(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 758 775**

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.12.2017 E 17207589 (7)**

(97) Fecha y número de publicación de la concesión europea: **25.09.2019 EP 3343832**

(54) Título: **Estructura de circuito de función física no clonable**

(30) Prioridad:

30.12.2016 CN 201611255571

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.05.2020

(73) Titular/es:

TONGXIN MICROELECTRONICS CO., LTD. (100.0%)
Floor 18, West Block, Building D Tsinghua, Tongfang Hi-Tech Plaza No.1 Wangzhuang Road 100083 Haidian District Beijing, CN

(72) Inventor/es:

SU, LINLIN;
SHENG, JINGGANG;
CHEN, GANG;
DING, YIMIN;
YUE, CHAO;
HOU, YAN y
XU, QIULIN

(74) Agente/Representante:

GARCÍA GONZÁLEZ, Sergio

DESCRIPCIÓN

Estructura de circuito de función física no clonable

Campo

La presente invención se refiere al campo de la seguridad de la información y, en particular, a la estructura de un circuito de función física no clonable (PUF).

Antecedentes

La función física no clonable (PUF) es una función que ingresa un incentivo para una entidad física y emite una respuesta impredecible utilizando una diferencia aleatoria de su inevitable construcción física interna. La PUF se aplica ampliamente en el campo de la seguridad del hardware.

Existen dos tipos de estructuras de circuito de PUF digital en la técnica convencional. Un tipo de PUF es una PUF basada en un árbitro, que logra una función PUF mediante diferentes retrasos de propagación de la señal digital entre diferentes chips. Un problema principalmente de este tipo de PUF es la inestabilidad del circuito. Cuando el circuito funciona a diferentes temperaturas y/o en diferentes entornos de tensión, la transmisión de la señal digital se verá afectada, lo que dará como resultado una salida inconsistente de los datos PUF. El otro tipo de PUF es una PUF basada en la Memoria Estática de Acceso Aleatorio (SRAM), que logra la unicidad al utilizar la aleatoriedad de los datos de la RAM cuando se enciende el chip. Sin embargo, la tasa de error de los datos PUF basados en SRAM es relativamente alta, lo que generalmente requiere circuito(s) de código de corrección de errores (ECC) a gran escala para garantizar la exactitud de los datos PUF basados en SRAM. Por ejemplo, para lograr la tasa de error de $6{,}85\times10^{-7}$, resultando en que el circuito PUF genere claves secretas de 2048 bits, se necesita tratar con al menos 7,75k bytes de ECC. En otras palabras, para producir datos de claves secretas de 2048 bits, se debe ocupar un espacio de almacenamiento SRAM de 7,75k bytes.

El documento de patente US 2016/330038 A1 divulga un aparato para generar valores digitales para proporcionar un valor digital aleatorio. El aparato genera el valor digital basado en una variación del procedimiento de semiconductores. El aparato incluye una unidad de generación para generar una pluralidad de valores digitales, basada en la variación del procedimiento de semiconductores, y una unidad de procesamiento para procesar los valores digitales y proporcionar un primer valor digital. La unidad de generación incluye una pluralidad de funciones físicamente no clonables (PUF). Un parámetro se aplica de manera diferente a las PUF, y las PUF generan los valores digitales.

El documento de patente US 2016/247769 A1 divulga una estructura de diseño para un circuito de identificación en chip, que incluye pares de conductores formados dentro de una o más capas de metalización. La distancia entre los conductores en cada par está predeterminada de modo que, dado que se conoce a través de las variaciones de la línea de chips, existe una posibilidad aleatoria de un corto. Diferentes máscaras forman primeros conductores (por ejemplo, líneas metálicas separadas por distancias variables y que tienen anchos diferentes) y segundos conductores (por ejemplo, vías metálicas separadas por distancias variables y que tienen anchos iguales). El primer y segundo conductores se alternan a través del chip. Debido a las diferentes distancias de separación y anchos de los primeros conductores, las diferentes distancias de separación de los segundos conductores y las variaciones aleatorias de alineación de la máscara, cada primer conductor puede acortar hasta dos segundos conductores. El patrón resultante de cortos y aperturas se utiliza como un identificador en chip o una clave privada.

Sumario

En vista de lo anterior, la presente invención proporciona una estructura de circuito de función física no clonable (PUF) para lograr la estabilidad del circuito y evitar el uso de circuito(s) ECC a gran escala para asegurar la exactitud de los datos PUF.

Con el fin de resolver el problema técnico mencionado anteriormente, se usan las siguientes soluciones técnicas en la presente invención.

