(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 684 846**

(21) Número de solicitud: 201730535

(51) Int. CI.:

H04L 9/32 (2006.01)
H03K 3/037 (2006.01)
H03K 3/011 (2006.01)
G06F 21/44 (2013.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

31.03.2017

(43) Fecha de publicación de la solicitud:

04.10.2018

(71) Solicitantes:

UNIVERSIDAD CARLOS III DE MADRID (100.0%)
Av. Gregorio Peces Barba, 1
28919 Leganés (Madrid) ES

(72) Inventor/es:

ENTRENA ARRONTES, Luis Alfonso;
MARTÍN GONZÁLEZ, Honorio y
SAN MILLÁN HEREDIA, Enrique

(54) Título: **Dispositivo y procedimiento para la identificación unívoca de un circuito integrado**

(57) Resumen:

La invención describe un dispositivo (1) que comprende: un primer circuito (2) generador de pulsos transitorios que tiene una entrada (2e) y una salida (2s); un segundo circuito (3) generador de pulsos transitorios, idéntico al primero excepto por las diferencias inherentes al proceso de fabricación, que tiene una entrada (3e) y una salida (3s); un circuito (4) árbitro que tiene unas primera y segunda entradas (4e1, 4e2) conectadas a la salida (2s) y a la salida (3s), y una salida (4s) de circuito árbitro, donde el circuito (4) árbitro está configurado para determinar si una señal de entrada "pregunta" introducida simultáneamente en la entrada (2e) y en la entrada (3e) llega antes como un pulso a la salida (2s) o a la salida (3s) y para emitir un pulso de salida en función de ello a través de la salida (4s) de circuito árbitro.

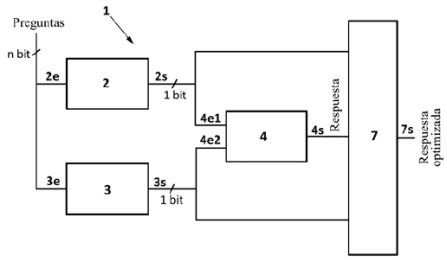

FIG. 5

ES 2 684 846 A1

DESCRIPCIÓN

Dispositivo y procedimiento para la identificación unívoca de un circuito integrado

OBJETO DE LA INVENCIÓN

La presente invención pertenece en general al campo de la electrónica, y más particularmente a las técnicas utilizadas para la identificación unívoca de circuitos integrados con el propósito de impedir su falsificación.

Un primer objeto de la presente invención es un novedoso dispositivo que contiene un circuito del tipo denominado Función Física Inclonable (PUF, Physically Unclonable Function) que proporciona una huella electrónica inclonable para un circuito integrado.

Un segundo objeto de la presente invención está dirigido al procedimiento que lleva a cabo el dispositivo anterior para obtener una huella electrónica inclonable para un circuito integrado.

ANTECEDENTES DE LA INVENCIÓN

La falsificación y reutilización de circuitos integrados constituye actualmente uno de los mayores desafíos de la industria electrónica. Según la empresa de análisis críticos IHS, estos problemas pueden suponer una perdida potencial para la industria de hasta 169 billones de dólares cada año. Es por ello que la identificación univoca de cada circuito integrado se ha convertido en uno de los mayores retos tecnológicos en estos días.

En este contexto, es conocido que los procesos de fabricación submicrométricos están sujetos a variaciones incontrolables que provocan la existencia de pequeñas diferencias en las características de cada transistor contenido en un circuito integrado. En efecto, pequeñas variaciones durante la fabricación de un circuito integrado provocan diferencias minúsculas en la velocidad del circuito y no hay nada que pueda hacerse para evitarlo. Actualmente, se están utilizando estas imperfecciones inevitables para crear una huella electrónica inclonable conocida como Función Física Inclonable (PUF, Physically Unclonable Function). En primer lugar, a un circuito integrado o chip que se desea identificar se le añade durante la fabricación un circuito de identificación adicional o circuito PUF. Como consecuencia de las mencionadas diferencias incontrolables inherentes al proceso de fabricación, este circuito PUF presenta unas características físicas únicas e inclonables. Por

tanto, basta con identificar de manera unívoca el circuito PUF para poder determinar de manera segura la identidad del circuito integrado o chip en su conjunto. Este procedimiento se ha convertido en una de las formas más sencillas de certificar que un circuito integrado es quien dice ser.

Dentro de este campo, merecen especial atención los denominados circuitos PUF de retardo o Arbiter PUF. Los circuitos Arbiter PUF se basan en la aleatoriedad de los retardos de los cables y puertas lógicas del circuito integrado, y son los más extendidos debido a su fácil implementación. En los últimos años, se han presentado diversas propuestas y solicitudes de patente sobre este tipo de circuitos denominados Arbiter PUF.

Un circuito PUF de retardo actualmente muy extendido es el denominado circuito PUF de anillos oscilantes descrito por G.E. Suh et al en "*Physical unclonable functions for device authentication and secret key generation*", Proc. Design Automation Conference (DAC 2007), pp9-14, Junio 2007. Este circuito, mostrado en la Fig. 1, incluye varios anillos oscilantes idénticos excepto por las variaciones incontrolables debidas al proceso de fabricación que están conectados a un par de multiplexores. Una señal de entrada denominada "*pregunta*" permite seleccionar 2 anillos oscilantes particulares (anillos oscilantes A y B). Se compara entonces la frecuencia de oscilación de estos dos anillos durante un periodo determinado: si el anillo oscilante A tiene una mayor frecuencia, la respuesta será '1'; en caso contrario, la respuesta será '0'.

Otro tipo de circuito PUF actualmente conocido es el denominado Glitch-PUF. Este tipo de circuito PUF se basa en el muestreo de los pulsos transitorios (denominados "glitches") que se producen durante el tiempo anterior al instante en el que un circuito alcanza un estado estable. Al igual que en el circuito PUF descrito anteriormente, los circuitos Glitch-PUF típicamente usan un esquema de pregunta/respuesta en el que cada respuesta depende exclusivamente de la pregunta y de la variación única de los retardos debidos a las tolerancias introducidas en los procesos de fabricación.

Para explicar mejor el modo de funcionamiento de los circuitos Glitch-PUF, supongamos un circuito Glitch-PUF que incluye como parte integrante un circuito sencillo como el mostrado en la Fig. 2, formado por una puerta XOR cuya salida constituye la entrada a una puerta AND. Las entradas a la puerta XOR son (x_1, x_2) y su salida se denomina x_{12}. Las entradas a la puerta AND son (x_{12}, x_3) y su salida se denomina y. Supongamos que a este circuito llega una entrada (x_1, x_2, x_3) = (1, 1, 1). Es evidente que, en régimen permanente, la salida de la puerta XOR sería x_{12} = 0 y por lo tanto la respuesta sería y = 0. Idealmente, la llegada hasta

el valor de la respuesta y = 0 se produciría de acuerdo con el diagrama de la Fig. 3a: todas las señales (x_1, x_2, x_3) adoptan su valor '1' de manera simultánea, y como consecuencia la salida y adopta el valor '0' en todo momento. Sin embargo, la realidad es que, debido a las pequeñas variaciones en los retardos de los diferentes transistores del circuito Glitch-PUF, la llegada al circuito de la Fig. 2 de los flancos de subida de las señales de entrada (x_1, x_2, x_3) no se produce simultáneamente. Concretamente, como se muestra en la Fig. 3b, la señal x_1 llega antes que la señal x_2, y por tanto durante un pequeño intervalo de tiempo la salida x_{12} de la puerta XOR adopta un valor '1'. Como la llegada del valor de x_3 = 1 se produce durante este pequeño intervalo, en la salida aparece un pulso transitorio de valor '1' antes de que ésta adopte el valor permanente de '0'. Puede deducirse fácilmente que para diferentes señales de entrada en el circuito Glitch-PUF, tanto los valores como los retardos de las diferentes señales de entrada (x_1, x_2, x_3) serían diferentes. Como consecuencia, se obtiene una pluralidad de pares pregunta-respuesta unívocos donde la pregunta está formada por el conjunto de señales de entrada al circuito Glitch-PUF y respuesta es la configuración de los diferentes pulsos transitorios que aparecen en la salida. Además, si bien en este ejemplo sencillo únicamente se produce un único pulso transitorio, es necesario tener en cuenta que para circuitos más complejos la respuesta transitoria realmente incluye un tren de pulsos transitorios de diferentes duraciones y retardos que corresponden de manera unívoca a cada pregunta particular.

Un inconveniente de los circuitos Glitch-PUF es que la duración de los pulsos transitorios es arbitrariamente pequeña, lo que puede hacerlos eventualmente difíciles de detectar. En efecto, la señal de salida del circuito Glitch-PUF se detecta a través de un muestreo de acuerdo con una determinada frecuencia de muestreo proporcionada por un reloj. Cuando un pulso en la salida y es muy estrecho, puede ocurrir que la frecuencia de muestreo no sea lo suficientemente alta como para detectarlo. Esta situación se muestra en la Fig. 3c, donde se supone que el valor de la salida se muestrea en cada flanco de subida de unos pulsos de un reloj CLK. Como se puede apreciar, un pulso en la señal de salida como el que aparece en esta figura no sería detectado.

Para solucionar este problema, se han propuesto diversas soluciones. Algunas de ellas están basadas en incrementar la frecuencia de muestreo de la respuesta del circuito Glitch-PUF, por ejemplo utilizando una pluralidad de señales de reloj desfasadas escalonadamente unas con respecto a otras. Otra solución se propone en el documento de D. Suzuki et al "*The glitch PUF: a new delay-PUF architecture exploiting glitch shapes*", Proceedings of the 12th international conference on Cryptographic hardawre and embedded systems (CHES'10), Springer-Verlag, Berlin, Heidelberg, 366-382. Este documento describe un

circuito Glich-PUF cuya salida es desfasada un pequeño período y muestreada con el mismo reloj. La Fig. 4 muestra un ejemplo del esquema descrito por Suzuki.

