(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 655 503**

(51) Int. Cl.:

G01R 31/3181 (2006.01)
G01R 31/3183 (2006.01)
G01R 31/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.02.2014** **PCT/SE2014/050145**

(87) Fecha y número de publicación internacional: **13.08.2015** **WO15119540**

(96) Fecha de presentación y número de la solicitud europea: **05.02.2014** **E 14706138 (6)**

(97) Fecha y número de publicación de la concesión europea: **01.11.2017** **EP 3102957**

(54) Título: **Gestión remota de pruebas de circuitos lógicos digitales**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.02.2018

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

DUBROVA, ELENA;
NÄSLUND, MATS;
CARLSSON, GUNNAR;
FORNEHED, JOHN y
SMEETS, BERNARD

(74) Agente/Representante:

ELZABURU, S.L.P

ES 2 655 503 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Gestión remota de pruebas de circuitos lógicos digitales

Campo técnico

La invención se relaciona con los dispositivos electrónicos que comprenden un circuito lógico digital y un módulo de prueba para probar el circuito lógico digital, los dispositivos remotos de gestión de la prueba para probar de manera remota los circuitos lógicos digitales comprendidos en los dispositivos electrónicos, los métodos correspondientes, los programas informáticos correspondientes, y los productos correspondientes de programas informáticos.

Antecedentes

Un fallo de hardware en un circuito lógico digital puede afectar de manera negativa a su funcionamiento. En concreto, esto aplica a los circuitos lógicos digitales que proporcionan funcionalidades de criptografía, ya que el funcionamiento seguro puede ser puesto en peligro por los fallos de hardware. Por lo tanto, es deseable que los circuitos lógicos digitales realicen un autodiagnóstico y unas comprobaciones automáticas (BIST) durante su tiempo de vida. Los circuitos integrados (IC) con funcionalidad BIST normalmente incorporan la lógica para la generación de las pruebas y el análisis de las respuestas de las pruebas en el chip.

El BIST lógico (LBIST), que se usa para probar los circuitos lógicos digitales, normalmente emplea un Generador de Patrones Pseudo Aleatorios (PRPG) para generar los patrones de la prueba que se aplican a los circuitos bajo prueba (CUT), y un Registro de Firma de Entrada Múltiple (MISR) para obtener una respuesta compacta, la así llamada firma, del CUT a estos patrones de la prueba. Un resultado incorrecto del MISR indica un fallo en el CUT.

El LBIST se usa normalmente en combinación con el diseño de escaneo, que es una técnica de diseño de la prueba que proporciona una manera simple de ajustar y observar cada celda, o elemento de almacenamiento, en un circuito lógico digital. En el diseño de escaneo, todos los elementos de almacenamiento del circuito lógico digital se conectan a uno o más registros de desplazamiento, llamados cadenas de escaneo, multiplexando sus respectivas entradas para apoyar el modo de escaneo que permite la carga y descarga en serie del contenido de la serie de escaneos. Para cada serie de escaneos, se carga un patrón de la prueba en la cadena de elementos de almacenamiento, y se lee el estado de cada elemento de almacenamiento. En el modo de operación normal, las series de escaneos no afectan al funcionamiento del circuito.

El LBIST es comúnmente gestionado y controlado por una unidad de control que o bien reside en el CUT o en la misma placa del circuito del CUT. La unidad de control inicia el LBIST proporcionando los parámetros de la prueba al PRPG, tales como el valor de inicialización y el número de patrones de la prueba a generar, en base a los cuales el PRPG genera los patrones de la prueba que posteriormente se aplican al CUT. Después, las respuestas a la prueba recibidas desde el CUT son compactadas por el MISR en una firma que se compara a la firma esperada para determinar el resultado de la prueba. Los parámetros de la prueba y la firma esperada se almacenan en una memoria o se cablean. Normalmente, el LBIST se realiza de manera automática en un encendido y un reinicio, o en respuesta a un desencadenante externo, por ejemplo, si un hardware o un software que supervisa el chip indica un fallo. Además, el LBIST se puede iniciar por un operador, por ejemplo, con propósitos de depuración cuando se envía a reparar un chip defectuoso.

En el LBIST conocido, se usa el mismo conjunto de patrones de la prueba cada vez que se realiza una prueba. Esto se debe al hecho de que el PRPG siempre empieza desde el mismo estado inicial, que está determinado por el valor de inicialización proporcionado durante la fabricación, y por consiguiente genera el mismo conjunto de patrones de la prueba. Además, la firma de la prueba que se obtiene mediante la acumulación y compactación de las respuestas de la prueba se compara a la misma firma esperada que se almacena o se cablea en el chip y se proporciona durante la fabricación. Esto abre una puerta a Troyanos de hardware, esto es, modificaciones maliciosas de elementos de circuitos durante el proceso de fabricación, que no cambian la firma creada por el MISR. Esto es posible ya que las respuestas de la prueba del CUT se acumulan y compactan en una firma, y la probabilidad de que un circuito defectuoso produzca la misma firma que el circuito correcto no es cero. Esto último es a menudo referido como “error de solapamiento”. La factibilidad de dicho ataque, se demostró recientemente para el hardware generador de números aleatorios de Intel usado en el procesador Ivy Bridge, que era considerado criptográficamente seguro y que estaba protegido por el LBIST tradicional (G. R. Becker, F. Regazzoni, C. Para, and W.P. Burleson, Troyanos de Nivel de Hardware Dopantes Sigilosos”, en Hardware Criptográfico y Sistemas Incrustados – CHES 2013”, Notas de Clase en Ciencia de la Computación, Volumen 8086, Springer Berlín Heidelberg, 2013, páginas 197-214).

El documento US 2006/0156144 A1 describe las soluciones para filtrar las respuestas a la prueba compactadas, para eliminar los efectos de los valores desconocidos de la prueba. Por ejemplo, una respuesta a la prueba compactada que se recibe desde un compactador de un circuito bajo prueba puede incluir uno o más valores de las respuestas a la prueba compactadas que son dependientes de uno o más respectivos valores desconocidos. La respuesta a la prueba compactada se filtra para eliminar la dependencia de al menos alguno de los valores de la respuesta a la prueba compactada sobre uno o más respectivos valores desconocidos, y se emite la respuesta de la prueba filtrada.

El documento 2005/0193294 A1 describe las soluciones para probar uno o más circuitos integrados que se configuran con una interfaz inalámbrica y un mecanismo de acceso a la prueba desde una estación de prueba para probar las estructuras que prueban los bloques funcionales sobre el circuito integrado. A través de la conexión inalámbrica, se pueden probar múltiples circuitos integrados o dispositivos equipados de manera similar bajo prueba simultáneamente. Las soluciones descritas también permiten la prueba concurrente de bloques funcionales comprobables de manera independiente o cualquier circuito integrado dado a prueba.

Compendio

Es un objetivo de la invención proporcionar una alternativa mejorada a las técnicas anteriores y al estado de la técnica.

Más específicamente, es un objetivo de la invención proporcionar una prueba integrada lógica mejorada de dispositivos electrónicos que comprenden un circuito lógico digital, y en concreto una prueba integrada lógica capaz de detectar modificaciones maliciosas de elementos de circuitos del circuito lógico digital. Objetivos adicionales de la invención son proporcionar un alcance mejorado de la prueba y permitir la prueba remota de una cantidad potencialmente grande de dispositivos electrónicos que tienen circuitos lógicos digitales similares.

Estos y otros objetivos de la invención se logran por medio de diferentes aspectos de la invención, como se define por las reivindicaciones independientes. Las realizaciones de la invención están caracterizadas por las reivindicaciones dependientes.

Según un primer aspecto de la invención, se proporciona un dispositivo electrónico. El dispositivo electrónico comprende un circuito lógico digital y un módulo de prueba. El módulo de prueba se adapta para recibir uno o más parámetros de la prueba desde un dispositivo remoto de gestión de la prueba y para generar uno o más patrones de la prueba basados en los parámetros de la prueba. El módulo de prueba se adapta además para aplicar los patrones de la prueba al circuito lógico digital, recibir una o más respuestas de la prueba desde el circuito lógico digital, compactar las respuestas de la prueba en una firma de la prueba, y transmitir la firma de la prueba al dispositivo remoto de gestión de la prueba.