La invención reivindicada es:

Una estructura de circuito de función física no clonable (PUF) que comprende: n grupos de conductores pasivos y n unidades XOR, estando los n grupos de conductores pasivos y las n unidades XOR en una relación de correspondencia uno a uno, donde:

cada uno de dichos grupos de conductores pasivos comprende m conductores pasivos, cada uno de dichos conductores pasivos comprende una primera terminal y una segunda terminal, la primera terminal de cada

uno de dichos conductores pasivos está conectada a una fuente de alimentación, y la segunda terminal está conectada a una terminal de entrada de la unidad XOR,

las segundas terminales de los conductores pasivos dentro de un mismo grupo de conductores pasivos están conectadas a la terminal de entrada de la unidad XOR correspondiente,

donde cuando el conductor pasivo está en un estado conectado, la segunda terminal del conductor pasivo emite una señal de alto nivel, cuando el conductor pasivo está en un estado desconectado, la segunda terminal del conductor pasivo emite una señal de bajo nivel y la señal emitida desde la segunda terminal del conductor pasivo se ingresa a la unidad XOR correspondiente, donde cada una de las n unidades XOR realiza una operación XOR en las señales emitidas por los conductores pasivos dentro del mismo grupo de conductores pasivos para obtener un resultado de operación XOR, y los resultados de la operación XOR obtenidos por todas las unidades XOR son datos PUF, donde n y m son números enteros positivos,

donde los anchos de los conductores pasivos dentro del mismo grupo de conductores pasivos no son exactamente iguales, y la diferencia de ancho entre el ancho de al menos un conductor pasivo del grupo de conductores pasivos y el ancho crítico del mismo grupo de conductores pasivos es menor o igual que un primer umbral para que dicho al menos un conductor pasivo tenga incertidumbre de conectividad en un procedimiento de fabricación del chip,
y/o

dentro del mismo grupo de conductores pasivos, dicho al menos un conductor pasivo comprende al menos un primer segmento de conductor pasivo y un segundo segmento de conductor pasivo, existe un espacio entre dicho primer segmento de conductor pasivo y dicho segundo segmento de conductor pasivo, y una diferencia de espacio entre al menos uno de dicho espacio y un espacio crítico es menor o igual que un segundo umbral, de modo que dicho al menos un conductor pasivo tiene incertidumbre de conectividad durante el procedimiento de fabricación del chip, en la que:

dicho ancho crítico es un ancho mínimo que asegura que el conductor pasivo pueda conectarse cuando el conductor pasivo se fabrica durante el procedimiento de fabricación del chip, y
dicho espacio crítico es un espacio mínimo que asegura que el conductor pasivo pueda conectarse cuando el conductor pasivo, que comprende una pluralidad de segmentos de conductores pasivos separados entre sí, se fabrica durante el procedimiento de fabricación del chip.

Opcionalmente, el intervalo del ancho de dicho conductor pasivo en el mismo grupo de conductores pasivos cubre el ancho crítico correspondiente a múltiples condiciones de procedimiento de fabricación de un chip.

Opcionalmente, al menos dos de dichos conductores pasivos tienen el mismo ancho en el mismo grupo de conductores pasivos.

Opcionalmente, el intervalo del espacio entre dicho primer segmento de conductor pasivo y dicho segundo segmento de conductor pasivo en el mismo grupo de conductores pasivos cubre el espacio crítico correspondiente a múltiples condiciones de procedimiento de fabricación de un chip.

Opcionalmente, al menos dos de dichos conductores pasivos tienen los mismos espacios entre dicho primer segmento de conductor pasivo y dicho segundo segmento de conductor pasivo dentro del mismo grupo de conductores pasivos.

Opcionalmente, la estructura del circuito además comprende: un circuito ECC, en el que una terminal de entrada de dicho circuito ECC está conectada con una terminal de salida de cada unidad XOR, la terminal de salida de dicho circuito ECC emite datos PUF, la longitud de dichos datos PUF son q bits, donde q es un número entero positivo, y el valor de q está relacionado con el valor de n y la estructura del circuito ECC.

Opcionalmente, dicho conductor pasivo comprende: uno de un alambre metálico, un polisilicio con siliciuro, un polisilicio no-siliciuro, una fuente de difusión de tipo n, una fuente de difusión de tipo p, un pozo n o un pozo p.

En comparación con la técnica anterior, la invención tiene los siguientes efectos beneficiosos.

La estructura de circuito de función física no clonable (PUF) proporcionada por la invención se basa en el principio de incertidumbre de conectividad en el procedimiento de fabricación de los conductores pasivos para los cuales cada conductor pasivo tiene un ancho cercano al valor crítico, y/o el espacio entre dos conductores pasivos adyacentes está cerca del valor crítico. En base al principio, en la estructura de circuito de función física no clonable (PUF) proporcionada por la presente invención, los anchos de los conductores pasivos en el mismo grupo de conductores pasivos no son exactamente los mismos, y/o, los espacios entre los segmentos de conductores pasivos de los conductores pasivos en el mismo grupo de conductores pasivos no son exactamente

iguales, y la aleatoriedad de la conectividad en los conductores pasivos se realiza por la diferencia de ancho y/o espacio, logrando así la función PUF.

Además, dado que la conexión y desconexión de los conductores pasivos se puede estabilizar después de que se completa la fabricación, y la estructura de circuito de función física no clonable (PUF) proporcionada por la presente invención no se ve afectada por el entorno de trabajo del chip y no requiere circuito(s) ECC a gran escala como circuito(s) de post-procesamiento. Por lo tanto, para lograr un rendimiento relativamente más estable, no resulta necesario tener circuito(s) ECC a gran escala para garantizar la exactitud de los datos PUF, y simplemente resulta opcional tener circuito(s) ECC simple(s) para garantizar la exactitud de los datos PUF.

Breve descripción de los dibujos

A fin de comprender claramente las realizaciones específicas de la presente invención, a continuación, se proporciona una breve descripción de los dibujos utilizados en las realizaciones específicas de la presente invención.

La Figura 1 es un diagrama esquemático de una estructura de circuito de función física no clonable (PUF) proporcionada por la primera realización de la presente invención.