Un problema adicional de los circuitos Glitch-PUF actualmente conocidos está relacionado con las condiciones cambiantes del entorno, lo que hace que la repetitividad sea baja.

DESCRIPCIÓN DE LA INVENCIÓN

La presente invención resuelve los problemas anteriores gracias a una nueva arquitectura en la que las salidas de dos circuitos generadores de pulsos transitorios, idénticos excepto por las diferencias inherentes al proceso de fabricación y en los que se ha introducido una determinada señal simultáneamente, se introducen en un denominado circuito árbitro. El circuito árbitro está configurado para determinar cuál de dos pulsos emitidos por los dos circuitos generadores ha llegado antes y para emitir una correspondiente señal de salida. Por ejemplo, si ha llegado antes el pulso de uno de los circuitos generadores de pulsos transitorios, el circuito árbitro emite un “1”, mientras que si ha llegado antes el pulso del otro circuito generador de pulsos transitorios, el circuito árbitro emite un “0”. De ese modo, para cada pulso individual producido como respuesta a una determinada señal “*pregunta*” formada por varios bits que se introduce en dichos circuitos generadores de pulsos transitorios, el árbitro emite un pulso de valor “1” o “0”.

Es decir, para cada señal “*pregunta*” de varios bits introducida simultáneamente en los dos circuitos generadores de pulsos transitorios, la salida de cada uno de dichos circuitos producirá un tren de pulsos durante un período de tiempo transitorio hasta que dicha salida queda estabilizada. Puesto que los dos circuitos generadores de pulsos transitorios son esencialmente idénticos, estas señales de salida estarán formadas por parejas de pulsos casi simultáneos en ambos circuitos. Consecuentemente, la señal emitida por el circuito árbitro también estará formada por un tren de pulsos de valor “1” o “0” que indican qué pulso concreto de cada pareja de pulsos del tren de pulsos de respuesta de dichos circuitos llegó antes al circuito árbitro.

De ese modo, cada “*pregunta*” formada por varios bits introducida en los circuitos generadores de pulsos transitorios produce la generación de al menos un tren de pulsos de salida del circuito árbitro que conforma una “*respuesta*” formada por varios bits, donde la señal “*respuesta*” está relacionada de manera unívoca con cada señal “*pregunta*”. Nótese que, en este contexto, cada circuito generador de pulsos transitorios puede emitir una respuesta formada por uno o por varios bits. Es más, en el segundo caso, cada circuito

generador de pulsos transitorios puede estar formado por una pluralidad de bus-circuitos generadores de pulsos transitorios, cada uno de los cuales emite una respuesta de un bit, de modo que la respuesta del circuito generador de pulsos transitorios sean varios bits. El propio circuito árbitro puede incluir además medios de almacenamiento de la señal "*respuesta*".

Una importante ventaja de este dispositivo es que es resistente a variaciones en las condiciones del entorno de operación. En efecto, es conocido que variaciones en las condiciones de operación, como por ejemplo la temperatura, pueden provocar variaciones en los retardos de los diferentes transistores que conforman un circuito generador de pulsos transitorios. Como consecuencia, pueden variar las características de las señales de salida de dicho circuito en el sentido de que puede variar la anchura de los pulsos o su ubicación temporal. Sin embargo, las variaciones provocadas por las condiciones de operación son esencialmente iguales en dos circuitos iguales. Gracias al funcionamiento diferencial del presente dispositivo, que está basado en la comparación de las señales de salida de dos circuitos idénticos, se consigue que los resultados obtenidos sean independientes de las condiciones del entorno de operación.

Según un primer aspecto de la presente invención, se describe un dispositivo para la identificación unívoca de un circuito integrado que comprende fundamentalmente un primer circuito generador de pulsos transitorios, un segundo circuito generador de pulsos transitorios, y un circuito árbitro. A continuación, se describen dichos elementos con mayor detalle:

a) Primer circuito generador de pulsos transitorios

Se trata de un circuito generador de pulsos transitorios que tiene una entrada de primer circuito de varios bits y una salida de primer circuito. Como se ha comentado, la salida puede ser de un bit o bien de varios bits. En el segundo caso, este primer circuito puede estar formado por una pluralidad de sub-circuitos generadores de pulsos transitorios, cada uno de los cuales emite una respuesta de un bit.

Un circuito generador de pulsos transitorios es un circuito que consiste normalmente en una función lógica combinacional que, para maximizar el número de pulsos transitorios generados, presenta un elevado número de caminos distintos de propagación. Además, es deseable la interconexión

de caminos para aumentar la complejidad y evitar así ataques predictivos.

b) Segundo circuito generador de pulsos transitorios

Se trata también de un circuito generador de pulsos transitorios que tiene una entrada de segundo circuito de varios bits y una salida de segundo circuito. Similarmente, la salida puede ser de un bit o bien de varios bits. En el segundo caso, este segundo circuito también puede estar formado por una pluralidad de sub-circuitos generadores de pulsos transitorios, cada uno de los cuales emite una respuesta de un bit.

El primer circuito y el segundo circuito son idénticos excepto por las diferencias inherentes al proceso de fabricación. Estas diferencias, como se ha comentado con anterioridad en este documento, provocan que los retardos en los diferentes elementos que componen los circuitos presenten pequeñas diferencias que son únicas e inclonables.

La entrada de primer circuito y la entrada de segundo circuito pueden estar configuradas para permitir la introducción de una misma señal "*pregunta*" formada por varios bits de manera simultánea en ambas. Por ejemplo, la entrada de primer circuito puede estar conectada a la entrada de segundo circuito. De ese modo, el dispositivo en conjunto tendría una única entrada a través de la cual se introduciría la señal "*pregunta*", la cual se transmitiría simultáneamente a las respectivas entradas de primer circuito y de segundo circuito. Esto, sin embargo, no es limitante y sería posible que la entrada de primer circuito y la entrada de segundo circuito no estuvieran conectadas.

c) Circuito árbitro

El circuito árbitro tiene unas primera y segunda entradas de circuito árbitro, respectivamente conectadas a la salida del primer circuito generador de pulsos transitorios y a la salida del segundo circuito generador de pulsos transitorios, y una salida de circuito árbitro. Estas primera y segunda entradas de circuito árbitro podrán ser de uno o de varios bits, dependiendo del tipo de circuitos generadores de pulsos transitorios elegidos. El circuito árbitro está configurado para determinar si cada pulso

de respuesta a una señal de entrada "*pregunta*" introducida simultáneamente en la entrada de primer circuito y en la entrada de segundo circuito llega antes a la salida de primer circuito o a la salida de segundo circuito y para emitir un pulso de salida en función de ello a través de la salida de circuito árbitro.

Con esta configuración, para cada señal "*pregunta*" formada por varios bits introducida simultáneamente en la entrada de primer circuito y la entrada de segundo circuito, las diferencias entre el primer y segundo circuitos inherentes al proceso de fabricación provocan diferencias en la temporización de los pulsos obtenidos respectivamente en la salida de primer circuito y la salida de segundo circuito, de manera que si el flanco de subida de un pulso aparece antes en la salida de primer circuito el circuito árbitro emite un '1', mientras que si el flanco de subida de un pulso aparece antes en la salida de segundo circuito el circuito árbitro emite un '0', obteniéndose en la salida de circuito árbitro una señal de salida que conforma una señal "*respuesta*" unívoca. Es decir, para cada señal "*pregunta*" formada por varios bits se obtiene una señal "*respuesta*" también formada por varios bits y unívocamente relacionada con aquella. De ese modo, para un número elevado de señales "*pregunta*" diferentes se obtendrá un correspondiente número de señales "*respuesta*" correspondientes y unívocas, lo que permite identificar de manera inequívoca el dispositivo de la invención.

Por tanto, este circuito resuelve los problemas anteriores, emitiendo una señal "*respuesta*" unívocamente relacionada con cada señal "*pregunta*". El circuito árbitro puede implementarse de diferentes modos siempre que sea capaz de determinar cuál de los pulsos de entrada llega antes y de emitir un pulso de salida en función de ello.

En una realización preferida de la invención, el circuito árbitro puede ser simplemente un registro de desplazamiento. A continuación se describe esta realización preferida.

c1) Registro de desplazamiento

El registro de desplazamiento tiene una entrada de datos que constituye la primera entrada de circuito árbitro, una entrada de reloj que constituye la segunda entrada de circuito árbitro, y una salida de registro de

desplazamiento que constituye la salida de circuito árbitro. De este modo, el registro de desplazamiento captará la señal presente en la salida de primer circuito en aquellos momentos en que se produzca un flanco de subida en la señal presente en la salida de segundo circuito. El funcionamiento del registro de desplazamiento en este contexto se describirá con mayor detalle más adelante en este documento con ayuda de las figuras adjuntas.

Con esta configuración, para cada señal "*pregunta*" de varios bits introducida simultáneamente en la entrada de primer circuito y la entrada de segundo circuito, si el flanco de subida de un pulso aparece antes en la salida de primer circuito el primer biestable del registro de desplazamiento recoge un '1', mientras que si el flanco de subida de un pulso aparece antes en la salida de segundo circuito el primer biestable del registro de desplazamiento recoge un '0'. Como consecuencia, a la salida del registro de desplazamiento se obtiene una señal de salida que constituye una señal "*respuesta*" unívoca para cada "*pregunta*". La pluralidad de pulsos de salida obtenidos en respuesta a una señal "*pregunta*" se transmite por el registro de desplazamiento y se recoge a la salida del mismo.