Según un segundo aspecto de la invención, se proporciona un dispositivo electrónico. El dispositivo electrónico comprende un circuito lógico digital y un módulo de prueba. El módulo de prueba se adapta para recibir uno o más parámetros de la prueba desde un dispositivo remoto de gestión de la prueba y para generar uno o más patrones de la prueba basados en los parámetros de la prueba. El módulo de prueba se adapta además para aplicar los patrones de la prueba al circuito lógico digital, recibir una o más respuestas de la prueba desde el circuito lógico digital, compactar las respuestas de la prueba en una firma de la prueba, recibir la firma esperada correspondiente a los patrones de la prueba desde el dispositivo remoto de gestión de la prueba, y determinar el resultado de la prueba. El resultado de la prueba se determina basado en la comparación de la firma esperada con la firma de la prueba.

Según un tercer aspecto de la invención, se proporciona un dispositivo remoto de gestión de la prueba. El dispositivo remoto de gestión de la prueba comprende unos medios adaptados para adquirir uno o más parámetros de la prueba que son adecuados para generar uno o más patrones de la prueba para un circuito lógico digital. Los medios se adaptan además para adquirir la firma esperada correspondiente a los patrones de la prueba, y transmitir los parámetros de la prueba a al menos un dispositivo electrónico que comprende el circuito lógico digital. Los medios se adaptan además para recibir la firma de la prueba desde al menos un dispositivo electrónico, y determinar el resultado de la prueba en base a la comparación de la firma esperada con la firma de la prueba.

Según un cuarto aspecto de la invención, se proporciona un dispositivo remoto de gestión de la prueba. El dispositivo remoto de gestión de la prueba comprende unos medios adaptados para adquirir uno o más parámetros de la prueba que son adecuados para generar uno o más patrones de la prueba para un circuito lógico digital. Los medios se adaptan además para adquirir la firma esperada correspondiente a los patrones de la prueba, transmitir los parámetros de la prueba a al menos un dispositivo electrónico que comprende el circuito lógico digital, y transmitir la firma esperada a al menos un dispositivo electrónico.

Según un quinto aspecto de la invención, se proporciona un método de prueba de un circuito lógico digital comprendido en un dispositivo electrónico. El método es realizado por el dispositivo electrónico. El método comprende la recepción de uno o más parámetros de la prueba desde un dispositivo remoto de gestión de la prueba y generar uno o más patrones de la prueba basados en los parámetros de la prueba. El método además comprende la aplicación de los patrones de la prueba al circuito lógico digital, la recepción de una o más respuestas de la prueba desde el circuito lógico digital, la compactación de las respuestas de la prueba en una firma de la prueba, y la transmisión de la firma de la prueba hasta el dispositivo remoto de gestión de la prueba.

Según un sexto aspecto de la invención, se proporciona un método de prueba de un circuito lógico digital comprendido en un dispositivo electrónico. El método es realizado por el dispositivo electrónico. El método comprende la recepción de uno o más parámetros de la prueba desde un dispositivo remoto de gestión de la prueba y la generación de uno o más patrones de la prueba basados en los parámetros de la prueba. El método además comprende la aplicación de los patrones de la prueba al circuito lógico digital, la recepción de una o más respuestas

de la prueba desde el circuito lógico digital, la compactación de las respuestas de la prueba en una firma de la prueba, la recepción de la firma esperada correspondiente a los patrones de la prueba desde el dispositivo remoto de gestión de la prueba, y la determinación del resultado de la prueba en base a la comparación de la firma esperada con la firma de la prueba.

Según un séptimo aspecto de la invención, se proporciona un método de prueba de un circuito lógico digital comprendido en un dispositivo electrónico. El método es realizado por un dispositivo remoto de gestión de la prueba. El método comprende la adquisición de uno o más parámetros de la prueba que son adecuados para generar uno o más patrones de la prueba para un circuito lógico digital. El método además comprende la adquisición de la firma esperada correspondiente a los patrones de la prueba y la transmisión de los parámetros de la prueba a al menos un dispositivo electrónico que comprende el circuito lógico digital. El método además comprende la recepción de la firma de la prueba desde al menos un dispositivo electrónico, y la determinación del resultado de la prueba en base a la comparación de la firma esperada con la firma de la prueba.

Según un octavo aspecto de la invención, se proporciona un método de prueba de un circuito lógico digital comprendido en un dispositivo electrónico. El método es realizado por un dispositivo remoto de gestión de la prueba. El método comprende la adquisición de uno o más parámetros de la prueba que son adecuados para generar uno o más patrones de la prueba para un circuito lógico digital. El método además comprende la adquisición de la firma esperada correspondiente a los patrones de la prueba, la transmisión de los parámetros de la prueba a al menos un dispositivo electrónico que comprende el circuito lógico digital, y la transmisión de la firma esperada a al menos un dispositivo electrónico.

Según aspectos adicionales de la invención, se proporcionan programas informáticos que comprenden instrucciones ejecutables por ordenador. Las instrucciones ejecutables por ordenador provocan que un dispositivo, cuando se ejecutan en una unidad de procesamiento comprendida en el dispositivo, realice el método según cualquiera de entre el primero, segundo, tercero, o cuarto, aspecto de la invención descritos anteriormente.

Según incluso aspectos adicionales de la invención, se proporcionan productos de programas informáticos que comprenden un medio de almacenamiento legible por ordenador. El medio de almacenamiento legible por ordenador tiene los programas informáticos según los aspectos correspondientes de la invención representados en este.

En el contexto actual, un dispositivo electrónico de acuerdo con una realización de la invención comprende un circuito lógico digital que implementa al menos parte de la funcionalidad que proporciona el dispositivo electrónico. Por ejemplo, el circuito lógico digital puede implementar una funcionalidad criptográfica, tal como un generador de números pseudo aleatorios o un codificador de flujo. El dispositivo electrónico se proporciona con un módulo de prueba con el propósito de probar el circuito lógico digital y puede además comprender otros tipos de circuitería distintos de la lógica digital, otros tipos de circuitería que no están probadas por las realizaciones de la invención. El módulo de prueba se puede integrar con el circuito lógico digital, por ejemplo, en un IC único, o se puede proporcionar con el circuito lógico digital, por ejemplo, en una placa de circuito común. El dispositivo electrónico puede estar comprendido en un dispositivo criptográfico, por ejemplo, una circuitería criptográfica. El dispositivo electrónico puede estar comprendido también en un terminal móvil, tal como un Equipo de Usuario (UE), un teléfono móvil, un teléfono inteligente, una tarjeta inteligente, una tableta, o un tipo de dispositivo Máquina-a-Máquina (M2M) o del Internet de las Cosas (IoT).

La invención hace uso de la comprensión del LBIST tradicional, que utiliza el mismo conjunto de patrones de prueba para probar un circuito lógico digital, el CUT, y realiza la misma firma esperada cada vez que se realiza la prueba, analiza el CUT supervisado vulnerable a Troyanos de hardware que aprovechen el error de solapamiento del MISR. Esto es debido al hecho de que se pueden realizar modificaciones maliciosas de elementos del circuito durante el proceso de fabricación que no cambian la firma creada por el MISR al compactar las respuestas de la prueba del circuito modificado, ya que la firma representa las respuestas acumuladas del CUT al conjunto completo de patrones de la prueba.

