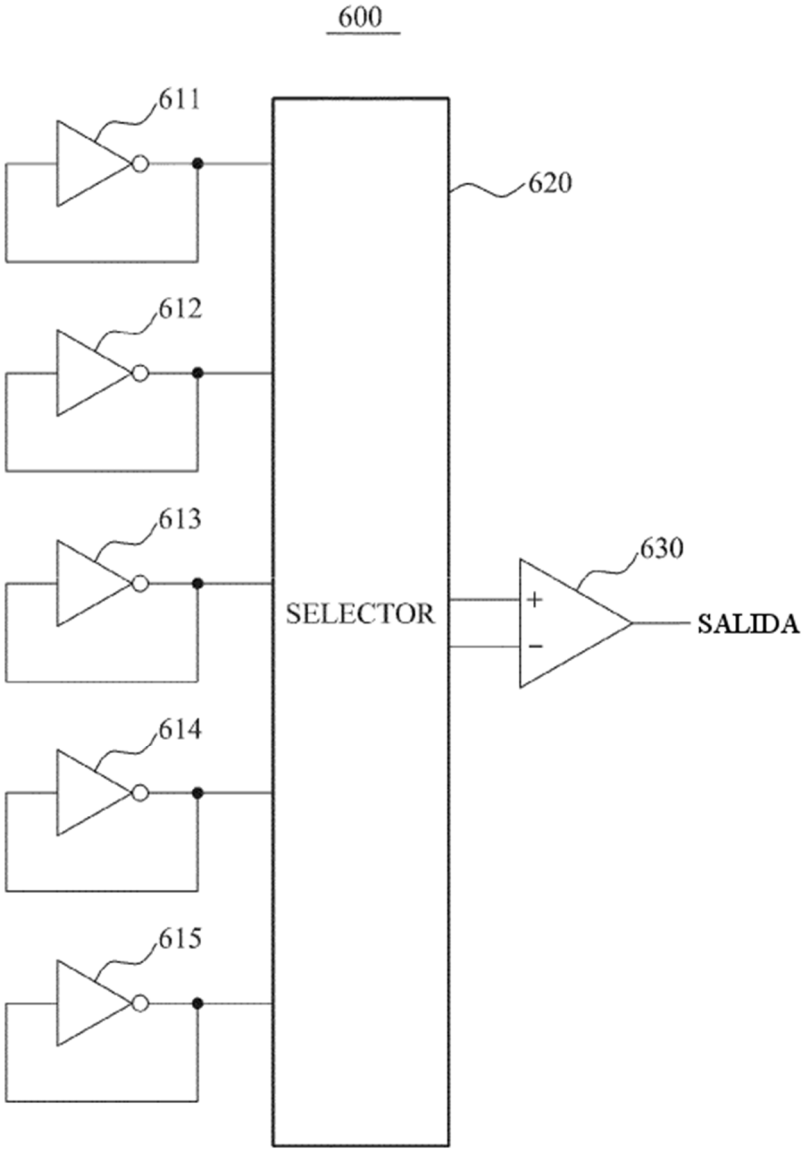

FIG. 7

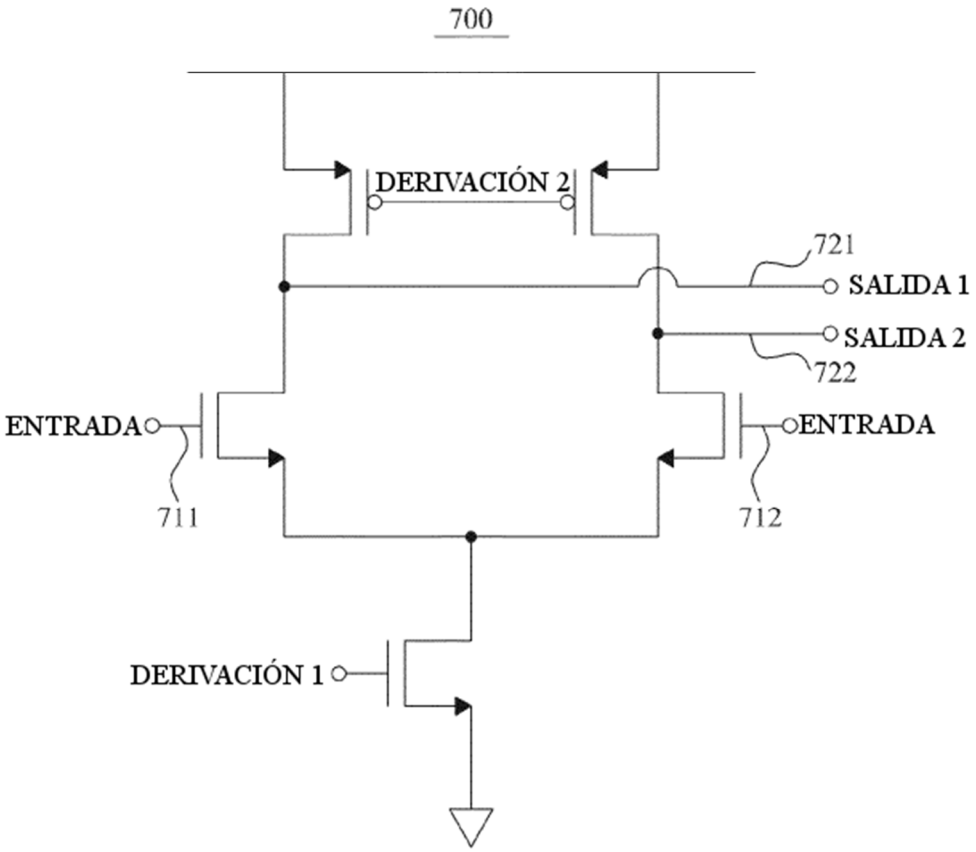
700
DERIVACIÓN 2
721
SALIDA 1
SALIDA 2
722
ENTRADA
ENTRADA
711
712
DERIVACIÓN 1