En otra realización preferida alternativa a la anterior, el circuito árbitro puede ser un circuito basado en un circuito conocido denominado circuito C-element. Un circuito C-element es un dispositivo digital ampliamente utilizado en circuitos asíncronos. El funcionamiento de un circuito C-element de 2 entradas (x_1,x_2) como el utilizado en esta invención viene descrito por la siguiente ecuación: $y_n=x_1*x_2+(x_1+x_2)*y_{n-1.}$ A modo de ejemplo, se puede mencionar además como referencia el documento de S.L. Lu, "*Improved design of CMOS multiple-input Muller-C-elements*", Electronic Letters, Pag.1680-1682, Vol.29, Nº19, 16 de Septiembre de 1993, que describe cómo diseñar un circuito C-element y sus características principales.

c2) Circuito basado en C-element

El circuito basado en C-element comprende un biestable de tipo RS, un registro de desplazamiento formado por biestables tipo D, y un circuito C-element de dos entradas. La entrada R del biestable RS constituye la primera entrada de circuito árbitro y la entrada S del biestable RS constituye la segunda entrada de circuito árbitro, y la salida del biestable RS está conectada a la entrada de datos del registro de desplazamiento.

Por otra parte, las dos entradas del circuito C-element están conectadas a las dos entradas de circuito árbitro, y la salida del circuito C-element está conectadas a las entradas de reloj del biestable RS y del registro de desplazamiento. Por último, la salida del registro de desplazamiento constituye la salida de circuito árbitro.

En este circuito árbitro, el biestable RS y los biestables D que conforman el registro de desplazamiento son usados en este circuito según una configuración maestro-esclavo para capturar los pulsos transitorios y enviar la señal de salida.

En una realización preferida de la invención, el dispositivo comprende además un medio de post-procesado para eliminar de la señal "*respuesta*" obtenida en la salida del circuito árbitro aquellos bits correspondientes a pulsos afectados por meta-estabilidad.

d) Un módulo de post-procesado

El módulo de post-procesado está conectado a la salida de primer circuito, a la salida de segundo circuito, y a la salida de circuito árbitro, y está configurado para detectar pulsos de la señal de salida de primer circuito y la señal de salida de segundo circuito cuya distancia temporal en los flancos de subida esté por debajo de un valor umbral y para eliminar de la señal "*respuesta*" recibida de la salida de circuito árbitro los bits correspondientes a dichos pulsos. La salida del módulo de post-procesado es por tanto una señal "*respuesta optimizada*" donde se ha eliminado toda aleatoriedad causada por bits procedentes de pulsos con meta-estabilidad.

En efecto, dentro de los correspondientes trenes de pulsos obtenidos como señal de respuesta de los circuitos generadores de pulsos transitorios a la señal de entrada "*pregunta*", pulsos cuya distancia temporal en los flancos de subida esté por debajo del valor umbral son pulsos afectados por meta-estabilidad en el sentido de que, al ser los flancos de subida casi simultáneos, puede ocurrir que en algunos casos el circuito árbitro considere que ha llegado antes el flanco de subida de la salida de primer circuito y en otros casos considere que ha llegado antes el flanco de subida de la salida de segundo circuito. Como consecuencia, se produciría una incongruencia en el correspondiente bit de la señal "*respuesta*" emitida

por el circuito árbitro, que alternaría entre ‘1’ y ‘0’ aleatoriamente a pesar de que la pregunta fuese la misma en todos los casos. Esto no es admisible en este contexto, y por tanto el módulo de post-procesado descrito detecta flancos de subida de pulsos de la salida de primer circuito y la salida de segundo circuito que están excesivamente cercanos y eliminan el bit correspondiente a ese pulso de la señal “*respuesta*”. De este modo, en esta realización particular se genera una señal “*respuesta optimizada*”.

Preferentemente, la detección de pulsos de la salida de primer circuito y la salida de segundo circuito cuya distancia temporal en los flancos de subida esté por debajo de un valor umbral se realiza por medio de un muestreador multifase configurado para muestrear las señales recibidas a través de la salida de primer circuito y la salida de segundo circuito

En otra realización preferida de la invención, el módulo de post-procesado comprende además un contador de flancos configurado para contar los flancos recibidos a través de la salida de primer circuito y la salida de segundo circuito, determinándose que la señal en la salida de circuito árbitro solo es válida si el número de flancos es el mismo. De ese modo se eliminan además de la señal “*respuesta*” pulsos espurios generados por las condiciones cambiantes del entorno de operación.

En otra realización preferida de la invención, el módulo de post-procesado comprende además un comparador iterativo de respuesta configurado para comparar una pluralidad de señales “*respuesta*” obtenidas a partir de la misma señal “*pregunta*”, repitiéndose la “*pregunta*” en caso de que el número de señales “*respuesta*” iguales sea menor que un valor umbral prestablecido.

En otra realización preferida de la invención, el módulo de post-procesado comprende además un circuito de compactación configurado para calcular la salida final del módulo de post-procesado una vez se ha dado como válida la respuesta generada. Para ello, se pueden utilizar circuitos compactadores tales como un MISR (Multiple Input Signature Register) o LFSR (Linear Feedback Shift Register).

Según un segundo aspecto de la invención, se describe un procedimiento para la identificación unívoca de un circuito integrado configurado para ser llevado a cabo por el dispositivo descrito anteriormente. Este procedimiento comprende los siguientes pasos:

1) Introducir simultáneamente una misma señal “*pregunta*” en una entrada de varios bits de un primer circuito generador de pulsos transitorios que tiene una salida de primer circuito de un bit, y en una entrada de varios bits de un segundo circuito generador de pulsos transitorios que tiene una salida de segundo circuito de un bit, donde el primer circuito y el segundo circuito son idénticos excepto por las diferencias inherentes al proceso de fabricación;

2) Introducir la salida de primer circuito en una primera entrada de un circuito árbitro y la salida de segundo circuito en la segunda entrada del circuito árbitro; y

3) Obtener en una salida del circuito árbitro una señal de salida que constituye una señal “*respuesta*” unívoca para dicha señal “*pregunta*” introducida simultáneamente en la entrada de primer circuito y la entrada de segundo circuito, debido a las diferencias entre el primer y segundo circuitos inherentes al proceso de fabricación que provocan diferencias en la temporización de los pulsos obtenidos respectivamente en la salida de primer circuito y la salida de segundo circuito, de manera que si el flanco de subida de un pulso aparece antes en la salida de primer circuito, el circuito árbitro emite un ‘1’, mientras que si el flanco de subida de un pulso aparece antes en la salida de segundo circuito, el circuito árbitro recoge un ‘0’.

En una realización preferida de la invención, el circuito árbitro es un registro de desplazamiento que tiene una entrada de datos que constituye la primera entrada de circuito árbitro, una entrada de reloj que constituye la segunda entrada de circuito árbitro, y una salida de registro de desplazamiento que constituye la salida de circuito árbitro. De ese modo, para cada señal “*pregunta*”, si el flanco de subida de un pulso aparece antes en la salida de primer circuito un primer biestable del registro de desplazamiento recoge un ‘1’, mientras que si el flanco de subida de un pulso aparece antes en la salida de segundo circuito el primer biestable del registro de desplazamiento recoge un ‘0’, obteniéndose en la salida de registro de desplazamiento una señal de salida que conforma una señal “*respuesta*” unívoca.

En otra realización preferida de la invención el procedimiento comprende además los pasos de detectar pulsos de la salida de primer circuito y la salida de segundo circuito cuya distancia temporal en los flancos de subida esté por debajo de un valor umbral, y eliminar de la señal “*respuesta*” recibida en la salida de circuito árbitro los bits correspondientes a dichos

pulsos.

En otra realización preferida de la invención, el procedimiento comprende además los pasos de contar los flancos de los pulsos recibidos a través de la salida de primer circuito y la salida de segundo circuito, y determinar que la señal en la salida de circuito árbitro es válida solo si el número de flancos es el mismo.

En otra realización preferida de la invención, el procedimiento comprende además el paso de comparar una pluralidad de señales "*respuesta*" obtenidas a partir de la misma señal "*pregunta*", repitiéndose la "*pregunta*" en caso de que el número de señales "*respuesta*" iguales sea menor que un valor umbral prestablecido.

En otra realización preferida de la invención, el procedimiento comprende además el paso de calcular la salida final de dicho módulo de post-procesado una vez se ha dado como válida la respuesta generada. Esto se puede hacer, por ejemplo, utilizando un módulo de compactación tal como un MISR o LFSR.

BREVE DESCRIPCIÓN DE LAS FIGURAS

La Fig. 1 muestra un ejemplo de circuito PUF de acuerdo con la técnica anterior.

La Fig. 2 muestra un ejemplo de circuito sencillo que ilustra los principios de los Glitch-PUF.

Las Figs. 3a-3c muestran varios diagramas temporales que ilustran el funcionamiento del circuito de la Fig. 2.

La Fig. 4 muestra un ejemplo de circuito Glitch-PUF de acuerdo con la técnica anterior.

La Fig. 5 muestra un ejemplo de dispositivo de acuerdo con la presente invención.

La Fig. 6 muestra un ejemplo de dispositivo según la presente invención donde el circuito árbitro es un registro de desplazamiento.

La Fig. 7 muestra un ejemplo de dispositivo según la presente invención donde el circuito árbitro es un circuito que incluye un circuito C-element.

La Fig. 8 muestra un ejemplo de circuito generador de pulsos transitorios según la presente

invención.

La Fig. 9 muestra un diagrama temporal que ilustra el funcionamiento del dispositivo de la presente invención cuando el circuito árbitro es un registro de desplazamiento.

La Fig. 10 muestra un diagrama temporal que ilustra el funcionamiento del dispositivo de la presente invención cuando el circuito árbitro es un circuito basado en C-element.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

Se describe a continuación un ejemplo particular de acuerdo con la presente invención donde se aprecian los diferentes elementos que componen el sistema y los diferentes pasos del procedimiento propuesto.