Las realizaciones de la invención mitigan este problema proporcionando un dispositivo electrónico y un dispositivo remoto de gestión de la prueba que se adaptan para realizar las pruebas lógicas de manera cooperativa. Más específicamente, esto se logra mediante la transmisión de los parámetros de la prueba desde el dispositivo remoto de gestión de la prueba hasta el dispositivo electrónico y la generación de los patrones de la prueba en base a los parámetros de la prueba recibidos desde el dispositivo remoto de gestión de la prueba. Además de proporcionar los parámetros de la prueba, el dispositivo remoto de gestión de la prueba también proporciona una firma esperada correspondiente al conjunto de patrones de la prueba generados por el dispositivo electrónico para detectar fallos de hardware en el circuito lógico digital, que incluyen las modificaciones maliciosas del circuito lógico digital. Esto se logra mediante la comparación de la firma de la prueba, obtenida mediante la compactación de las respuestas a la prueba del circuito lógico digital, con la firma esperada. La comparación de la firma de la prueba con la firma esperada se realiza bien en el dispositivo remoto de gestión de la prueba o bien en el dispositivo electrónico. Si se realiza en el dispositivo remoto de gestión de la prueba, la firma de la prueba se transmite desde el dispositivo electrónico hasta el dispositivo remoto de gestión de la prueba para su comparación posterior con la firma esperada. Si se realiza en el dispositivo electrónico, la firma esperada se transmite desde el dispositivo remoto de gestión de la prueba al dispositivo electrónico para su comparación posterior con la firma de la prueba.

Las realizaciones de la invención son ventajosas sobre el LBIST tradicional ya que se pueden usar diferentes conjuntos de patrones de prueba cada vez que se realiza una prueba, mejorando de este modo el alcance de la prueba. En concreto, mediante el uso de diferentes valores de inicialización, el PRPG genera patrones de la prueba que empiezan desde un estado inicial diferente, lo que resulta en diferentes secuencias de patrones de la prueba. Esto es ventajoso ya que se obstaculiza la provisión de Troyanos de hardware durante la fabricación, por la razón de que el adversario no tiene un conocimiento total de los patrones de prueba que se generarán durante la vida útil del circuito lógico digital, el CUT.

Es importante notar que la generación de las firmas esperadas es computacionalmente muy exigente, ya que se basa en la simulación del circuito lógico digital a ser probado, esto es, del diseño del circuito lógico digital. Por lo tanto, no es factible generar las firmas esperadas en el dispositivo electrónico, ya que tal enfoque aumentaría de manera considerable la complejidad del dispositivo electrónico así como su área de chip y consumo energético. Tampoco es factible almacenar una gran cantidad de firmas esperadas pregeneradas, que resultan en un considerable aumento en los requisitos de almacenamiento. Estos aspectos son de máxima importancia para las pruebas integradas de los terminales móviles, y en concreto para los dispositivos M2M/IoT que están caracterizados por unos recursos de computación limitados y que comúnmente están alimentados por baterías.

Las realizaciones de la invención proporcionan pruebas lógicas de circuitos lógicos digitales con protección mejorada contra los Troyanos de hardware así como un alcance de las pruebas mejorado. Además de esto, el enfoque de prueba remota descrito en la presente memoria es ventajoso en escenarios M2M/IoT ya que permite una eficiente gestión de la prueba remota y la detección de fallos en un número de dispositivos potencialmente grande. Esto aplica en particular a la prueba de uno a muchos de un gran número de dispositivos similares, o un gran número de dispositivos que comprenden circuitos lógicos digitales similares.

Según una realización de la invención, el resultado de la prueba se determina como que indica un fallo en el circuito lógico digital si la firma esperada difiere de la firma de la prueba. En otras palabras, se indica un fallo si la firma de la prueba obtenida mediante la compactación de las respuestas de la prueba acumuladas recibidas desde el circuito lógico digital difiere de la firma esperada. Esto es, la prueba ha fallado. De lo contrario, el resultado de la prueba se determina como que indica que la prueba ha pasado.

Según una realización de la invención, la información correspondiente al resultado de la prueba se transmite desde el dispositivo electrónico hasta el dispositivo remoto de gestión de la prueba. Esto aplica a las realizaciones de la invención que realizan la comparación de la firma de la prueba con la firma esperada en el dispositivo electrónico. La información transmitida puede comprender el resultado de la prueba, esto es, la información que indica si la prueba ha fallado o ha pasado.

Según una realización de la invención, el módulo de prueba se adapta además para realizar autocomprobaciones lógicas en el circuito lógico digital. Dichas pruebas, pueden, por ejemplo, ser realizadas en el encendido o el reinicio, o en respuesta a un desencadenante externo. Con este fin, el módulo de prueba genera uno o más patrones de la prueba basados en los parámetros de la prueba almacenados o cableados, aplica los patrones de la prueba al circuito lógico digital, compacta los resultados de la prueba recibidos desde el circuito lógico digital en una firma de la prueba, y compara la firma de la prueba con la firma esperada almacenada o cableada.

Según una realización de la invención, los medios del dispositivo remoto de gestión de la prueba se adaptan además para adquirir las firmas esperadas mediante la computación de las firmas esperadas en base a los parámetros de la prueba y el diseño del circuito lógico digital. Como se discutió anteriormente, el cálculo de las firmas esperadas por medio de la simulación del circuito lógico digital es computacionalmente muy exigente y por lo tanto no es factible que se realice en el dispositivo electrónico. Como una alternativa, se pueden almacenar las firmas esperadas pregeneradas, por ejemplo, en una base de datos, en el dispositivo remoto de gestión de la prueba o en un almacenamiento externo accesible por el dispositivo remoto de gestión de la prueba.

Incluso aunque las ventajas de la invención se han descrito en algunos casos con referencia a las realizaciones de un cierto aspecto de la invención, un razonamiento correspondiente aplica a las realizaciones de otros aspectos de la invención.

Objetivos, características, y ventajas adicionales de la invención resultarán evidentes al estudiar la siguiente descripción detallada, los dibujos y las reivindicaciones adjuntas. Aquellos expertos en la técnica se darán cuenta de que la diferentes características de la invención se pueden combinar para crear otras realizaciones distintas de aquellas descritas a continuación.

Breve descripción de los dibujos

Los objetivos, características y ventajas anteriores, así como los objetivos adicionales, de la invención, se comprenderán mejor a través de la siguiente descripción ilustrativa y no limitante de las realizaciones de la invención, con referencia a los dibujos adjuntos, en los cuales:

La Fig. 1 muestra un diagrama de bloques de un IC conocido con funcionalidad LBIST.

La Fig. 2 muestra un diagrama de bloques funcional de un módulo LBIST conocido.

La Fig. 3 ilustra de manera esquemática una prueba remota de acuerdo con una realización de la invención.

La Fig. 4 muestra un dispositivo electrónico de acuerdo con una realización de la invención.

La Fig. 5 muestra un módulo de prueba de acuerdo con una realización de la invención.

La Fig. 6 muestra un módulo de prueba de acuerdo con otra realización de la invención.

La Fig. 7 muestra un método de prueba realizado por el dispositivo electrónico, de acuerdo con una realización de la invención.

La Fig. 8 muestra un método de prueba realizado por el dispositivo electrónico, de acuerdo con otra realización de la invención.

La Fig. 9 muestra un método de prueba realizado por el dispositivo remoto de gestión de la prueba, de acuerdo con una realización de la invención.

La Fig. 10 muestra un método de prueba realizado por el dispositivo remoto de gestión de la prueba, de acuerdo con otra realización de la invención.

La Fig. 11 muestra un IC, de acuerdo con una realización de la invención.

La Fig. 12 muestra un SoM, de acuerdo con una realización de la invención.

La Fig. 13 muestra un terminal móvil, de acuerdo con una realización de la invención.

Todas las figuras son esquemáticas, no necesariamente a escala, y generalmente sólo muestran las partes que son necesarias para dilucidar la invención, en donde otras partes se pueden omitir o simplemente sugerir.

Descripción detallada

La invención se describirá más plenamente ahora de aquí en adelante con referencia a los dibujos adjuntos, en los que se muestran ciertas realizaciones de la invención. Esta invención puede, sin embargo, ser realizada de muchas formas diferentes y no se debería interpretar como limitada a las realizaciones expuestas en el presente documento. Más bien, estas realizaciones son proporcionadas a modo de ejemplo para que la descripción sea exhaustiva y completa, y transmita completamente el alcance de la invención a aquellos expertos en la técnica. El alcance de la invención está definido por las reivindicaciones.