La Figura 2 es un diagrama esquemático de una estructura de circuito de función física no clonable (PUF) proporcionada por la segunda realización de la presente invención.

La Figura 3 es un diagrama estructural específico de un circuito de código de corrección de errores (ECC) proporcionado por la segunda realización de la presente invención.

La Figura 4 es un diagrama estructural esquemático de un grupo conductor pasivo proporcionado por la tercera realización de la presente invención.

Descripción detallada de las realizaciones

En lo sucesivo, se describen a detalle realizaciones específicas de la presente invención con referencia a los dibujos adjuntos.

Como se describe en la sección de Antecedentes, la función física no clonable (PUF) es una función que genera una respuesta única e impredecible usando una diferencia aleatoria de su construcción física intrínseca inevitable. Por lo tanto, la estructura de circuito de función física no clonable (PUF) de acuerdo con las realizaciones de la presente solicitud se basa en el principio de incertidumbre de conectividad en el procedimiento de fabricación de los conductores pasivos para los cuales cada conductor pasivo tiene un ancho cercano al valor crítico, y/o el espacio entre dos conductores pasivos adyacentes está cerca del valor crítico.

En base a los principios anteriores, la presente invención proporciona la realización específica de la estructura de circuito de función física no clonable (PUF). Primero, consulte la Primera Realización.

Específicamente, los conductores pasivos con ancho y/o espacio cerca del valor crítico pueden conectarse o desconectarse en el procedimiento de fabricación. En este punto, el estado conectado y el estado desconectado de los conductores pasivos son aleatorios.

En base a los principios anteriores, la presente invención proporciona la realización específica de la estructura de circuito de función física no clonable (PUF). En primer lugar, se describe la Primera Realización.

<u>Primera Realización</u>

La Figura 1 es un diagrama esquemático de una estructura de circuito de función física no clonable (PUF) de acuerdo con una primera realización de la presente invención. Como se muestra en la Figura 1, la estructura de circuito de función física no clonable (PUF) puede incluir:

n grupos de conductores pasivos 10(1) a 10(n) y n unidades XOR 20(1) a 20(n), donde n es un número entero positivo.

Cada uno de los n grupos de conductores pasivos 10 incluye m conductores pasivos NET(0) a NET(m-1), donde m es un número entero positivo. Cada conductor pasivo NET incluye una primera terminal y una segunda terminal, en el que la primera terminal de cada conductor pasivo NET está conectada a una fuente de alimentación VDD, la segunda terminal de cada conductor pasivo NET está conectada a una terminal de entrada de una unidad XOR 20, en el que los conductores pasivos NET en el mismo grupo de conductores pasivos 10 están conectados a las terminales de entrada de la misma unidad XOR 20. Por lo tanto, en la estructura de

circuito de función física no clonable (PUF) proporcionada por la presente invención, un grupo de conductores pasivos 10 corresponde a una unidad XOR 20, de modo que el número de las unidades XOR corresponde al número del grupo de conductores pasivos.

En las realizaciones de la presente invención, el conductor pasivo incluye uno de un alambre metálico, un polisilicio con siliciuro, un polisilicio no-siliciuro, una fuente de difusión de tipo n, una fuente de difusión de tipo p, un pozo n y un pozo p.

Cada una de dichas n unidades XOR 20(1) a 20(n) realiza una operación XOR en señales ingresadas por la segunda terminal del conductor pasivo para obtener un resultado de operación XOR, el resultado de operación XOR son datos PUF, y los datos PUF son emitidos por una terminal de salida de la unidad XOR. En la realización de la presente invención, la longitud total de dichos datos PUF es de n bits, donde n y m son números enteros positivos.

En la realización de la presente invención, los anchos de los m conductores pasivos NET en un grupo de conductores pasivos 10 no son exactamente los mismos. Específicamente, en el mismo grupo de conductores pasivos 10, los anchos de los m conductores pasivos NET pueden ser diferentes entre sí, y pueden ser parcialmente idénticos y parcialmente diferentes, en el que la diferencia de ancho entre el ancho y el ancho crítico de una porción de los conductores pasivos NET dentro del mismo grupo de conductores pasivos 10 son menores o iguales que el primer umbral, de modo que al menos una parte del conductor pasivo tiene una incertidumbre de conectividad en el procedimiento de fabricación del chip. Por lo tanto, en la estructura de circuito de función física no clonable (PUF) proporcionada por la realización de la presente invención, una parte de los conductores pasivos está en el estado conectado, mientras que la otra parte de los conductores pasivos está en el estado desconectado.

En la primera realización de la presente patente, el ancho crítico es un ancho mínimo que asegura que el conductor pasivo debe poder conectarse cuando el conductor pasivo se fabrica en un procedimiento de fabricación del chip. El primer umbral puede ser un valor empírico basado en una serie de resultados experimentales.

La estructura de circuito de función física no clonable (PUF) proporcionada por la presente invención logra una función física no clonable utilizando la incertidumbre de conectividad del conductor pasivo cuyo valor de ancho está cerca del ancho crítico.