La Fig. 5 muestra un ejemplo de dispositivo (1) de acuerdo con la presente invención donde se aprecian las diferentes partes que lo componen. Concretamente, el dispositivo (1) comprende un primer circuito (2) generador de pulsos transitorios que tiene una entrada (2e) de primer circuito de n bits y una salida (2s) de primer circuito, y un segundo circuito (3) generador de pulsos transitorios que tiene una entrada (3e) de segundo circuito de n bits y una salida (3s) de segundo circuito. En este ejemplo, las dos entradas (2e, 3e) están conectadas entre sí.

Por motivos de simplicidad de la descripción, en este ejemplo particular las salidas (2s, 3s) de los primer y segundo circuitos (2, 3) son de un único bit, y en consecuencia las entradas (4e1, 4e2) del circuito (4) árbitro son también de un único bit. Sin embargo, es fácil extrapolar este ejemplo a una configuración en que dichas salidas (2s, 3s) tengan varios bits, y por tanto también las entradas (4e1, 4e2) tengan varios bits. En ese caso, el circuito árbitro (4) incluiría los elementos necesarios para gestionar la comparación entre los pulsos transitorios que se producen en cada pareja de bits correspondientes del primer y segundo circuitos (2, 3), de modo que a la salida del circuito (4) árbitro se obtendrían varias señales "*respuesta*" para cada señal "*pregunta*".

Los circuitos (2, 3) generadores de pulsos transitorios son conocidos en la técnica. Por ejemplo, puede utilizarse una función lógica combinacional de n bits de entrada y 1 bit de salida. La Fig. 8 muestra un ejemplo de circuito multiplicador de este tipo en el que el bit más significativo (dependiente de todas las etapas) se toma como salida. La señal de entrada está formada por la palabra de 8 bits (A_0, A_1, A_2, A_3, B_0, B_1, B_2, B_3) y la salida está

formada por palabra de 1 bit ‘s’. Ambos circuitos (2, 3) serán idénticos excepto por las minúsculas diferencias inherentes al proceso de fabricación.

La salida (2s) de primer circuito está conectada a una primera entrada (4e1) de un circuito (4) árbitro y la salida (3s) de segundo circuito está conectada a una segunda entrada (4e2) del circuito (4) árbitro. Como se ha comentado, el circuito (4) árbitro está configurado de modo que emite un ‘1’ cuando el flanco de subida de un pulso aparece antes en la primera salida (2s), y recogerá un ‘0’ cuando el flanco de subida de un pulso aparece antes en la segunda salida (3s).

Para describir esto con más detalle, la Fig. 6 muestra un ejemplo de dispositivo (1) según la invención donde el circuito (4) árbitro es un registro de desplazamiento. En este caso, la salida (2s) de primer circuito está conectada a la entrada (4e1) de datos del registro (4) de desplazamiento, y la salida (3s) de segundo circuito está conectada a la entrada (4e2) de reloj del registro (4) de desplazamiento.

El diagrama de la Fig. 9 muestra claramente el funcionamiento del dispositivo mostrado en la Fig. 6. En la Fig. 9 se representa la señal de la salida (2s) de primer circuito, la señal de la salida (3s) de segundo circuito, y los datos que se van almacenando en el registro (4) de desplazamiento y que constituyen señal “*respuesta*” que posteriormente se emite a través de la salida (4s) de registro de desplazamiento. El diagrama muestra un primer pulso cuyo flanco de subida llega más tarde a la salida (3s) de segundo circuito. Esta salida (3s) de segundo circuito constituye la entrada (4e2) de reloj del registro (4) de desplazamiento, y por tanto provoca la adquisición del dato que en ese momento esté presente en la salida (2s) de primer circuito. Puesto que la salida (2s) de primer circuito ya ha adoptado el valor ‘1’ cuando llega el flanco de subida de este primer pulso a la salida (3s) de segundo circuito, el primer bit que adquiere el registro (4) de desplazamiento es un ‘1’. Cuando llega el flanco de subida del segundo pulso a la salida (3s) de segundo circuito, la señal de la salida (2s) de primer circuito también ha adoptado ya el valor ‘1’, y por tanto el registro (4) de desplazamiento vuelve a adquirir un ‘1’. Sin embargo, cuando llega el flanco de subida del tercer pulso a la salida (3s) de segundo circuito, la señal de la salida (2s) de primer circuito aún está en el valor ‘0’. Es decir, el tercer pulso llega antes a la salida (3s) de segundo circuito. Por tanto, en este caso el registro (4) de desplazamiento adquiere un ‘0’. Este proceso continua todo el tiempo que dura la respuesta transitoria a la pregunta que se ha introducido en el dispositivo, obteniéndose así una señal “*respuesta*” de varios bits a la salida (4s) del registro (4) de desplazamiento que está unívocamente relacionada con la “*pregunta*” realizada. Se puede realizar una pluralidad de “*preguntas*” diferentes para

obtener una correspondiente pluralidad de "*respuestas*" unívocamente relacionadas, lo que permite identificar de manera inequívoca un dispositivo particular.

Ahora bien, como se mencionó con anterioridad en este documento, existen pulsos que presentan meta-estabilidad que pueden introducir incongruencias en los resultados obtenidos. Por ejemplo, el cuarto pulso representado en la Fig. 7 llega de manera simultánea a la salida (2s) de primer circuito y a la salida (3s) de segundo circuito. Como consecuencia, puede ocurrir que algunas veces el registro (4) de desplazamiento considere que ha llegado antes el flanco de subida del pulso en la salida (2s) de primer circuito y adquiera un '1', y otras veces considere que ha llegado antes el flanco de subida del pulso en la salida (3s) de segundo circuito y adquiera un '0'. Es decir, para la misma "*pregunta*" existirían en este ejemplo dos "*respuestas*" diferentes.

Para evitar esto, el circuito de que se muestra en el ejemplo de la Fig. 5 comprende un módulo (7) de post-procesado destinado a eliminar de la "*respuesta*" obtenida a la salida (4s) del registro (4) de desplazamiento los bits correspondientes a pulsos con meta-estabilidad. El módulo (7) de post-procesado está conectado a la salida (2s) de primer circuito, a la salida (3s) de segundo circuito, y a la salida (4s) del registro de desplazamiento. Este módulo (7) de post-procesado recibe las señales de la salida (2s) de primer circuito y de la salida (3s) de segundo circuito y busca en ambas pulsos correspondientes cuyos flancos de subida sean casi simultáneos. Por ejemplo, se puede considerar que los flancos de subida de un determinado pulso de la señal de la salida (2s) de primer circuito y la señal de la salida (3s) de segundo circuito son simultáneos cuando están separados por menos de un número de nanosegundos determinado. Cuando el módulo (7) de post-procesado encuentra un pulso de este tipo, busca en la señal obtenida del registro (4) de desplazamiento el bit correspondiente a este pulso y lo elimina. Se obtiene así a la salida (7s) del módulo (7) de post-procesado una señal "*respuesta optimizada*" donde los bits correspondientes a pulsos con meta-estabilidad han sido eliminados.

La Fig. 7 muestra otro ejemplo de dispositivo (1) según la invención donde el circuito (4) árbitro está implementado basándose en un circuito C-element, un biestable tipo RS y un registro de desplazamiento formado por biestables tipo D. El circuito C-element será el encargado de generar las señales de reloj para los 2 biestables que funcionan en modo maestro-esclavo. Específicamente, el biestable RS actualizará su salida cuando las entradas (4e1,4e2) del C-element valgan 0 y el estado anterior del C-element fuera 1. Por el contrario, el registro de desplazamiento formado por biestables D actualizará su salida cuando las entradas (4e1,4e2) del C-element valgan 1 y el estado anterior del C-element fuera 1. Con

esta implementación, se consigue reducir la metaestabilidad y filtrar los pulsos espurios aparecidos por variaciones en el entorno de operación.

La Fig. 10 muestra una diagrama temporal que ilustra el funcionamiento del dispositivo (1) de la Fig. 7. En esta figura se pueden distinguir 4 casos hasta que se alcanza el régimen permanente, los cuatro casos se marcan en la parte superior del diagrama.

En el primer caso, un pulso transitorio es propagado por el primer circuito (2) generador de pulsos transitorios hasta alcanzar el árbitro (4). Se ve como el pulso de la primera entrada (4e1) llega y termina antes que el pulso de la entrada (4e2) correspondiente al segundo circuito (3) generador de pulsos transitorios. En este caso, cuando ambas entradas están a 1, el circuito C-element hace que el registro de desplazamiento guarde el valor previo almacenado en el biestable RS, en este caso un ‘0’. Cuando ambas entradas (4e1, 4e2) vuelven a 0, el circuito C-element hace que el biestable RS actualice su valor, en este caso a 1, ya que las entradas del biestable justo antes del flanco de bajada son 01.

En el segundo caso, la situación es la opuesta, es decir, llega y termina antes el pulso de la entrada (4e2) del segundo circuito (3) generador de pulsos transitorios. Por ello, siguiendo un proceso análogo al anterior, el registro de desplazamiento captura el valor previo almacenado en el biestable RS (‘1’) y, en el flanco de bajada generado en el C-element, el biestable RS actualiza su valor, en este caso a ‘0’.E

En el tercer caso, se produce un pulso espurio se produce en la entrada (4e2) sin que ello afecte a la salida final.

Por último, en el cuarto caso, ambos pulsos a través de las señales (4e1, 4e2) llegan a la vez generando un flanco de subida a la salida del circuito C-element que hace que el registro de desplazamiento se actualice con el último valor del biestable RS. Como la entrada (4e2) se ha propagado más rápido que la entrada (4e1), el valor almacenado por el biestable RS en el flanco de bajada del circuito C-element será ‘1’.