En la Fig.1 se ilustra un IC 100 como ejemplo de un dispositivo electrónico con una funcionalidad LBIST convencional. El IC 100 puede, por ejemplo, ser un microprocesador, un IC de Aplicación Específica (ASIC), o una Matriz de Puertas Programables en Campo (FPGA). Puede también ser parte de un IC mayor, un Sistema en Chip (SoC), esto es, un IC que integra todos los componentes de un sistema electrónico en un chip único, un Sistema en Paquete (SiP), que es un número de circuitos integrados encapsulados en un módulo o paquete único, o un Sistema en Módulo (SoM), que es un ordenador completo integrado construido en una placa de circuito única. El IC 100 comprende un circuito 101 lógico digital, el CUT, que implementa al menos parte de la funcionalidad que el IC 100 proporciona, y un módulo LBIST 102 para realizar las pruebas lógicas en el CUT 101.

El módulo LBIST 102, que se ilustra en más detalles en la Fig. 2, comprende un PRPG 201, que puede estar basado en un Registro de Desplazamiento con Retroalimentación Lineal (LFSR), para generar los patrones pseudoaleatorios de la prueba que se aplican al CUT 101 durante la prueba a través de las entradas 111 de la prueba. Un patrón de la prueba comprende una pluralidad de valores binarios, uno para cada entrada 111 de la prueba. Los patrones de la prueba se generan basados en uno o más parámetros de la prueba que se almacenan o se cablean en 202 en el módulo LBIST 102. Normalmente, los parámetros de la prueba comprenden un valor de inicialización, que define un estado inicial del PRPG 201, y un número de patrones a generar de la prueba. El módulo LBIST 102 comprende además un MISR 203 para compactar las respuestas a la prueba recibidas desde el CUT 101 a través de los resultados 112 de la prueba, comúnmente referidos como “datos de pisoteo”, en una firma de la prueba, y una decisión lógica 204 para comparar la firma de la prueba obtenida del MISR 203 con la firma esperada que se almacena o se cablea en 205 en el módulo LBIST 102. El resultado de esta comparación se hace disponible por medio de una señal 115 que indica el resultado de la prueba a un circuito externo, por ejemplo, una unidad de supervisión de fallos proporcionada junto con el IC 100. El módulo LBIST 102 comprende además un controlador 206 para controlar la operación del módulo LBIST 102 y el CUT 101 por medio de una o más señales 113 de control. El controlador 206 realiza normalmente secuencias de pruebas lógicas de manera autónoma, por ejemplo en un encendido o un reinicio, en respuesta a una condición de fallo detectado, o en respuesta a un desencadenante externo recibido a través de una unidad 114 de entrada de control opcional. La entrada 114 de control se puede usar también para alternar el IC 100 entre un modo de operación normal y un modo de prueba, o para iniciar un ciclo de pruebas, y puede, por ejemplo, conectarse a una unidad de supervisión de fallos proporcionada junto con el IC 100.

El LBIST se usa normalmente en combinación con un diseño de escaneo, que es una técnica de diseño para pruebas que proporciona una manera simple de ajustar y observar cada celda, o elemento de almacenamiento, en un circuito lógico digital tal como el CUT 101. En el diseño de escaneo, las celdas de un circuito lógico digital, tal como el CUT 101, se conectan en uno o más registros de desplazamiento, llamadas cadenas 114 de escaneos. Las cadenas 114 de escaneo se proporcionan con las entradas 111 de las pruebas que se multiplexan (los multiplexores no se muestran en la Fig. 2) para apoyar un modo de escaneo que permite la carga y descarga en serie de los contenidos de las cadenas 114 de escaneo a través de las entradas 111 de las pruebas y los resultados 112 de las pruebas, respectivamente. Las cadenas de escaneos se definen durante el diseño del circuito y son representativas para probar el rendimiento operacional de partes del CUT. Normalmente, las cadenas de escaneo se posicionan antes y después, esto es, interpuestas con, partes de circuitos funcionales del CUT de tal manera que para cada parte funcional existe (i) una “cadena de escaneo anterior” que proporciona las entradas a los componentes de circuito de la parte funcional, y (ii) una “cadena de escaneo siguiente” que recibe los resultados de la parte funcional.

Un ciclo de prueba normalmente implica la selección de un modo de escaneo y la carga en serie de un patrón de prueba en las cadenas 114 de escaneo a través de las entradas 111 de la prueba. Cuando las cadenas 114 de escaneo están totalmente cargadas, se selecciona el modo normal de operación del CUT 101, a través de las señales 113 de control, y se aplica un ciclo de reloj, aplicando de este modo el patrón de la prueba cargado a las entradas de la lógica combinacional implementada por el CUT 101. La respuesta del CUT 101 a los valores de entrada definidos por los patrones de la prueba está disponible en los resultados 112 de la prueba de la lógica combinacional. Finalmente, el modo de escaneo del CUT 101 se selecciona de nuevo, y se aplica un ciclo de reloj para descargar los valores de los resultados de las cadenas 114 de escaneo a través de los resultados 112 de la prueba. Mientras que los resultados se sacan de las cadenas 114 de escaneo, el siguiente patrón de la prueba se puede cargar en las cadenas 114 de escaneo. El MISR 203 compacta y acumula las respuestas a la prueba recibidas a través de los resultados 112 en una firma de la prueba que se compara posteriormente, a través de la lógica 204 de decisión, a la firma 205 esperada almacenada o cableada en el módulo LBIST 102. Un resultado del MISR incorrecto, esto es, una firma que difiere de la firma esperada, esto es, la firma de un CUT 101 sin fallos, indica un fallo.

En el LBIST tradicional, como se describe anteriormente con referencia a las FIg. 1 y 2, se aplica el mismo conjunto de patrones de prueba al CUT 101 cada vez que se realizan las pruebas lógicas, esto es, cada vez que se ejecuta un ciclo de prueba. Esto es debido al hecho de que los parámetros de la prueba, el estado inicial del PRPG 201 y el número de patrones de la prueba a ser generados, así como la firma esperada correspondiente, necesitan ser almacenados o cableados en el IC 100. Las desventajas de este enfoque del estado de la técnica son dobles. En primer lugar, ya que se usa el mismo conjunto de patrones de prueba cada vez que se realizan las pruebas lógicas durante la vida útil del IC 100, y el conjunto de patrones de prueba es conocido cuando se fabrica el chip, el chip es vulnerable a Troyanos de hardware que aprovechen el error de solapamiento del MISR 203. Un adversario puede aprovechar el conocimiento de los patrones de la prueba y la firma esperada correspondiente para modificar de manera maliciosa los elementos de circuito durante el proceso de fabricación, de manera tal que la firma de la prueba creada por el MISR para la prueba de unos vectores establecidos es idéntica a la del diseño del circuito original. En segundo lugar, ya que los patrones de la prueba se generan de manera pseudoaleatoria, se requiere un gran número de patrones de prueba para lograr un alcance satisfactorio de la prueba. Normalmente del orden de 10000 patrones de prueba o más. La limitación en el tamaño del conjunto de pruebas proviene del requisito de que se espera que se complete un ciclo de pruebas dentro de un tiempo razonable, lo que depende de la dedicación disponible. Por ejemplo, para una estación base de radio u otro nodo de la red de acceso por radio, se espera que se complete un ciclo de pruebas para las pruebas en campo en menos de diez segundos. Por lo tanto no es factible aumentar de manera considerable el tamaño del conjunto de pruebas, esto es, el conjunto de patrones de prueba, ya que esto resultaría en un considerable aumento del tiempo de ejecución del ciclo de pruebas. No es factible usar diferentes conjuntos de pruebas para cada ciclo de pruebas para mejorar el alcance de la prueba ya que cada conjunto de patrones de prueba requiere una firma esperada correspondiente para determinar si el chip ha pasado o no. Mientras que la generación de los patrones de prueba por el PRPG no es computacionalmente muy exigente, la generación de las firmas esperadas correspondientes constituye un esfuerzo computacional considerable, ya que requiere la simulación de la lógica combinacional implementada por el CUT en software, y calcular la respuesta de la lógica combinacional simulada para cada patrón de la prueba. En otras palabras, además del CUT, el chip requeriría el procesamiento de medios suficientemente complejos para simular la lógica combinacional implementada por el CUT y calcular las respuestas de salida del CUT a los patrones de prueba de entrada. Obviamente, esto provocaría un considerable aumento en la complejidad del chip. También se apreciará que no es factible almacenar las firmas pregeneradas para conjuntos de pruebas variados o grandes, debido al correspondiente aumento de los recursos de almacenamiento requeridos.