Debe hacer notar que el ancho crítico varía con las condiciones del procedimiento de fabricación del chip, es decir, el ancho crítico está relacionado con la condición del procedimiento de fabricación del chip. Para permitir que la estructura de circuito de función física no clonable (PUF) proporcionada por la presente invención logre la función física no clonable en múltiples procedimientos de fabricación de chips diferentes, en la estructura de circuito de función física no clonable (PUF) proporcionada por la presente invención, el intervalo de ancho de los conductores pasivos dentro del mismo grupo de conductores pasivos cubre los anchos críticos de la pluralidad de diferentes procedimientos de fabricación de chips.

Además, cuanto mayor sea el conductor pasivo con el mismo ancho, mayor será la probabilidad de obtener el ancho crítico, más fácil se logra el ancho crítico y más fácil se logra la aleatoriedad de conexión del conductor pasivo. Por lo tanto, para aumentar la probabilidad de obtener el ancho crítico, al menos dos conductores pasivos NET tienen el mismo valor de ancho dentro del mismo grupo de conductores pasivos 10.

La estructura de circuito de función física no clonable (PUF) proporcionada por la realización de la presente invención funciona de la siguiente manera.

Las primeras terminales de todos los conductores pasivos NET en los respectivos grupos de conductores pasivos 10(1) a 10(n) están conectadas a la fuente de alimentación VDD. Cuando el conductor pasivo NET está en un estado conectado, la segunda terminal del conductor pasivo NET genera un nivel alto, la lógica es “1”; y cuando el conductor pasivo está en un estado desconectado, la segunda terminal del conductor pasivo emite un nivel bajo, la lógica es “0”. La segunda terminal del conductor pasivo NET está conectada a la terminal de entrada de la unidad XOR correspondiente 20. Dado que los anchos de los conductores pasivos NET en el mismo grupo de conductores pasivos 10 son diferentes, después de que se complete la fabricación del grupo de conductores pasivos bajo diferentes condiciones del procedimiento de fabricación del chip, en el mismo grupo de conductores pasivos 10, algunos conductores pasivos NET están en estado conectado, y algunos conductores pasivos NET están en estado desconectado. Por lo tanto, en la segunda terminal del conductor pasivo NET, algunas salidas son altas y algunas salidas son bajas, y la lógica correspondiente es “1” y “0” respectivamente.

Cada unidad XOR 20 realiza una operación XOR en señales de m conductor pasivo NET en el correspondiente grupo de conductor pasivo 10 para obtener un resultado de operación XOR, y la terminal de salida de la unidad XOR 20 emite el resultado de operación XOR. Los resultados de la operación XOR de las n unidades XOR 20

son los datos PUF, y los datos PUF incluyen q bits. El resultado de la operación XOR emitido por la unidad XOR 20 está directamente relacionado con la aleatoriedad de la conexión de los conductores pasivos NET.

Lo anterior es la realización específica de la estructura de circuito de función física no clonable (PUF) proporcionada por la primera realización de la presente invención. En la realización específica, los anchos de los conductores pasivos en el mismo grupo de conductores pasivos no son exactamente los mismos, y la aleatoriedad de la conexión del conductor pasivo se realiza por los diferentes anchos, y luego se puede realizar la función PUF.

Además, debido a la conexión y desconexión del conductor pasivo, el estado estable se puede lograr después de que se complete la fabricación del conductor pasivo, y no se ve afectado por el entorno de trabajo del chip, y no requiere un gran número de circuito(s) ECC como circuito(s) de post-procesamiento. Por lo tanto, para lograr un rendimiento relativamente más estable, no resulta necesario tener circuito(s) ECC a gran escala para garantizar la exactitud de los datos PUF para la estructura de circuito de función física no clonable (PUF) proporcionada por la presente invención, y simplemente resulta opcional tener circuito(s) ECC simple(s) para garantizar la exactitud de los datos PUF.

Además, cuando el entorno de aplicación del chip es más severo, puede conducir a una tasa de error de bits más alta de los datos PUF. Con el fin de mejorar la calidad de los datos PUF y evitar errores de datos PUF a lo largo del tiempo, la presente invención proporciona además la segunda realización.

Segunda Realización

Debe hacer notar que, la estructura de circuito de función física no clonable (PUF) descrita en la segunda realización se obtiene en función de la estructura de circuito de función física no clonable (PUF) descrita en la primera realización. Por lo tanto, la estructura de circuito proporcionada por la segunda realización tiene muchas similitudes con la estructura de circuito proporcionada por la primera realización. A modo de resumen, la segunda realización de la presente invención proporciona una mayor descripción de las diferencias en cuanto a los detalles, y la primera realización de la presente invención tiene la descripción relacionada de las similitudes.

La Figura 2 es un diagrama esquemático de la estructura de circuito de función física no clonable (PUF) proporcionada por la segunda realización de la presente invención. Como se muestra en la Figura 2, además de los n grupos de conductores pasivos 10(1) a 10(n) y las n unidades XOR 20(1) a 20(n) mostradas en la Figura 1, la estructura del circuito puede comprender además opcionalmente: un circuito ECC 30.

La terminal de entrada del circuito ECC 30 está conectada a las terminales de salida de todas las unidades XOR 20(1) a 20(n), de modo que el circuito ECC 30 procesa los datos PUF emitidos por las unidades XOR 20(1) a 20(n), para obtener los datos PUF válidos.