REIVINDICACIONES

1. Dispositivo (1) para la identificación unívoca de un circuito integrado, caracterizado por que comprende:

- un primer circuito (2) generador de pulsos transitorios que tiene una entrada (2e) de primer circuito de varios bits y una salida (2s) de primer circuito;

- un segundo circuito (3) generador de pulsos transitorios que tiene una entrada (3e) de segundo circuito de varios bits y una salida (3s) de segundo circuito, donde el primer circuito (2) y el segundo circuito (3) son idénticos excepto por las diferencias inherentes al proceso de fabricación;

- un circuito (4) árbitro que tiene unas primera y segunda entradas (4e1, 4e2) de circuito árbitro, respectivamente conectadas a la salida (2s) de primer circuito y a la salida (3s) de segundo circuito, y una salida (4s) de circuito árbitro, donde el circuito (4) árbitro está configurado para determinar si cada pulso de respuesta a una señal de entrada "*pregunta*" introducida simultáneamente en la entrada (2e) de primer circuito y en la entrada (3e) de segundo circuito llega antes a la salida (2s) de primer circuito o a la salida (3s) de segundo circuito y para emitir un pulso de salida en función de ello a través de la salida (4s) de circuito árbitro,

de modo que, para cada señal "*pregunta*" introducida simultáneamente en la entrada (2e) de primer circuito y la entrada (3e) de segundo circuito, las diferencias entre el primer y segundo circuitos (2, 3) inherentes al proceso de fabricación provocan diferencias en la temporización de los pulsos obtenidos respectivamente en la salida (2s) de primer circuito y la salida (3s) de segundo circuito, de manera que si el flanco de subida de un pulso aparece antes en la salida (2s) de primer circuito el circuito (4) árbitro emite un '1', mientras que si el flanco de subida de un pulso aparece antes en la salida (3s) de segundo circuito el circuito (4) árbitro emite un '0', obteniéndose en la salida (4s) de circuito (4) árbitro una señal de salida que conforma una señal "*respuesta*" unívoca.

2. Dispositivo (1) de acuerdo con la reivindicación 1, donde la salida (2s) del primer circuito (2) generador de pulsos transitorios, la salida (3s) del segundo circuito (3) generador de pulsos transitorios, y las primera y segunda entradas (4e1, 4e2) de circuito árbitro tienen un bit.

3. Dispositivo (1) de acuerdo con la reivindicación 2, donde el circuito (4) árbitro es un registro (4) de desplazamiento que tiene una entrada de datos que constituye la primera entrada (4e1) de circuito árbitro, una entrada de reloj que constituye la segunda entrada (4e2) de circuito árbitro, y una salida de registro de desplazamiento que constituye la salida

(4s) de circuito árbitro, de modo que, para cada señal "*pregunta*", si el flanco de subida de un pulso aparece antes en la salida (2s) de primer circuito un primer biestable del registro (4) de desplazamiento recoge un '1', mientras que si el flanco de subida de un pulso aparece antes en la salida (3s) de segundo circuito el primer biestable del registro (4) de desplazamiento recoge un '0', obteniéndose en la salida (4s) de registro de desplazamiento una señal de salida que conforma una señal "*respuesta*" unívoca.

4. Dispositivo (1) de acuerdo con la reivindicación 2, donde el circuito (4) árbitro es un circuito basado en un circuito C-element que comprende: un biestable de tipo RS, un registro de desplazamiento formado por biestables tipo D, y un circuito C-element de dos entradas, donde la entrada R del biestable RS constituye la primera entrada de circuito árbitro y la entrada S del biestable RS constituye la segunda entrada de circuito árbitro, y donde la salida del biestable RS está conectada a la entrada de datos del registro de desplazamiento, y donde las dos entradas del circuito C-element están conectadas a las dos entradas de circuito árbitro, y donde la salida del circuito C-element está conectada a las entradas de reloj del biestable RS y del registro de desplazamiento, y donde la salida del registro de desplazamiento constituye la salida de circuito árbitro.

5. Dispositivo (1) de acuerdo con cualquiera de las reivindicaciones anteriores, que además comprende un módulo (7) de post-procesado conectado a la salida (2s) de primer circuito, a la salida (3s) de segundo circuito, y a la salida (4s) de circuito (4) árbitro, donde el módulo (7) de post-procesado está configurado para detectar pulsos de la salida (2s) de primer circuito y la salida (3s) de segundo circuito cuya distancia temporal en los flancos de subida esté por debajo de un valor umbral y para eliminar de la señal "*respuesta*" recibida en la salida (4s) de circuito árbitro los bits correspondientes a dichos pulsos.

6. Dispositivo (1) de acuerdo con la reivindicación 5, donde la detección de pulsos de la salida (2s) de primer circuito y la salida (3s) de segundo circuito cuya distancia temporal en los flancos de subida esté por debajo de un valor umbral se realiza por medio de un muestreador multifase configurado para muestrear las señales recibidas a través de la salida (2s) de primer circuito y la salida (3s) de segundo circuito.

7. Dispositivo (1) de acuerdo con cualquiera de las reivindicaciones 5-6, donde el módulo (7) de post-procesado comprende además un contador de flancos configurado para contar los flancos recibidos a través de la salida (2s) de primer circuito y la salida (3s) de segundo circuito, determinándose que la señal en la salida (4s) de circuito árbitro solo es válida si el número de flancos es el mismo.

8. Dispositivo (1) de acuerdo con cualquiera de las reivindicaciones 5-7, donde el módulo (7) de post-procesado comprende además un comparador iterativo de respuesta configurado para comparar una pluralidad de señales "*respuesta*" obtenidas a partir de la misma señal "*pregunta*", repitiéndose la "*pregunta*" en caso de que el número de señales "*respuesta*" iguales sea menor que un valor umbral prestablecido.

9. Dispositivo (1) de acuerdo con cualquiera de las reivindicaciones 5-8, donde el módulo (7) de post-procesado comprende además un circuito de compactación configurado para calcular la salida final de dicho módulo (7) de post-procesado una vez se ha dado como válida la respuesta generada.

10. Procedimiento para la identificación unívoca de un circuito integrado, caracterizado por que comprende los siguientes pasos:

- introducir simultáneamente una misma señal "*pregunta"* en una entrada (2e) de varios bits de un primer circuito (2) generador de pulsos transitorios que tiene una salida (2s) de primer circuito, y en una entrada (3e) de varios bits de un segundo circuito (3) generador de pulsos transitorios que tiene una salida (3s) de segundo circuito, donde el primer circuito (2) y el segundo circuito (3) son idénticos excepto por las diferencias inherentes al proceso de fabricación;
- introducir la salida (2s) de primer circuito en una primera entrada (4e1) de un circuito (4) árbitro y la salida (3s) de segundo circuito en la segunda entrada (4e2) del circuito (4) árbitro; y
- obtener en una salida (4s) del circuito (4) árbitro una señal de salida que constituye una señal "*respuesta*" unívoca para dicha señal "*pregunta*" introducida simultáneamente en la entrada (2e) de primer circuito y la entrada (3e) de segundo circuito, debido a las diferencias entre el primer y segundo circuitos (2, 3) inherentes al proceso de fabricación que provocan diferencias en la temporización de los pulsos obtenidos respectivamente en la salida (2s) de primer circuito y la salida (3s) de segundo circuito, de manera que si el flanco de subida de un pulso aparece antes en la salida (2s) de primer circuito, el circuito (4) árbitro emite un '1', mientras que si el flanco de subida de un pulso aparece antes en la salida (3s) de segundo circuito, el circuito (4) árbitro recoge un '0'.

11. Procedimiento de acuerdo con la reivindicación 10, donde la salida (2s) del primer circuito (2) generador de pulsos transitorios, la salida (3s) del segundo circuito (3) generador de pulsos transitorios, y las primera y segunda entradas (4e1, 4e2) de circuito árbitro tienen

un bit.

12. Procedimiento de acuerdo con la reivindicación 11, donde el circuito (4) árbitro es un registro (4) de desplazamiento que tiene una entrada de datos que constituye la primera entrada (4e1) de circuito árbitro conectada a la salida (2s) de primer circuito, una entrada de reloj que constituye la segunda entrada (4e2) de circuito árbitro conectada a la salida (3s) de segundo circuito, y una salida de registro de desplazamiento que constituye la salida (4s) de circuito árbitro, de modo que, para cada señal "*pregunta*", si el flanco de subida de un pulso aparece antes en la salida (2s) de primer circuito un primer biestable del registro (4) de desplazamiento recoge un '1', mientras que si el flanco de subida de un pulso aparece antes en la salida (3s) de segundo circuito el primer biestable del registro (4) de desplazamiento recoge un '0', obteniéndose en la salida (4s) de registro de desplazamiento una señal de salida que conforma una señal "*respuesta*" unívoca.

13. Procedimiento de acuerdo con cualquiera de las reivindicaciones 10-12, que además comprende los pasos de detectar pulsos de la salida (2s) de primer circuito y la salida (3s) de segundo circuito cuya distancia temporal en los flancos de subida esté por debajo de un valor umbral, y eliminar de la señal "*respuesta*" recibida en la salida (4s) de circuito árbitro los bits correspondientes a dichos pulsos.

14. Procedimiento de acuerdo con cualquiera de las reivindicaciones 10-13, que además comprende los pasos de contar los flancos de los pulsos recibidos a través de la salida (2s) de primer circuito y la salida (3s) de segundo circuito, y determinar que la señal en la salida (4s) de circuito árbitro es válida solo si el número de flancos es el mismo.

15. Procedimiento de acuerdo con cualquiera de las reivindicaciones 10-14, que además comprende el paso de comparar una pluralidad de señales "*respuesta*" obtenidas a partir de la misma señal "*pregunta*", repitiéndose la "*pregunta*" en caso de que el número de señales "*respuesta*" iguales sea menor que un valor umbral prestablecido.