A continuación, y con referencia a las Fig. 3 a 13, se describe la prueba remota de acuerdo con las realizaciones de la invención.

La Fig. 3 ilustra un sistema 300 que comprende un dispositivo 310 remoto de gestión de la prueba y uno o más dispositivos electrónicos 320 dispuestos para comunicarse los unos con los otros a través de una red 301 de comunicaciones. El dispositivo 310 remoto de gestión de la prueba puede, por ejemplo, ser un ordenador personal que se proporciona con un programa informático de acuerdo con una realización de la invención, o una unidad de

supervisión de fallos dedicada, como se describe más adelante. El dispositivo 310 remoto de gestión de la prueba se puede implementar también como una máquina virtual para su ejecución en un entorno computación en la nube.

Cada uno de los dispositivos 320 electrónicos comprende un circuito lógico digital, un CUT 101, y un Módulo de Pruebas (TM) 322 para realizar las pruebas lógicas sobre el CUT 101, como se describe más adelante. Se apreciará que, aunque los dispositivos electrónicos 320 se ilustran en la Fig. 3 como que se comunican de manera directa con el dispositivo 310 remoto de gestión de la prueba, los dispositivos electrónicos 320 pueden estar comprendidos en terminales móviles, por ejemplo, UE, ordenadores, tabletas, dispositivos M2M, y así sucesivamente, a través de los cuales se realiza la comunicación con el dispositivo 310 remoto de gestión de la prueba. La red 301 de comunicaciones puede, por ejemplo, ser una o una combinación de una Red de Área Local (LAN), una LAN Inalámbrica (WLAN), una Red de Área Extensa (WAN), Internet, una red corporativa, una red de radio celular tal como el Sistema Global para las Comunicaciones Móviles (GSM), el Sistema Universal de Telecomunicaciones Móviles (UMTS), o la Evolución a Largo Plazo (LTE), o una red ad-hoc, en malla o capilar. La comunicación entre el dispositivo 310 remoto de gestión de la prueba y los dispositivos electrónicos 320 se puede efectuar por medio de un protocolo de comunicación adecuado conocido en la técnica, por ejemplo, el Protocolo de Control de la Transmisión (TCP), el Protocolo de Datagramas de Usuario (UDP), o cualquier protocolo de gestión de dispositivos tal como el TR.069 (Foro de Banda Ancha), la Gestión de Dispositivos de la Alianza Móvil Abierta (OMA), o la M2M de Peso ligero de la OMA.

Las realizaciones de la invención realizan pruebas lógicas del CUT 101 de una manera distribuida, en lugar de una manera autónoma como en la técnica anterior. Con este fin, el dispositivo 310 remoto de gestión de la prueba adquiere los parámetros de la prueba, basados en los cuales se puede generar un conjunto de patrones de la prueba usando un PRPG, y una firma esperada correspondiente al conjunto de patrones de la prueba. Los parámetros de la prueba se transmiten, a través de la red 301 de comunicaciones, hasta al menos uno de los dispositivos electrónicos 320. En base a los parámetros de la prueba recibidos, el dispositivo electrónico 320 genera unos patrones de la prueba y presenta pruebas lógicas similares al LBIST convencional descrito con referencia a las Fig. 1 y 2. Esto es, los patrones de la prueba generados se aplican al CUT 101 y las respuestas a la prueba del CUT 101 se compactan en una firma de la prueba, que posteriormente se compara a la firma esperada correspondiente para determinar el resultado de la prueba, esto es, si el CUT 101 ha pasado o fallado para el conjunto de patrones de prueba. La comparación puede o bien realizarse en el dispositivo 310 remoto de gestión de la prueba o en el dispositivo electrónico 320. Si la comparación se realiza en el dispositivo 310 remoto de gestión de la prueba, la firma de la prueba se transmite desde el dispositivo electrónico 320 hasta el dispositivo 310 remoto de gestión de la prueba, donde se compara a la firma esperada y por consiguiente se determina el resultado de la prueba. Si la comparación se realiza en el dispositivo electrónico 320, la firma esperada se transmite desde el dispositivo 310 remoto de gestión de la prueba al dispositivo electrónico 320, donde se compara a la firma de la prueba y por consiguiente se determina el resultado de la prueba.

Mediante la selección apropiada de los parámetros de la prueba se mitigan los problemas asociados con el LBIST convencional. En concreto, mediante la transmisión de los diferentes valores de inicialización que definen el estado inicial del PRPG, es posible realizar las pruebas lógicas usando diferentes conjuntos de pruebas cada vez que se realiza una prueba, simplemente usando diferentes valores de inicialización, mejorando de este modo la detección de Troyanos de hardware. Además, el tamaño del conjunto de pruebas se puede aumentar, mientras se mantiene una baja carga de comunicación, transmitiendo los parámetros de la prueba para este efecto, dando instrucciones a los dispositivos electrónicos 320 para generar un conjunto de pruebas de un tamaño deseado. De esta manera, se puede mejorar el alcance de las pruebas. Con este fin, los parámetros de las pruebas comprenden al menos un valor de inicialización, un número de los patrones de la prueba a ser generados, y una o más secuencias de números de los patrones de la prueba a ser generados. Transmitiendo una lista de uno o más números de secuencia a los dispositivos electrónicos de acuerdo con una realización de la invención, además de un valor de inicialización, se pueden seleccionar y generar los patrones de la prueba específicos, debido al carácter determinista de las secuencias generadas por los PRPG. De este modo, las pruebas lógicas de pueden adaptar a partes específicas del circuito lógico digital.

Las realizaciones de la invención son ventajosas ya que se alivia la necesidad de aumentar la complejidad de las pruebas lógicas integradas que soportan los IC con varios conjuntos de pruebas, y/o conjuntos de pruebas que proporcionan un alcance de la prueba aumentado. Dejando al dispositivo 310 remoto de gestión de la prueba, mejor que el dispositivo electrónico 320, calcular o almacenar las firmas esperadas, se superan las limitaciones en cuanto a computación, almacenamiento, y recursos energéticos, de los dispositivos electrónicos 320.

Se apreciará que se puede realizar la gestión de la prueba remota de acuerdo con las realizaciones de la invención de una manera uno a uno, como se describió anteriormente con referencia a la Fig. 3, o de una manera uno a muchos. En el último caso, los parámetros de la prueba se transmiten a varios dispositivos electrónicos 320 que o bien son idénticos o al menos comprenden CUT 101 idénticos, de manera tal que se puede usar un conjunto común de patrones de prueba y sus correspondientes firmas esperadas. Si la comparación de la firma de la prueba con la firma esperada se realiza en el dispositivo 310 remoto de gestión de la prueba, cada dispositivo electrónico 320 transmite su firma de la prueba al dispositivo 310 remoto de gestión de la prueba, donde se comparan a la firma esperada por dispositivo. En consecuencia, si la comparación se realiza en los dispositivos electrónicos 320, la firma

esperada se transmite a los dispositivos electrónicos 320. Las pruebas de uno a muchos tienen la ventaja adicional de que la firma esperada, el cálculo de la cual es computacionalmente exigente, se puede usar para probar un número potencialmente grande de dispositivos electrónicos 320. Esto es de una importancia particular para los escenarios M2M/IoT en los cuales se despliegan grandes cantidades de pequeños dispositivos con unos recursos de computación, almacenamiento y batería limitados. A continuación, se discute la invención en el contexto de pruebas uno a uno, esto es, el dispositivo 310 remoto de gestión de la prueba gestiona un único dispositivo electrónico 320. Sin embargo, las realizaciones no se limitan a pruebas uno a uno y las correspondientes realizaciones para pruebas uno a muchos se pueden prever fácilmente.