Debe hacer notar que, en la segunda realización de la presente invención, las estructuras y la relación de conexión de los grupos conductores pasivos 10(1) a 10(n) y las unidades XOR 20(1) a 20(n) son completamente iguales a los de los grupos de conductores pasivos 10(1) a 10(n) y las unidades XOR 20(1) a 20(n) en la primera realización de la presente invención, que no se describen a detalle en la presente memoria, y a modo de resumen, la primera realización tiene la descripción relacionada.

El circuito ECC 30 puede ser cualquier tipo de circuito ECC. Para que la selección de los circuitos ECC sea diferente, el número de bits q de los datos PUF generados por la estructura de circuito de función física no clonable (PUF) proporcionada por la segunda realización de la presente aplicación también es diferente.

Debe hacer notar que, en la segunda realización de la presente invención, m solo está relacionado con el procedimiento de fabricación del chip, y q es la longitud de los datos PUF finalmente requeridos, donde q es un número entero positivo y $n \geq q$. Cuando la estructura de circuito de función física no clonable (PUF) comprende el circuito ECC, q está relacionado con el valor de n y la estructura del circuito ECC, y n, q necesita satisfacer la relación relativa del algoritmo seleccionado por el circuito ECC. Por ejemplo, como se muestra en la Figura 3, si el circuito ECC 30 usa el código de repetición repetir (3) y el código de Hamming ham (7, 4), m = 40 y q = 1024, entonces n = 1024*3*7/4 = 5376. Cada grupo de conductores pasivos comprende 40 conductores pasivos con diferentes anchos, hay un total de 5376 grupos de conductores pasivos, y finalmente se genera el total de 1024 bits de datos PUF.

Lo anterior es la descripción de la realización específica de la estructura de circuito de función física no clonable (PUF) proporcionada por la segunda realización de la presente invención. En la realización específica, además de lograr los efectos beneficiosos descritos en la primera realización, la calidad de los datos PUF puede mejorarse y los errores de los datos PUF pueden prevenirse con el tiempo.

Debe hacer notar que, en la primera realización y la segunda realización descritas anteriormente, la

incertidumbre de conexión del conductor pasivo se logra por la magnitud del valor de ancho del conductor pasivo. En otra realización de la presente invención, cada uno de los conductores pasivos puede dividirse en múltiples segmentos del conductor pasivo, y la incertidumbre de conexión del conductor pasivo se logra utilizando el espacio entre los segmentos del conductor pasivo. La tercera realización se proporciona adicionalmente por la presente invención.

Tercera Realización

Debe hacer notar que una estructura de circuito de función física no clonable (PUF) proporcionada por la tercera realización tiene muchas similitudes con las de la descripción en la primera realización. A modo de resumen, la tercera realización de la presente invención proporciona una mayor descripción de las diferencias en cuanto a los detalles, y la primera realización de la presente invención tiene la descripción relacionada de las similitudes.

Debe hacer notar que, en la tercera realización de la presente invención, las estructuras y la relación de conexión de los grupos conductores pasivos 10(1) a 10(n) y las unidades XOR 20(1) a 20(n) son completamente iguales a las de los grupos de conductores pasivos 10(1) a 10(n) y las unidades XOR 20(1) a 20(n) en la primera realización de la presente invención, que no se describen a detalle en a presente memoria, y a modo de resumen, la primera realización tiene la descripción relacionada.

La estructura de circuito de función física no clonable (PUF) proporcionada por la tercera realización difiere de la de la primera realización en que: como se muestra en la Figura 4 (la Figura 4 muestra un diagrama esquemático de la relación de conexión de un grupo conductor pasivo y una unidad XOR), cada uno de los conductores pasivos NET en el grupo de conductores pasivos comprende al menos un primer segmento de conductores pasivos S1 y un segundo segmento de conductores pasivos S2 separados entre sí, hay un cierto espacio D entre el primer segmento de conductores pasivos S1 y el segundo segmento de conductor pasivo S2, y los espacios D(1) a D(m) entre los primeros segmentos de conductores pasivos S1 y los segundos segmentos de conductores pasivos S2 del respectivo conductor pasivo NET no son exactamente iguales. Como una realización opcional de la presente invención, cada uno de los conductores pasivos NET comprende dos segmentos separados del primer segmento de conductor pasivo S1 y el segundo segmento de conductor pasivo S2.

Debe hacer notar que, en la tercera realización de la presente invención, el valor del espacio entre los primeros segmentos de conductores pasivos S1 y los segundos segmentos de conductores pasivos S2 difiere del espacio crítico, y su diferencia es menor o igual que el segundo umbral, para una porción de los conductores pasivos en el mismo grupo de conductores pasivos, de modo que al menos una porción de los conductores pasivos tiene incertidumbre de conexión en el procedimiento de fabricación del chip. Es decir, en la estructura de circuito de función física no clonable (PUF) proporcionada por la tercera realización de la presente invención, una parte de los conductores pasivos está en un estado conectado, y la otra parte de los conductores pasivos está en un estado desconectado.

En la tercera realización de la presente invención, dicho espacio crítico es un espacio mínimo que asegura que el conductor pasivo debe poder conectarse como fabricante del conductor pasivo en el procedimiento de fabricación del chip, cuando un conductor pasivo comprende una pluralidad de los segmentos de conductores pasivos separados entre sí. El segundo umbral puede ser un valor empírico basado en una serie de resultados experimentales.