16. Procedimiento de acuerdo con cualquiera de las reivindicaciones 10-15, que además comprende el paso de calcular la salida final de dicho módulo (7) de post-procesado una vez se ha dado como válida la respuesta generada.

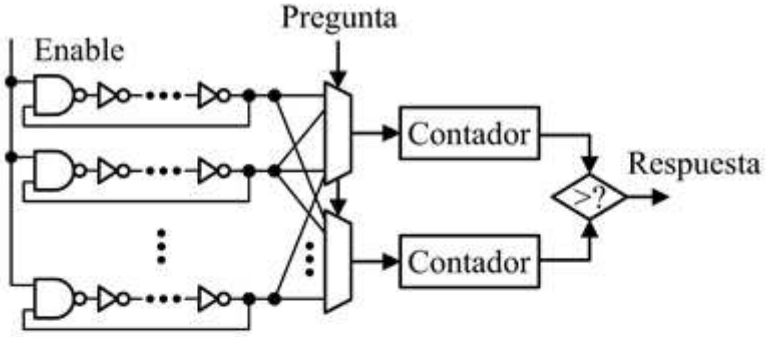

FIG. 1
TÉCNICA ANTERIOR

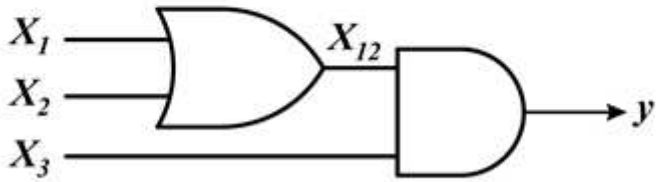

FIG. 2
TÉCNICA ANTERIOR

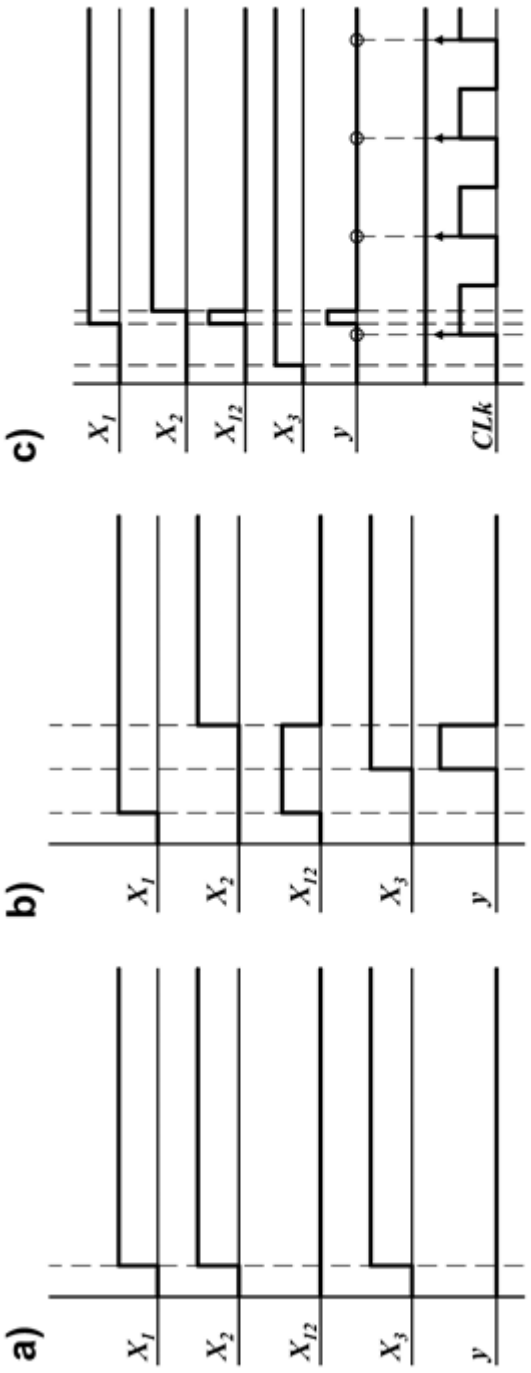

FIG. 3
TÉCNICA ANTERIOR

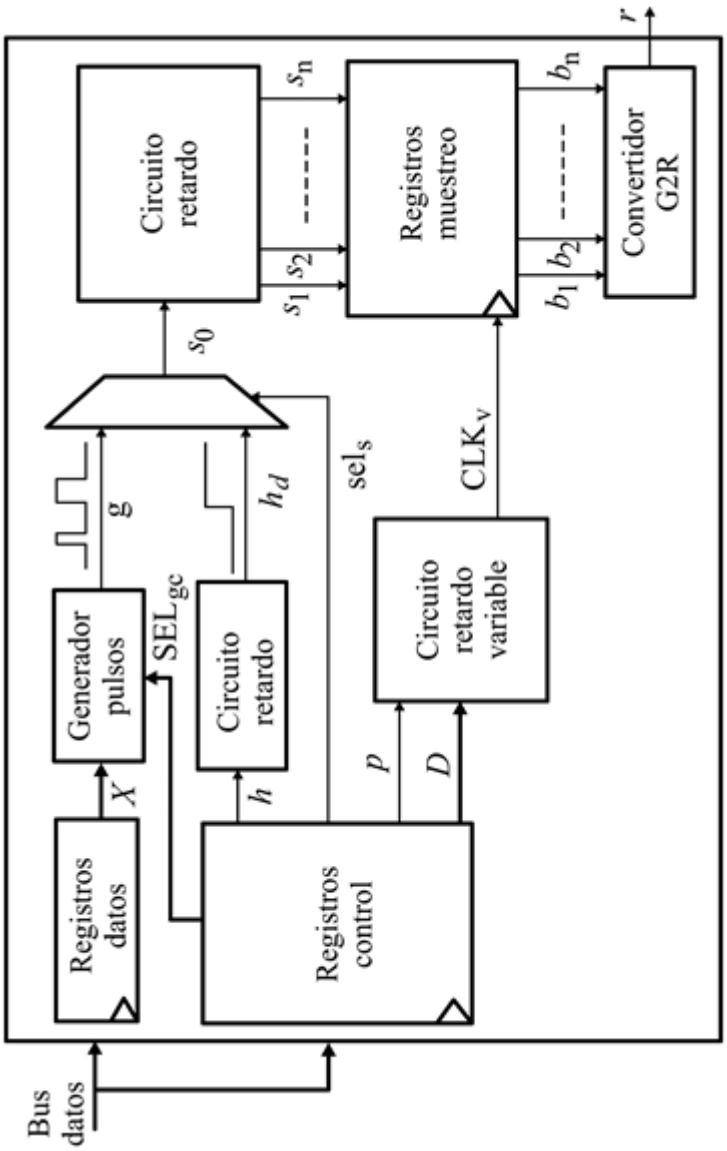

FIG. 4
TÉCNICA ANTERIOR

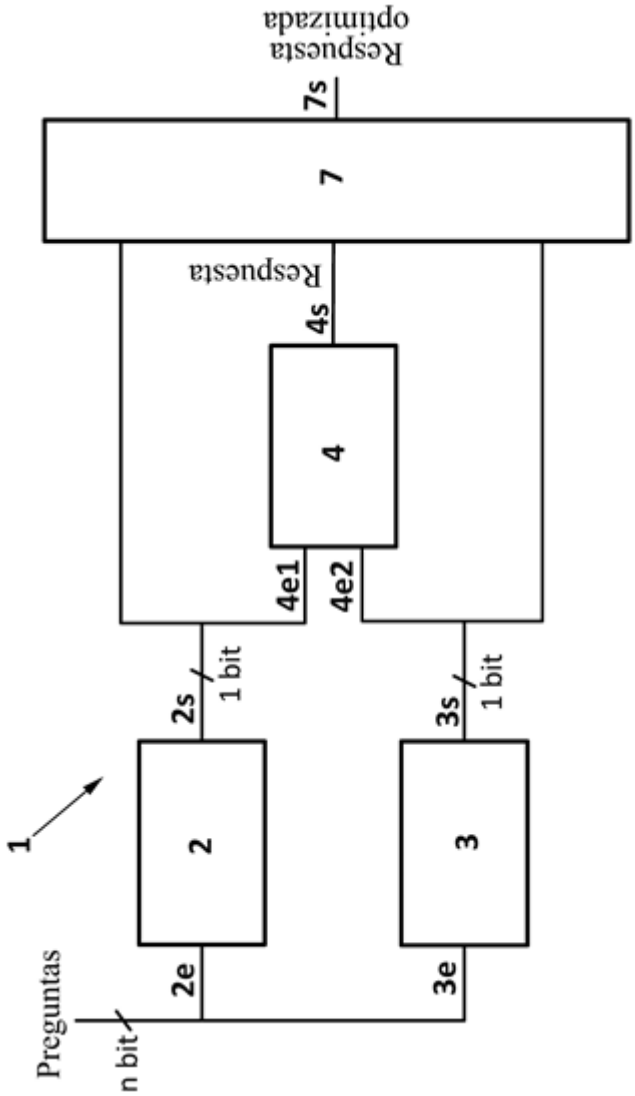
Respuesta optimizada
7s
7
Respuesta
4s
4
4e1
4e2
2s
1 bit
3s
1 bit
1
2
3
2e
3e
Preguntas
n bit