FIG. 8

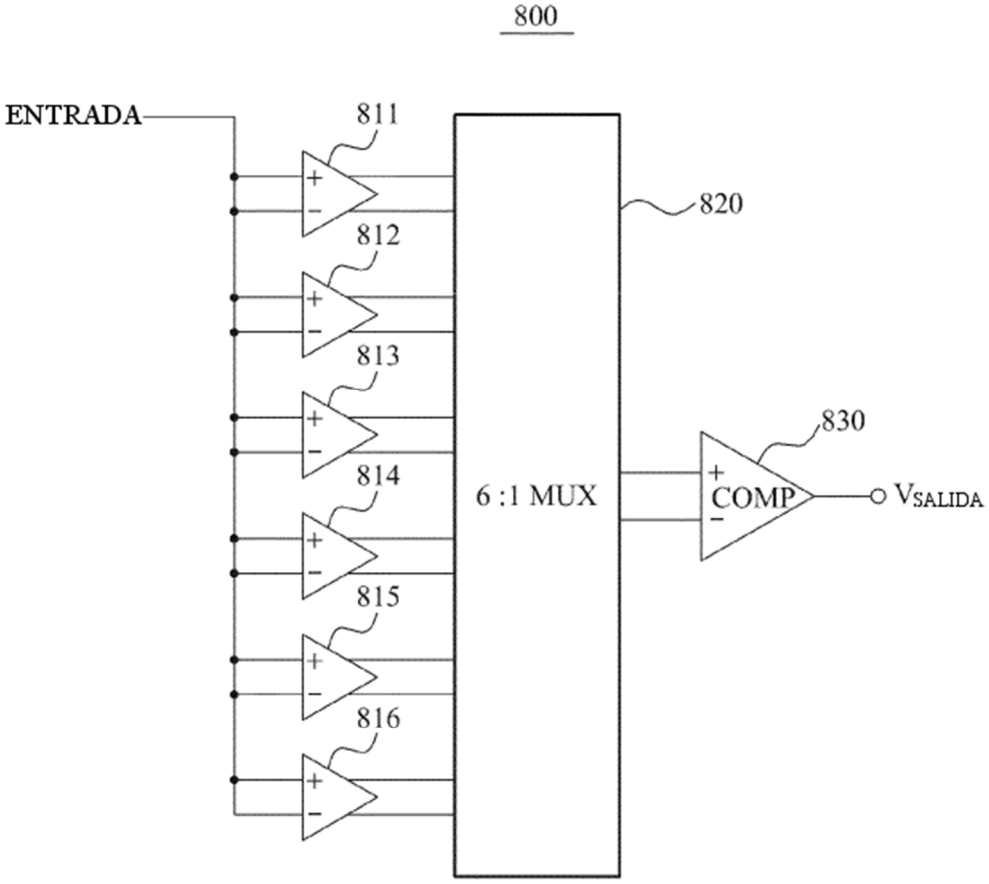
800
ENTRADA
811
812
813
814
815
816
820
6 :1 MUX
830
COMP
VSALIDA