Además con referencia a la Fig. 3, se describe ahora una realización del dispositivo 310 remoto de gestión de la prueba. El dispositivo 310 remoto de gestión de la prueba comprende unos medios de procesamiento, tales como una unidad 311 de procesamiento y una memoria 312 que comprende un programa informático 313, y una Interfaz 314 de Red (NI), adaptada para adquirir uno o más parámetros de la prueba adecuados para generar uno o más patrones de la prueba para un circuito lógico digital, el CUT 101, comprendido en uno o más dispositivos electrónicos 320, y para adquirir una firma esperada correspondiente al conjunto de patrones de la prueba. Los parámetros de la prueba pueden, por ejemplo, ser proporcionados por un operador del dispositivo 310 remoto de gestión de la prueba o recuperados desde una base de datos 315 con la que se proporciona el dispositivo 310 remoto de gestión de la prueba o que tiene acceso a esta. Los parámetros de la prueba se pueden adquirir cuando se inicia una prueba, por ejemplo, solicitada por el operador, desencadenada por una indicación de fallo recibida desde uno de los dispositivos 320 electrónicos o desde una unidad de supervisión de fallos, o basada en una planificación. Los medios se adaptan además para transmitir los parámetros de la prueba al dispositivo electrónico 320 donde se usan para generar los patrones de la prueba, como se describe con más detalle a continuación. Los parámetros de la prueba se transmiten al dispositivo electrónico 320 mediante la interfaz 314 de red, a través de la red 301 de comunicaciones. Los medios se adaptan además para recibir la firma de la prueba correspondiente a la firma esperada desde el dispositivo electrónico 320, y para determinar el resultado de la prueba basado en la comparación de la firma esperada con la firma recibida de la prueba. La firma de la prueba se recibe desde el dispositivo electrónico 320 mediante la interfaz 314 de red, a través de la red 301 de comunicaciones. De manera opcional, los medios se adaptan además para determinar el resultado de la prueba como que indica un fallo en el CUT 101 si la firma esperada difiere de la firma recibida de la prueba desde el dispositivo electrónico 320.

De manera alternativa, los medios comprendidos en el dispositivo 310 remoto de gestión de la prueba se pueden adaptar para transmitir la firma esperada al dispositivo electrónico 320 y, de manera opcional, recibir la información perteneciente al resultado de la prueba para los patrones de la prueba desde el dispositivo electrónico 320, antes que recibir la firma de la prueba desde el dispositivo electrónico 320 y determinar el resultado de la prueba en el dispositivo 310 remoto de gestión de la prueba.

De manera opcional, los medios comprendidos en el dispositivo 310 remoto de gestión de la prueba se pueden adaptar para encriptar la comunicación con el dispositivo electrónico 320, por ejemplo, usando un Intérprete de Órdenes Seguro (SSH), una Capa de Puertos Seguros (SSL), Seguridad en la Capa de Transporte (TSL), IPsec, o similares, como es conocido en la técnica. Esto es, los medios se adaptan para encriptar los parámetros de la prueba, y, opcionalmente la firma esperada, que se transmite al dispositivo electrónico 320, y para descifrar la firma de la prueba o el resultado de la prueba que se reciben desde el dispositivo electrónico 320. De manera adicional, el dispositivo 310 remoto de gestión de la prueba se puede adaptar para autenticar la comunicación con el dispositivo 320 electrónico como es sabido en la técnica, evitando de este modo los tipos de ataques de hombre en el medio y de suplantación.

Opcionalmente además, los medios se adaptan para calcular la firma esperada en base a la simulación del diseño de circuito del CUT 101, esto es, la lógica combinacional subyacente, que usa los patrones de la prueba como entradas, como es conocido en la técnica. Como una alternativa, la firma esperada se puede almacenar en la base de datos 315 y ser recuperada cuando se realice una prueba con un conjunto de patrones de prueba correspondientes a la firma esperada almacenada.

Con referencia a las Fig. 4 a 6, se describen ahora las realizaciones del dispositivo electrónico 320. Igual que con el IC 100 descrito con referencia a las Fig. 1 y 2, el dispositivo electrónico 320 comprende un circuito 101 lógico digital, el CUT, que implementa al menos parte de la funcionalidad que proporciona el dispositivo electrónico 320, y un módulo 322 de prueba para realizar las pruebas lógicas en el CUT 101. El dispositivo 320 puede, por ejemplo, ser un IC 1100 ilustrado en la Fig. 11, que comprende un circuito 1101 de lógica digital y un módulo 1102 de prueba, tal como un microprocesador, un ASIC, o una FPGA. Puede ser también parte de un IC mayor, un SoC, un SiP 1200, o un SoM 1200, ilustrados en la Fig. 12, que comprende un circuito 1201 lógico digital y un módulo 1202 de prueba. Una realización del dispositivo electrónico 320 puede, por ejemplo, estar comprendida por una circuitería criptográfica tal como un cifrado de flujo o los circuitos para el cifrado y/o el descifrado. Aún más, una realización del dispositivo electrónico 320 puede estar comprendida también en un terminal móvil tal como un teléfono móvil 1300, ilustrado en la Fig. 13, que comprende un circuito 1301 lógico digital y un módulo 1302 de prueba.

Una realización 500 del módulo 322 de prueba se ilustra en la Fig. 5. De manera similar al módulo LBIST 102, el módulo de prueba 500 comprende un PRPG 201 para generar patrones de prueba pseudoaleatorios y un MISR 203 para compactar las respuestas a la prueba recibidas desde el CUT 101 a través de los resultados 112 de la prueba

en la firma de la prueba. En contraste al módulo LBIST 102, los parámetros de la prueba no se almacenan o se cablean sino que se reciben desde el dispositivo 310 remoto de gestión de la prueba. Con este fin, el módulo 500 de prueba comprende un módulo 507 de comunicación configurado para comunicarse con un dispositivo remoto de gestión de la prueba a través de una red de comunicaciones, tal como el dispositivo 310 remoto de gestión de la prueba ilustrado en la Fig. 3. Más específicamente, el módulo 507 de comunicación se configura para recibir los parámetros de la prueba y proporcionar los parámetros de la prueba proporcionados al PRPG 201, por ejemplo, a través de un módulo 502 configurado para almacenar de manera temporal los parámetros de la prueba. El módulo 507 de comunicación se configura además para recibir una firma de la prueba desde el MISR 203 y para transmitir la firma de la prueba al dispositivo remoto de gestión de la prueba.

El controlador 506 del módulo 500 de prueba comprende unos medios de procesamiento, tales como una memoria 511 que almacena el programa informático 512, y una unidad de procesamiento 510 que ejecuta el programa informático 512, a través de la cual el controlador 506 está operativo para controlar el módulo 500 de prueba para realizar las pruebas lógicas en respuesta a la recepción de los parámetros de la prueba desde el dispositivo remoto de gestión de la prueba. Más específicamente, el módulo 500 de prueba está operativo para recibir uno o más parámetros de la prueba desde un dispositivo remoto de gestión de la prueba, a través del módulo 507 de comunicación, generar uno o más patrones de la prueba basados en los parámetros recibidos de la prueba, usando el PRPG 201, aplicar los patrones de la prueba al CUT 101, recibir las repuestas a la prueba desde el CUT 101, compactar las respuestas a la prueba en una firma de la prueba, usando el MISR 203, y transmitir la firma de la prueba al dispositivo remoto de gestión de la prueba, usando el módulo 507 de comunicación.

De manera opcional, el controlador 506 se puede configurar además para realizar pruebas lógicas de manera autónoma, por ejemplo, en un encendido o un reinicio, en respuesta a una condición de fallo, o en respuesta a un desencadenante externo recibido a través de una entrada 114 de control opcional. La entrada 114 de control se puede usar también para alternar el dispositivo electrónico 320 entre un modo normal de operación y un modo de prueba, o para iniciar un ciclo de prueba, y puede, por ejemplo, estar conectado a una unidad de supervisión de fallos proporcionada junto con el dispositivo electrónico 320.