La estructura de circuito de función física no clonable (PUF) proporcionada por la tercera realización de la presente invención logra la función física no clonable utilizando la incertidumbre de conectividad del espacio entre el primer segmento de conductor pasivo S1 y el segundo segmento de conductor pasivo S2 cuando el valor del espacio está cerca del espacio crítico.

Debe hacer notar que el espacio crítico varía con las condiciones del procedimiento de fabricación del chip, es decir, el espacio crítico está relacionado con las condiciones del procedimiento de fabricación del chip. Para permitir que la estructura de circuito de función física no clonable (PUF) proporcionada por la tercera realización de la presente invención logre la función física no clonable en múltiples procedimientos de fabricación de chips diferentes, en la estructura de circuito de función física no clonable (PUF) proporcionada por la presente invención, el intervalo de los valores de espacio del primer segmento de conductor pasivo y el segundo segmento de conductor pasivo dentro del mismo grupo de conductores pasivos cubre los espacios críticos de la pluralidad de diferentes procedimientos de fabricación de chips.

Además, cuanto mayor sea el conductor pasivo con el mismo espacio, mayor será la probabilidad de obtener el espacio crítico, más fácil se logra el espacio crítico y más fácil se logra la aleatoriedad de conexión del conductor pasivo. Por lo tanto, para aumentar la probabilidad de obtener el espacio crítico, al menos dos conductores pasivos en el mismo grupo conductor pasivo tienen el mismo espacio entre los segmentos de conductores pasivos.

Lo anterior es la realización específica de la estructura de circuito de función física no clonable (PUF) proporcionada por la tercera realización de la presente invención. En la realización específica, los espacios entre los segmentos de conductores pasivos de los conductores pasivos en el mismo grupo de conductores pasivos no son exactamente los mismos, y la aleatoriedad de conexión de los conductores pasivos se logra utilizando los diferentes anchos y/o espacios diferentes, y entonces se puede realizar la función PUF.

Además, debido a la conexión y desconexión del conductor pasivo, el estado estable se puede lograr después de que se complete la fabricación del conductor pasivo, y no se ve afectado por el entorno de trabajo del chip, y no requiere de circuito(s) ECC a gran escala como circuito(s) de post-procesamiento. Por lo tanto, para lograr un rendimiento relativamente más estable, no resulta necesario tener circuito(s) ECC a gran escala para garantizar la exactitud de los datos PUF para la estructura de circuito de función física no clonable (PUF) proporcionada por la presente invención, y simplemente resulta opcional tener circuito(s) ECC simple(s) para garantizar la exactitud de los datos PUF.

Además, como otra realización de la presente invención, como la descripción en la segunda realización, un circuito ECC puede agregarse opcionalmente a la estructura de circuito de función física no clonable (PUF) descrita en la tercera realización. Es similar entre la estructura de circuito en la tercera realización y la estructura del circuito descrita en la segunda realización, y será fácilmente evidente para los expertos en la técnica basándose en la estructura de circuito descrita en la segunda realización, y por lo tanto no se describirá en detalle en la presente memoria descriptiva.

Además, como la realización extendida de la realización de la presente invención, la primera realización y la tercera realización descritas anteriormente pueden combinarse. Es decir, en el mismo grupo de conductores pasivos, los anchos de al menos una parte de los conductores pasivos pueden ser diferentes, y al menos una parte de los conductores pasivos puede comprender un primer segmento de conductor pasivo y un segundo segmento de conductor pasivo separados entre sí, y los espacios entre los primeros segmentos de conductores pasivos y los segundos segmentos de conductores pasivos son diferentes. De este modo, en la realización combinada, a través de la diferencia entre el ancho del conductor pasivo y el espacio entre los segmentos de conductores pasivos, se realiza la incertidumbre de la conexión y desconexión del conductor pasivo, de modo que se puede llevar a cabo la función PUF de la estructura de circuito de función física no clonable (PUF).