FIG. 9

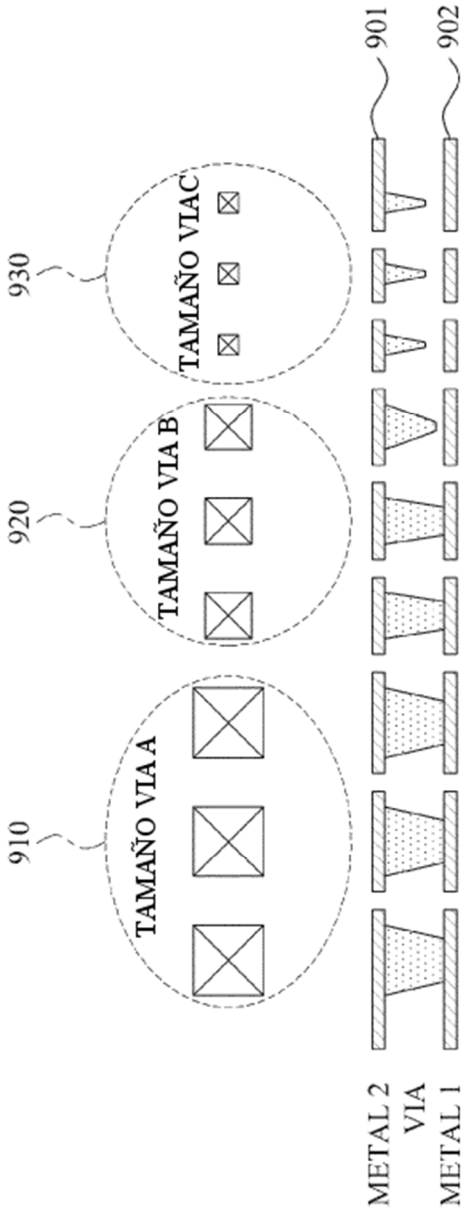
910
TAMAÑO VIA A
920
TAMAÑO VIA B
930
TAMAÑO VIAC
901
902
METAL 2
VIA
METAL 1
VALOR
0 0 0 0 0 1 1 1 1