Una realización 600 alternativa del módulo 322 de prueba se describe ahora con referencia a la Fig. 6. De manera similar al módulo 500 de prueba, el módulo 600 de prueba comprende un PRPG 201 para generar los patrones pseudoaleatorios de la prueba y un MISR 203 para compactar las respuestas a la prueba recibidas desde el CUT 101 a través de los resultados 112 de la prueba en una firma de la prueba. Además, el módulo 600 de prueba comprende un módulo 607 de comunicación configurado para comunicarse con un dispositivo remoto de gestión de la prueba a través de una red de comunicaciones, tal como el dispositivo 310 remoto de gestión de la prueba ilustrado en la Fig. 3. De manera similar al módulo 507 de comunicación, el módulo 607 de comunicación se configura para recibir los parámetros de la prueba y proporcionar los parámetros de la prueba recibidos al PRPG 201, por ejemplo, a través del módulo 502 configurado para almacenar de manera temporal los parámetros de la prueba.

El módulo 600 de prueba comprende además una lógica 604 de decisión configurada para comparar la firma de la prueba obtenida del MISR 203 con la firma esperada, como es conocido en la técnica. Sin embargo, a diferencia del módulo LBIST 102, la firma esperada no se almacena o se cablea en el módulo 600 de prueba sino que se recibe desde el dispositivo remoto de gestión, a través del módulo 607 de comunicación. Con este fin, el módulo 607 de comunicación se configura para recibir la firma esperada y proporcionar la firma esperada recibida a la lógica 604 de decisión, por ejemplo, a través de un módulo 605 configurado para almacenar de manera temporal la firma esperada. La lógica 604 de decisión se puede configurar además para proporcionar el resultado de la comparación, esto es, el resultado de la prueba, al módulo 607 de comunicación que se puede configurar además para transmitir la información perteneciente al resultado de la prueba al dispositivo de gestión remoto. Opcionalmente además, la lógica 604 de decisión se puede configurar para hacer disponible el resultado de la prueba a un circuito externo, por ejemplo, una unidad de supervisión de fallos proporcionada junto con el dispositivo electrónico 320, por medio de una señal 115.

El controlador 606 del módulo 600 de prueba comprende unos medios de procesamiento, tales como una memoria 611 que almacena un programa informático 612, y una unidad 610 de procesamiento que ejecuta el programa informático 612, a través del cual el controlador 606 está operativo para controlar el módulo 600 de prueba para realizar las pruebas lógicas en respuesta a los parámetros de la prueba recibidos desde el dispositivo de gestión remoto. Más específicamente, el módulo 600 de prueba está operativo para recibir uno o más parámetros de la prueba desde un dispositivo remoto de gestión de la prueba, a través del módulo 607 de comunicación, generar uno o más patrones de la prueba basados en los parámetros de la prueba recibidos, usando el PRPG 201, aplicar los patrones de la prueba al CUT 101, recibir las respuestas a la prueba desde el CUT 101, compactar las respuestas a la prueba en la firma de la prueba, usando el MISR 203, recibir la firma esperada correspondiente al conjunto de patrones de la prueba desde el dispositivo remoto de gestión de la prueba, a través del módulo 607 de comunicación, y determinar el resultado de la prueba basado en la comparación de la firma esperada recibida con la firma de la prueba, usando la lógica 604 de decisión.

De manera opcional, el controlador 606 se puede configurar además para realizar pruebas lógicas de manera autónoma, por ejemplo, en el encendido o en un reinicio, en respuesta a una condición de fallo, o en respuesta a un

desencadenante externo recibido a través de una entrada 114 de control opcional. La entrada 114 de control se puede usar también para alternar el dispositivo electrónico 320 entre un modo normal de operación y un modo de pruebas, o para iniciar un ciclo de pruebas, y puede, por ejemplo, conectarse a una unidad de supervisión de fallos proporcionada junto con el dispositivo electrónico 320.

Las realizaciones del módulo 322 de prueba, así como los módulos 500 y 600, y en concreto los módulos 507 y 607 de comunicación, se pueden configurar además para encriptar la comunicación con el dispositivo remoto de gestión de la prueba, por ejemplo, usando SSH, SSL, TSL, IPsec, o similar, como es conocido en la técnica. Esto es, se descifran los parámetros de la prueba y, opcionalmente, la firma esperada, recibida desde el dispositivo remoto de gestión de la prueba. En consecuencia, la firma de la prueba y el resultado de la prueba se encripta antes de la transmisión al dispositivo remoto de gestión de la prueba. De manera adicional, el dispositivo electrónico 320 se puede adaptar para autenticar la comunicación con el dispositivo 310 remoto de gestión de la prueba como es conocido en la técnica, evitando de este modo los ataques de hombre en el medio y de suplantación.

La comunicación entre los módulos 507 y 607 de comunicación y los controladores 506 y 606, respectivamente, se pueden efectuar de acuerdo con el IEEE 1149.1 “Arquitectura de Escaneo en Frontera y Puerto de Acceso a la Prueba Estándar”, comúnmente nombrado como Grupo de Acción de la Prueba de Conjunta (JTAG).

A continuación, se describen realizaciones adicionales de la invención con referencia a las Fig. 7 a 10.

En la Fig. 7, se ilustra una realización de un método 700 de prueba de un circuito lógico digital comprendido en un dispositivo electrónico, tal como un CUT 101 comprendido en un dispositivo electrónico 320. El método 700 es realizado por el dispositivo electrónico y comprende la recepción en 701 de uno o más parámetros de la prueba desde un dispositivo remoto de gestión de la prueba, tal como el dispositivo 310 remoto de gestión de la prueba, y la generación en 702 de uno o más patrones de la prueba basados en los parámetros de la prueba recibidos. El método 700 comprende además la aplicación en 703 del patrón de la prueba al circuito lógico digital, la recepción en 704 de una o más respuestas a la prueba desde el circuito lógico digital, una por cada patrón de la prueba, la compactación en 705 de las respuestas a la prueba recibidas desde el circuito lógico digital en la firma de la prueba, y la transmisión en 706 de la firma de la prueba al dispositivo remoto de gestión de la prueba. El método 700 puede comprender además pasos adicionales de acuerdo con lo que se describió anteriormente, en particular con referencia a las Fig. 3 a 6.

En la Fig. 8, se ilustra una realización de otro método 800 de prueba de un circuito lógico digital comprendido en un dispositivo electrónico, tal como el CUT 101 comprendido en el dispositivo electrónico 320. El método 800 es realizado por el dispositivo electrónico y comprende la recepción en 801 de uno o más parámetros de la prueba desde un dispositivo remoto de gestión de la prueba, tal como el dispositivo 310 remoto de gestión de la prueba, y la generación en 802 de uno o más patrones de la prueba basados en los parámetros de la prueba recibidos. El método 800 comprende además la aplicación en 803 de los patrones de la prueba al circuito lógico digital, la recepción en 804 de una o más respuestas a la prueba desde el circuito lógico digital, una por cada patrón de la prueba, la compactación en 805 de las respuestas a la prueba recibidas desde el circuito lógico digital en una firma de la prueba, la recepción en 806 de una firma esperada correspondiente a los patrones de la prueba desde el dispositivo remoto de gestión de la prueba, y la determinación en 807 de los resultados de la prueba basados en la comparación de la firma esperada recibida con la firma de la prueba. Opcionalmente, el método 800 puede comprender la transmisión en 808 de la información perteneciente al resultado de la prueba hasta el dispositivo remoto de gestión de la prueba. El método 800 puede comprender además pasos adicionales de acuerdo con lo que se describió anteriormente, en concreto con referencia a las Fig. 3 a 6.

Las realizaciones de los métodos 700 u 800 pueden ser implementadas por un programa informático 512 (o 612) que comprende instrucciones ejecutables por ordenador para provocar que un dispositivo, tal como un módulo 500 (o 600) de prueba las realice en consecuencia, cuando las instrucciones ejecutables por ordenador se ejecutan en una unidad 510 (o 610) de procesamiento comprendida en el dispositivo. Con referencia a lo que se ha descrito aquí anteriormente, se apreciará que algunos o todos los pasos del método 700 (u 800) se realicen en cooperación con otras partes funcionales del módulo 500 (o 600) de prueba. Por ejemplo, el paso 701 de recepción de uno o más parámetros de la prueba desde un dispositivo remoto de gestión de la prueba se realiza en cooperación con el módulo 507 de comunicación, y el paso 702 de generación de uno o más patrones de la prueba basados en los parámetros de la prueba recibidos se realiza en cooperación con el PRPG 201.