FIG. 5

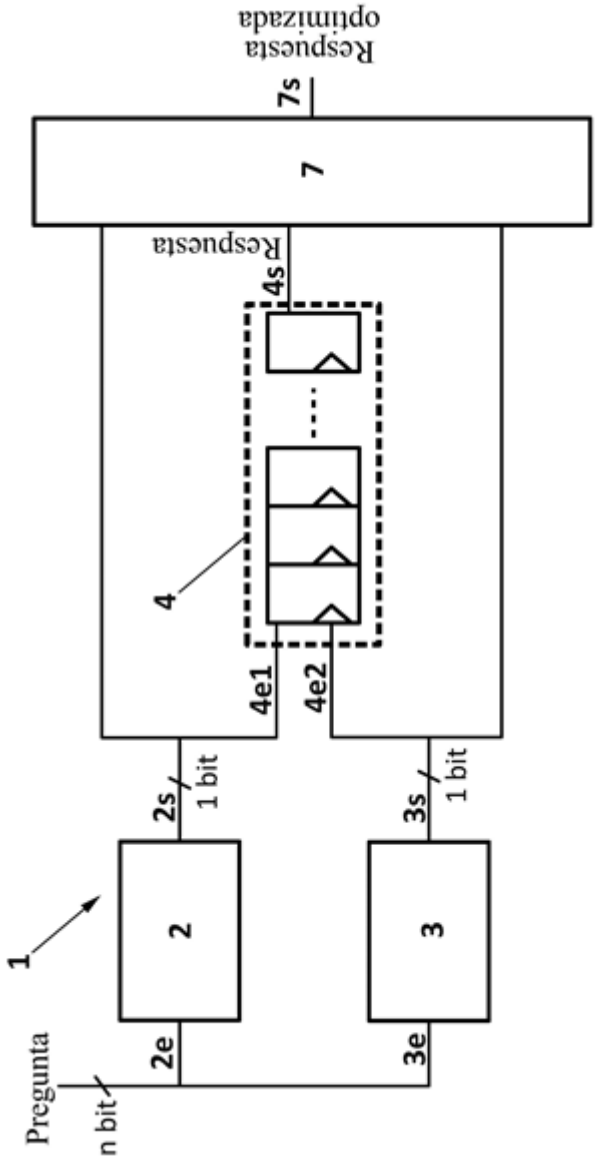
Respuesta optimizada
7s
7
Respuesta
4s
4
4e1
4e2
2s
1 bit
3s
1 bit
1
2
3
2e
3e
Pregunta
n bit

FIG. 6

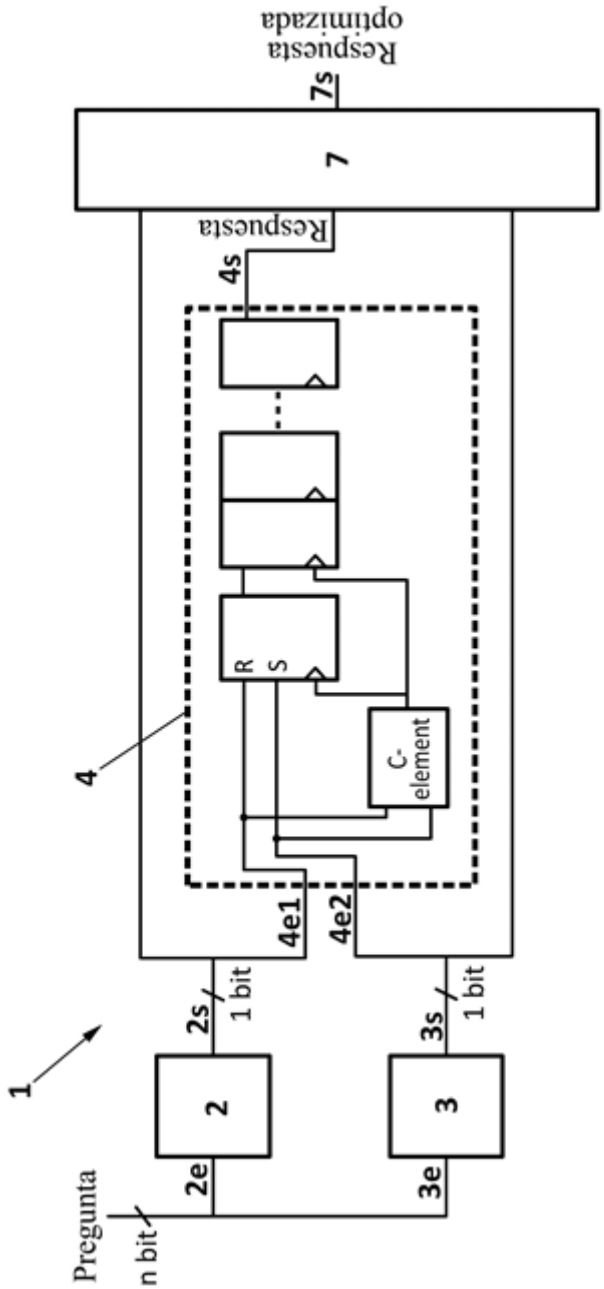
Respuesta optimizada
7s
7
Respuesta
4s
4
R
S
C-element
4e1
4e2
2s
1 bit
3s
1 bit
1
2
3
2e
3e
Pregunta
n bit

FIG. 7

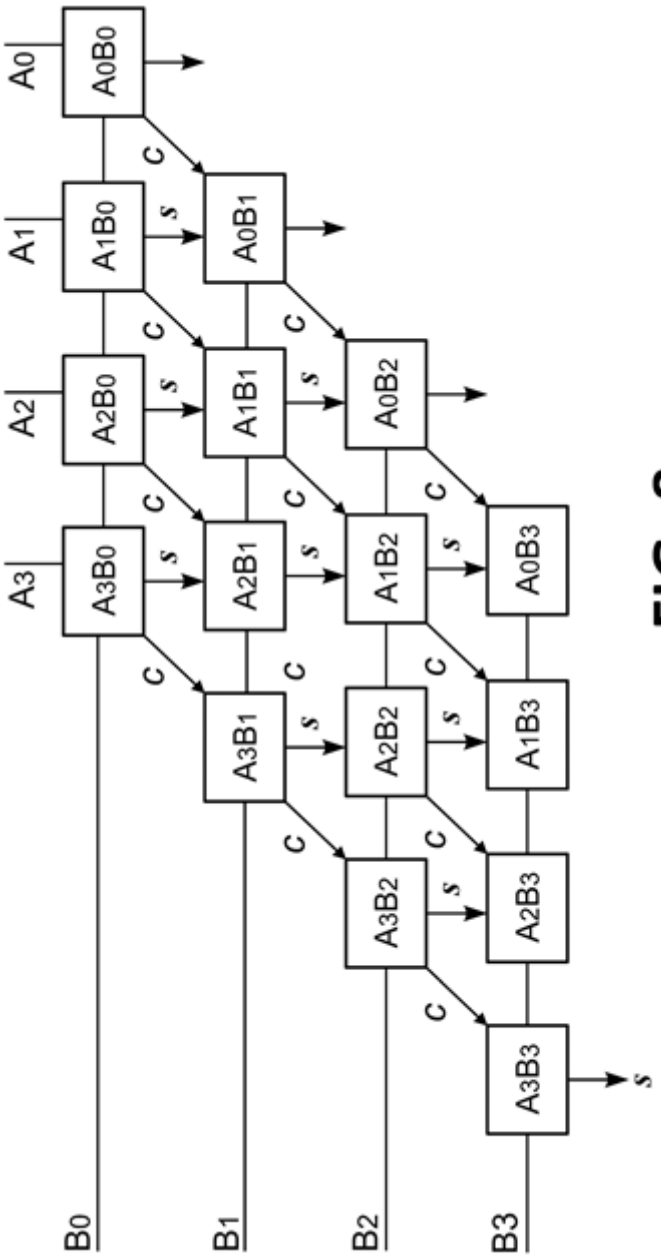
A0
A1
A2
A3
B0
B1
B2
B3
A0B0
A1B0
A0B1
A2B0
A1B1
A0B2
A3B0
A2B1
A1B2
A0B3
A3B1
A2B2
A1B3
A3B2
A2B3
A3B3
C
S

FIG. 8

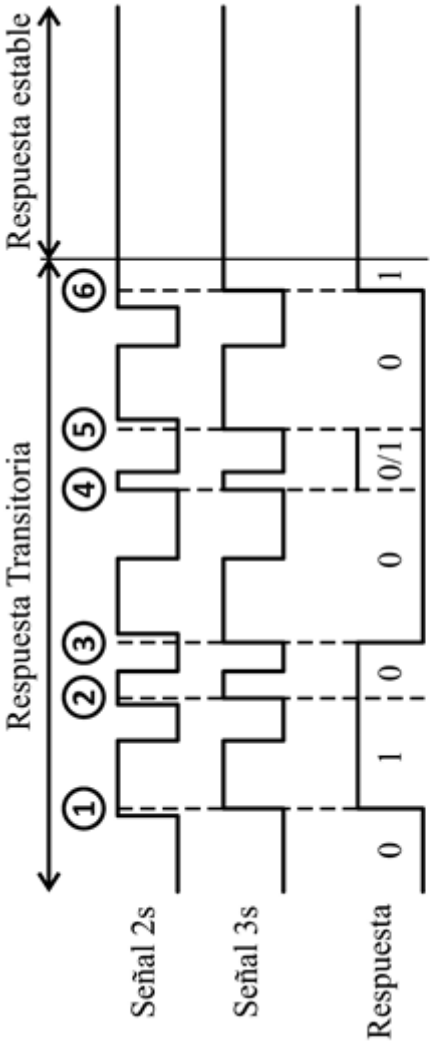
Respuesta estable
Respuesta Transitoria
1
2
3
4
5
6
Señal 2s
Señal 3s
Respuesta
0
1
0
0
0/1
0
1