REIVINDICACIONES

1. Una estructura de circuito de función física no clonable, que comprende n grupos de conductores pasivos (10(1), 10(2), 10(3), ... 10(n)) y n unidades XOR (20(1), 20(2), 20(3), ... 20(n)), estando los n grupos de conductores pasivos (10(1), 10(2), 10(3), ... 10(n)) y las n unidades XOR (20(1), 20(2), 20(3), ... 20(n)) en una relación de correspondencia uno a uno, en la que:
cada uno de dichos grupos de conductores pasivos (10(1), 10(2), 10(3), ... 10(n)) comprende m conductores pasivos (NET(0), NET(1), ... NET(m-2), NET(m-1)), cada uno de dichos conductores pasivos (NET(0), NET(1), ... NET(m-2), NET(m-1)) comprende una primera terminal y una segunda terminal, la primera terminal de cada uno de dichos conductores pasivos (NET(0), NET(1), ... NET(m-2), NET(m-1)) está conectada a una fuente de alimentación, y la segunda terminal está conectada a una terminal de entrada de la unidad XOR (20(1), 20(2), 20(3), ... 20(n)),
en la que la segunda terminal del conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) dentro de un mismo grupo de conductores pasivos (10(1), 10(2), 10(3), ... 10(n)) está conectada a la terminal de entrada de la unidad XOR correspondiente (20(1), 20(2), 20(3), ... 20(n)),
en la que cuando el conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) está en un estado conectado, la segunda terminal del conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) emite una señal de alto nivel, cuando el conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) está en un estado desconectado, la segunda terminal del conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) emite una señal de bajo nivel, y la señal emitida desde la segunda terminal del conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) se ingresa en la unidad XOR correspondiente,
en la que cada una de las n unidades XOR (20(1), 20(2), 20(3), ... 20(n)) realiza una operación XOR en las señales emitidas por los conductores pasivos (NET(0), NET(1), ... NET(m-2), NET(m-1)) dentro del mismo grupo de conductores pasivos (10(1), 10(2), 10(3), ... 10(n)) para obtener un resultado de operación XOR, y los resultados de la operación XOR obtenidos por todas las unidades XOR (20(1), 20(2), 20(3), ... 20(n)) son datos PUF, en la que n y m son números enteros positivos, **caracterizada porque:**
los anchos de los conductores pasivos (NET(0), NET(1), ... NET(m-2), NET(m-1)) dentro del mismo grupo de conductores pasivos no son exactamente iguales, y la diferencia de ancho entre el ancho de al menos un conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) del grupo de conductores pasivos (10(1), 10(2), 10(3), ... 10(n)) y un ancho crítico del mismo grupo de conductores pasivos (10(1), 10(2), 10(3), ... 10(n)) es menor o igual que un primer umbral de modo que dicho al menos un conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) tenga incertidumbre de conectividad en un procedimiento de fabricación del chip,
o
dentro del mismo grupo de conductores pasivos (NET(0), NET(1), ... NET(m-2), NET(m-1)), dicho al menos un conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) comprende al menos un primer segmento de conductor pasivo y un segundo segmento de conductor pasivo, un espacio (D(1), D(2), ... D(m-2), D(m-1)) existe entre dicho primer segmento de conductor pasivo y dicho segundo segmento de conductor pasivo, y una diferencia de espacio entre al menos un espacio (D(1), D(2), ... D(m-2), D(m-1)) y un espacio crítico es menor o igual que un segundo umbral de modo que dicho al menos un conductor pasivo (NET(0), NET(1)), ... NET(m-2), NET(m-1)) tiene incertidumbre de conectividad durante el procedimiento de fabricación del chip, en la que:
dicho ancho crítico es un ancho mínimo que garantiza que el conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) pueda conectarse cuando el conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) se fabrica durante el procedimiento de fabricación del chip, y
dicho espacio crítico es un espacio mínimo que asegura que el conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) pueda conectarse cuando el conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) que comprende una pluralidad de segmentos de conductores pasivos separados entre sí se fabrica durante el procedimiento de fabricación del chip.

2. La estructura de circuito de acuerdo con la reivindicación 1, en la que el intervalo del ancho de dicho conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) en el mismo grupo de conductores pasivos (10(1), 10(2), 10(3), ... 10(n)) cubre el ancho crítico correspondiente a una pluralidad de condiciones de procedimiento de fabricación de un chip.

3. La estructura de circuito de acuerdo con la reivindicación 1 o la reivindicación 2, en la que al menos dos de dichos conductores pasivos (NET(0), NET(1), ... NET(m-2), NET(m-1)) tienen el mismo ancho en el mismo grupo de conductores pasivos (10(1), 10(2), 10(3), ... 10(n)).

4. La estructura de circuito de acuerdo con la reivindicación 1, en la que el intervalo del espacio (D(1), D(2), ... D(m-2), D(m-1)) entre dicho primer segmento de conductor pasivo y dicho segundo segmento de conductor pasivo en el mismo grupo de conductores pasivos (10(1), 10(2), 10(3), ... 10(n)) cubre el espacio crítico correspondiente a una pluralidad de condiciones de procedimiento de fabricación de un chip.

5. La estructura de circuito de acuerdo con la reivindicación 1 o la reivindicación 4, en la que al menos dos de dichos conductores pasivos (NET(0), NET(1), ... NET(m-2), NET(m-1)) tienen los mismos espacios (D(1), D(2), ... D(m-2), D(m-1)) entre dicho primer segmento de conductor pasivo y dicho segundo segmento de conductor pasivo dentro del mismo grupo de conductores pasivos (10(1), 10(2), 10(3), ... 10(n)).

6. La estructura de circuito de acuerdo con una cualquiera de las reivindicaciones 1 a 5, que además comprende: un circuito de código de corrección de errores (ECC) (30), en la que una terminal de entrada de dicho circuito ECC (30) está conectada con una terminal de salida de cada una de dichas unidades XOR (20(1), 20(2), 20(3), ... 20(n)), la terminal de salida de dicho circuito ECC (30) emite datos PUF, la longitud de dichos datos PUF es q bits, en la que q es un número entero positivo, y el valor de q está relacionado con el valor de n y la estructura del circuito ECC (30).

7. La estructura de circuito de acuerdo con una cualquiera de las reivindicaciones 1 a 6, en la que el conductor pasivo (NET(0), NET(1), ... NET(m-2), NET(m-1)) comprende uno de entre un alambre metálico, un polisilicio con siliciuro, un polisilicio no-siliciuro, una fuente de difusión de tipo n, una fuente de difusión de tipo p, un pozo n y un pozo p.