FIG. 10

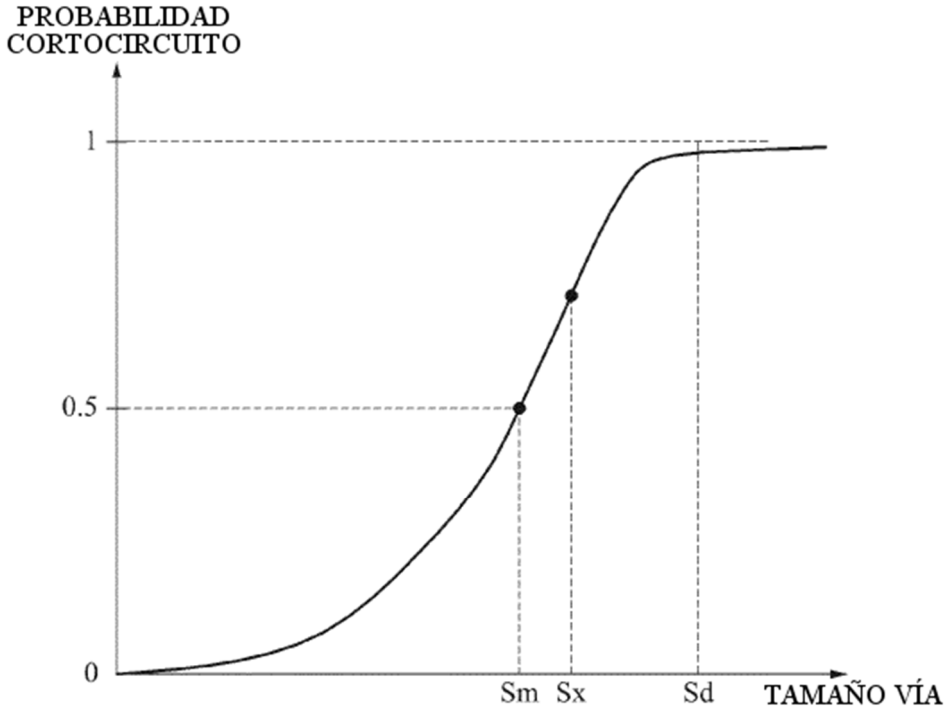

FIG. 11

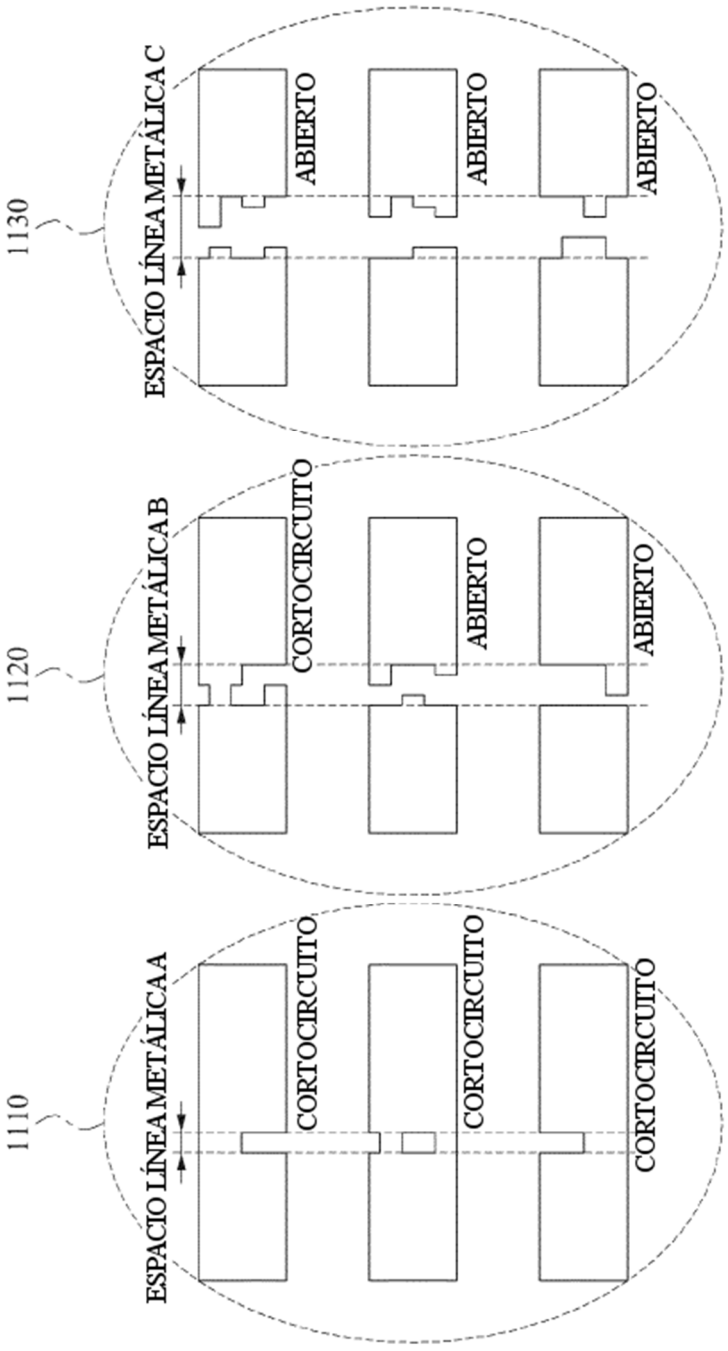
1110
ESPACIO LÍNEA METÁLICA A
CORTOCIRCUITO
CORTOCIRCUITO
CORTOCIRCUITO
1120
ESPACIO LÍNEA METÁLICA B
CORTOCIRCUITO
ABIERTO
ABIERTO
1130
ESPACIO LÍNEA METÁLICA C
ABIERTO
ABIERTO
ABIERTO

FIG. 12

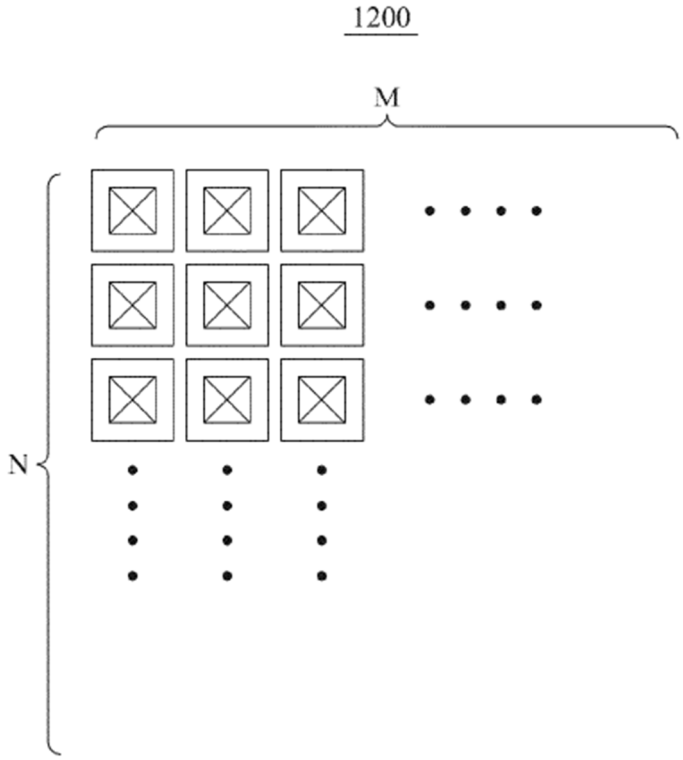

FIG. 13