FIG. 9

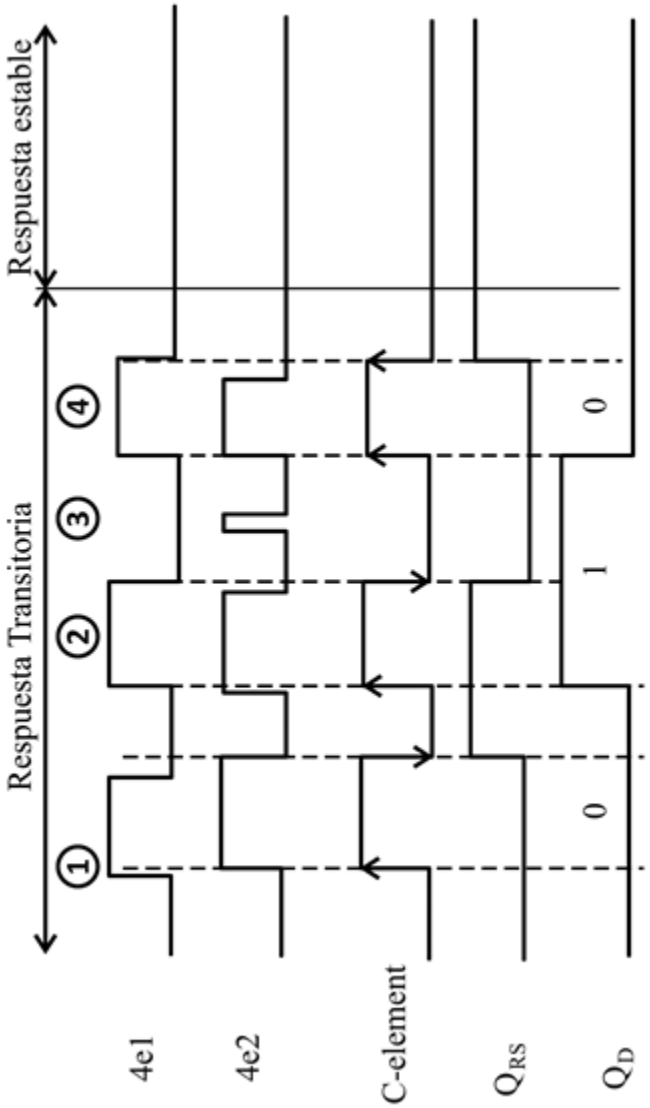
Respuesta estable
Respuesta Transitoria
1
2
3
4
0
1
0
4e1
4e2
C-element
Q_{RS}
Q_D

FIG. 10

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201730535

(22) Fecha de presentación de la solicitud: 31.03.2017

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** Ver Hoja Adicional

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	US 2003204743 A1 (DEVADAS SRINIVAS et al.) 30/10/2003, párrafos [0055,0057,0114-118,0106,0160,0377,0378], figuras 10,11,12,56	1-3,10-12
A		4-9,13-16
A	CN 106470024 A (FREESCALE SEMICONDUCTOR INC) 01/03/2017, resumen, figura 1	4
A	US 2014327468 A1 (PFEIFFER DIRK et al.) 06/11/2014, resumen, párrafo [0047], figura 14	4-9, 13-16
A	EP 2665225 A1 (MITSUBISHI ELECTRIC CORP) 20/11/2013, resumen, párrafos [0015,0035], figuras 9,10	1-16
A	US 2014041040 A1 (POTKONJAK MIODRAG et al.) 06/02/2014, párrafos [0097,0110], figura 10	1-16

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
26.09.2017	F. J. Dominguez Gomez	1/5

CLASIFICACIÓN OBJETO DE LA SOLICITUD

H04L9/32 (2006.01)
H03K3/037 (2006.01)
H03K3/011 (2006.01)
G06F21/44 (2013.01)

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L, H03K, G06F

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, INSPEC, WPI, NPL, IEEE

Fecha de Realización de la Opinión Escrita: 26.09.2017

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	4-9,13-16	**SI**
	Reivindicaciones	1-3,10-12	**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones	4-9,13-16	**SI**
	Reivindicaciones	1-3,10-12	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	US 2003204743 A1 (DEVADAS SRINIVAS et al.)	30.10.2003
D02	CN 106470024 A (FREESCALE SEMICONDUCTOR INC)	01.03.2017
D03	US 2014327468 A1 (PFEIFFER DIRK et al.)	06.11.2014
D04	EP 2665225 A1 (MITSUBISHI ELECTRIC CORP)	20.11.2013
D05	US 2014041040 A1 (POTKONJAK MIODRAG et al.)	06.02.2014

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento del estado de la técnica anterior más próximo al objeto de la solicitud. Este documento afecta a la novedad de algunas reivindicaciones, tal y como se explicará a continuación:

Reivindicaciones independientes

Reivindicación 1

En relación con la reivindicación 1 en el documento D01 se describe, de forma explícita o implícita, lo siguiente (las referencias entre paréntesis se refieren a D01):

Dispositivo (1010, figura 56, párrafos [0377,0388]) para la identificación unívoca de un circuito integrado, que comprende:
- un primer circuito (1012) generador de pulsos transitorios que tiene una entrada de primer circuito de varios bits (b1-128) y una salida de primer circuito;
- un segundo circuito (1014) generador de pulsos transitorios que tiene una entrada de segundo circuito de varios bits (b1-128) y una salida de segundo circuito, donde el primer circuito (1012) y el segundo circuito (1014) son idénticos excepto por las diferencias inherentes al proceso de fabricación;
- un circuito (1020, figura 56) árbitro que tiene unas primera y segunda entradas de circuito árbitro, respectivamente conectadas a la salida de primer circuito (1016) y a la salida de segundo circuito (1018), y una salida de circuito árbitro, donde el circuito (1020) árbitro está configurado para determinar si cada pulso de respuesta a una señal de entrada pregunta (b1-128) introducida simultáneamente en la entrada de primer circuito y en la entrada de segundo circuito llega antes a la salida de primer circuito o a la salida de segundo circuito y para emitir un pulso de salida en función de ello a través de la salida de circuito árbitro, de modo que, para cada señal pregunta introducida simultáneamente en la entrada de primer circuito y la entrada de segundo circuito, las diferencias entre el primer y segundo circuitos inherentes al proceso de fabricación provocan diferencias en la temporización de los pulsos obtenidos respectivamente en la salida de primer circuito y la salida de segundo circuito, de manera que si el flanco de subida de un pulso aparece antes en la salida de primer circuito el circuito árbitro emite un "1", mientras que si el flanco de subida de un pulso aparece antes en la salida de segundo circuito el circuito (1020) árbitro emite un "0", obteniéndose en la salida de circuito árbitro una señal de salida que conforma una señal respuesta unívoca (párrafo [0377]).

El objeto de la reivindicación 1 ha sido divulgado de manera idéntica en D01. Por lo mencionado, la reivindicación 1 no presenta novedad (Artículo 6.1 LP).

Reivindicación 10

En relación con la reivindicación 10 en el documento D01 se describen los elementos funcionales de la reivindicación 1 y las acciones que realizan, que son las etapas que caracterizan la reivindicación 10, por lo que los mismos argumentos son aplicables.
Por lo mencionado, la reivindicación 10 no presenta novedad (Artículo 6.1 LP).

Reivindicaciones dependientes

Reivindicaciones 2,3,11,12

Las reivindicaciones 2-3 y 11-12 añaden a las características de las reivindicaciones de las que dependen (1 y 10 respectivamente) elementos que se encuentran asimismo divulgados explícita o implícitamente en D01, como que la salida de los circuitos PUF es de 1 bit (párrafo [0377]), y que el circuito árbitro está formado por biestables (párrafo [0378]).

Por lo mencionado, las reivindicaciones 2-3 y 11-12 no presentan novedad (Artículo 6.1 LP).

Reivindicación 4

La reivindicación 4, dependiente de la 1, caracteriza el circuito árbitro mediante un circuito de tipo C-element. que comprende biestables RS y un registro de desplazamiento con biestables tipo D, conectados de una manera particular que se refleja en la descripción y figuras.

Estas características no están presentes en D01, y según la descripción, producen el efecto técnico de filtrar la metaestabilidad del circuito árbitro en situaciones de simultaneidad de las entradas. Por tanto, el problema técnico objetivo que se deriva de dichas características, sería como reducir dicha metaestabilidad.

El documento D02 del estado de la técnica revela el uso de circuitos C-element para la generación de pulsos de reloj sin saltos espúreos, en relación con el espacio y la fiabilidad de estos elementos en los circuitos integrados. Sin embargo no menciona la posibilidad de usarse en un dispositivo para identificación unívoca de circuitos integrados, ni el problema técnico objetivo mencionado.

En los documentos D03, D04 y D05, se divulgan diversos aspectos relacionados con la corrección de errores a la salida de los circuitos PUF, pero no mencionan el problema de la metaestabilidad del circuito árbitro.

Se considera que un experto en la materia partiendo del documento D01 y considerando el conjunto del estado de la técnica, no podría reconocer el problema técnico objetivo, y por lo tanto tampoco resolverlo de la manera que se divulga en la solicitud para llegar al objeto de la reivindicación 4.

Por lo mencionado, la reivindicación 4 presenta novedad (Artículo 6.1 LP) y actividad inventiva (Artículo 8.1 LP).

Reivindicaciones 5-9

Las reivindicaciones 5-9 dependen directa o indirectamente de la reivindicación 4, por lo que también presentan novedad (Artículo 6.1 LP) y actividad inventiva (Artículo 8.1 LP).

Reivindicaciones 13-16

La reivindicación 13, dependiente de la 10, añade las etapas de detectar pulsos de salida de los circuitos PUF simultáneos en relación a un valor umbral de tiempo, y eliminar la respuesta de la salida del circuito árbitro, las cuales no se encuentran en los documentos del estado de la técnica.

Estas etapas producen el mismo efecto técnico mencionado para la reivindicación 4 y por lo tanto su argumentación es aplicable.

Por lo mencionado, la reivindicación 13 presenta novedad (Artículo 6.1 LP) y actividad inventiva (Artículo 8.1 LP).

Las reivindicaciones 14-16 dependen directa o indirectamente de la reivindicación 13, por lo que también presentan novedad (Artículo 6.1 LP) y actividad inventiva (Artículo 8.1 LP).