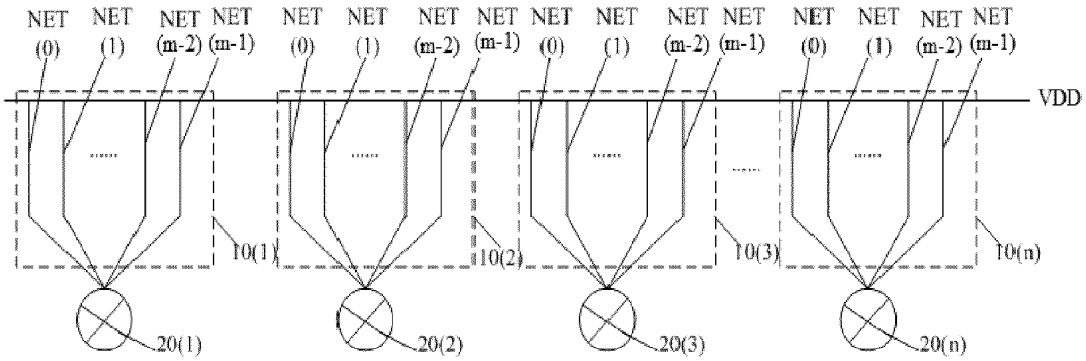

Figura 1

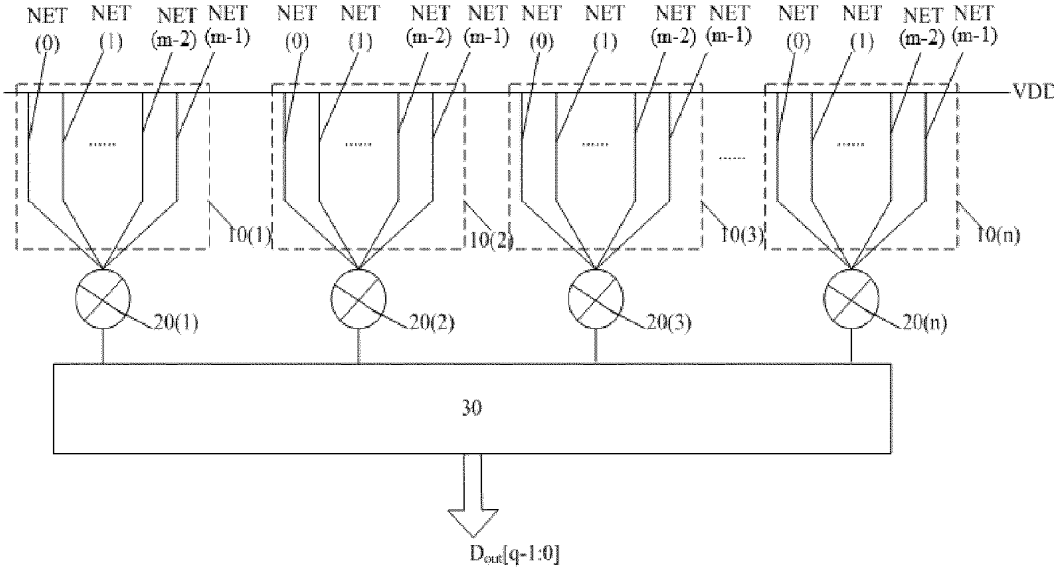

Figura 2

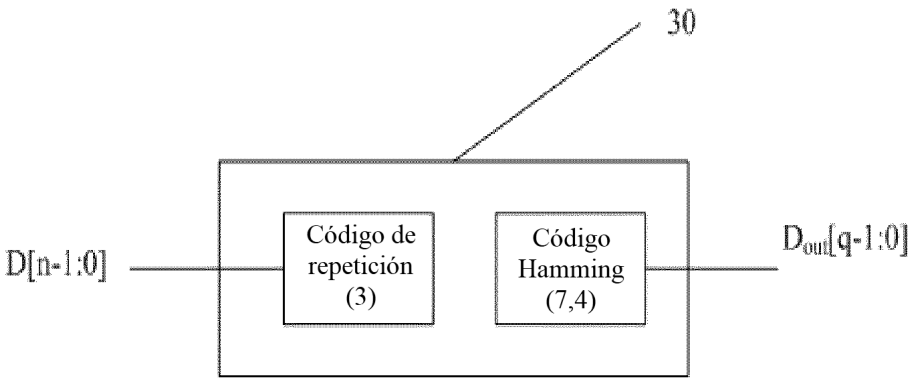

Figura 3

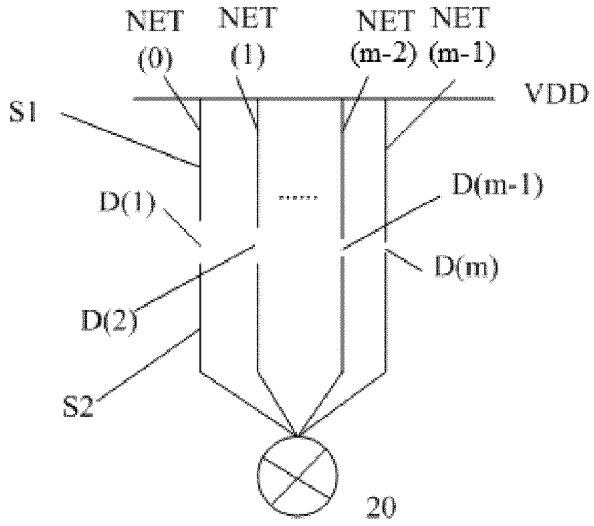

Figura 4