En la Fig. 9, se ilustra una realización de un método 900 de prueba de un circuito lógico digital comprendido en un dispositivo electrónico, tal como un CUT 101 comprendido en un dispositivo electrónico 320. El método 900 es realizado por un dispositivo remoto de gestión de la prueba, tal como el dispositivo 310 remoto de gestión de la prueba. El método comprende la adquisición en 901 de uno o más parámetros de la prueba adecuados para generar uno o más patrones de la prueba para un circuito lógico digital, la adquisición en 902 de una firma esperada correspondiente a los patrones de la prueba, y la transmisión en 903 de los parámetros de la prueba a al menos un dispositivo electrónico que comprende el circuito lógico digital. El método 900 comprende además la recepción en 904 de una firma de la prueba desde al menos un dispositivo electrónico, y la determinación en 905 de un resultado de la prueba basado en la comparación de la firma esperada con la firma de la prueba recibida. El método 900

puede comprender además pasos adicionales de acuerdo con lo que se ha descrito aquí anteriormente, en concreto con referencia a las Fig. 3 a 6.

En la Fig. 10, se ilustra otra realización de un método 1000 de prueba de un circuito lógico digital comprendido en un dispositivo electrónico, tal como un CUT 101 comprendido en un dispositivo electrónico 320. El método 1000 es realizado por un dispositivo remoto de gestión de la prueba, tal como el dispositivo 310 remoto de gestión de la prueba. El método 1000 comprende la adquisición en 1001 de uno o más parámetros de la prueba adecuados para generar uno o más patrones de la prueba para un circuito lógico digital, la adquisición en 1002 de una firma esperada correspondiente a los patrones de la prueba, la transmisión en 1003 de los parámetros de la prueba a al menos un dispositivo electrónico que comprende el circuito lógico digital, y la transmisión en 1004 de la firma esperada a al menos un dispositivo. Opcionalmente, el método 1000 puede comprender además la recepción en 1005 de la información perteneciente a un resultado de la prueba para los patrones de la prueba desde el al menos un dispositivo electrónico. El método 1000 puede comprender además pasos adicionales de acuerdo con lo que se ha descrito aquí anteriormente, en concreto con referencia a las Fig. 3 a 6..

Las realizaciones de los métodos 900 o 1000 pueden ser implementadas por un programa informático 313 que comprende instrucciones ejecutables por ordenador para provocar que un dispositivo funcione en consecuencia, cuando las instrucciones ejecutables por ordenador se ejecutan en una unidad 311 de procesamiento comprendido en el dispositivo.

Una persona experta en la técnica se dará cuenta que la invención de ninguna manera está limitada a las realizaciones descritas anteriormente. También se apreciará que las realizaciones de la invención se pueden implementar en hardware, esto es, en diferentes tipos de circuitería electrónica, software, esto es, medios de procesamiento que ejecutan un programa informático adecuado, o en cualquier combinación de los mismos. El alcance de la invención está definido por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un dispositivo electrónico (320; 1100; 1200; 1300) que comprende:

un circuito (101) lógico digital , y un módulo (322; 600) de prueba que se adaptan para:

recibir uno o más parámetros adecuados de la prueba para generar uno o más patrones de la prueba para el circuito lógico digital desde un dispositivo remoto de gestión de la prueba,

generar uno o más patrones de la prueba basados en los parámetros de la prueba,

aplicar los patrones de la prueba al circuito lógico digital,

recibir una o más respuestas a la prueba desde el circuito lógico digital, y

compactar las respuestas a la prueba en una firma de la prueba,

estando el dispositivo electrónico caracterizado en que el módulo de prueba se adapta además para:

recibir una firma esperada correspondiente a los patrones de la prueba desde el dispositivo remoto de gestión de la prueba, y

determinar el resultado de la prueba basado en la comparación de la firma esperada con la firma de la prueba.

2. El dispositivo electrónico según la reivindicación 1, estando el módulo de prueba adaptado para determinar el resultado de la prueba como indicando un fallo en el circuito lógico digital si la firma esperada difiere de la firma de la prueba.

3. El dispositivo electrónico según las reivindicaciones 1 o 2, estando el módulo de prueba adaptado además para transmitir la información perteneciente al resultado de la prueba hasta el dispositivo remoto de gestión de la prueba.

4. El dispositivo electrónico según cualquiera de las reivindicaciones 1 a 3, que comprende además un generador (201) pseudo aleatorio adaptado para generar patrones de la prueba basados en los parámetros de la prueba.

5. El dispositivo electrónico según cualquiera de las reivindicaciones 1 a 4, en donde los parámetros de la prueba comprenden al menos uno de un valor de inicialización, un número de patrones de la prueba a ser generados, y uno o más números de secuencia de los patrones de la prueba a ser generados.

6. El dispositivo electrónico según cualquiera de las reivindicaciones 1 a 5, siendo cualquiera de entre un Circuito Integrado (1100), un Sistema en Chip (1100), un Sistema en Paquete (1200), o un Sistema en Módulo (1200).

7. Un dispositivo criptográfico que comprende el dispositivo electrónico según cualquiera de las reivindicaciones 1 a 6.

8. Un terminal móvil (1300) que comprende el dispositivo electrónico según cualquiera de las reivindicaciones 1 a 6, o el dispositivo criptográfico según la reivindicación 7.

9. Un dispositivo (310) remoto de gestión de la prueba para probar un circuito (101) lógico digital comprendido en el dispositivo electrónico según cualquiera de las reivindicaciones 1 – 6, comprendiendo el dispositivo remoto de gestión de la prueba los medios (311 – 315) adaptados para:

adquirir una firma esperada correspondiente a los patrones de la prueba, y

transmitir los parámetros de la prueba a al menos un dispositivo electrónico que comprende el circuito lógico digital,

estando el dispositivo remoto de gestión de la prueba caracterizado en que los medios se adaptan además para:

transmitir la firma esperada hasta el al menos un dispositivo electrónico.

10. El dispositivo remoto de gestión de la prueba según la reivindicación 9, estando además los medios adaptados para recibir la información perteneciente al resultado de la prueba para los patrones de la prueba desde el al menos un dispositivo electrónico.

11. El dispositivo remoto de gestión de la prueba según las reivindicaciones 9 o 10, estando además los medios adaptados para adquirir la firma esperada mediante el cálculo de la firma esperada en base a los parámetros de la prueba y el diseño del circuito lógico digital.

12. El dispositivo remoto de gestión de la prueba según cualquiera de las reivindicaciones 9 a 11, en donde los parámetros de la prueba comprenden al menos uno con un valor de inicialización, un número de patrones de la prueba a ser generados, y uno o más números de secuencia de los patrones de la prueba a ser generados.

13. Un método (800) de prueba de un circuito (101) lógico digital comprendido en el dispositivo electrónico según cualquiera de las reivindicaciones 1 – 6, siendo el método realizado por el dispositivo electrónico y comprendiendo:

la recepción (801) de uno o más parámetros de la prueba adecuados para generar uno o más patrones de la prueba para el circuito lógico digital desde un dispositivo (310) remoto de gestión de la prueba,

la generación (802) de uno o más patrones de la prueba basados en los parámetros de la prueba,

la aplicación (803) de los patrones de la prueba al circuito lógico digital,

la recepción (804) de una o más respuestas a la prueba desde el circuito lógico digital, y

la compactación (805) de las respuestas a la prueba en una firma de la prueba,

estando el método caracterizado en que comprende además:

la recepción (806) de una firma esperada correspondiente a los patrones de la prueba desde el dispositivo remoto de gestión de la prueba, y

la determinación (807) de un resultado de la prueba basado en la comparación de la firma esperada con la firma de la prueba.

14. El método según la reivindicación 13, en donde la determinación de un resultado de la prueba comprende indicar un fallo en el circuito lógico digital si la firma esperada difiere de la firma de la prueba.

15. El método (800) según las reivindicaciones 13 o 14, comprendiendo además la transmisión (808) de la información perteneciente al resultado de la prueba hasta el dispositivo remoto de gestión de la prueba.

16. El método según cualquiera de las reivindicaciones 13 a 15, en donde los patrones de la prueba se generan basados en los parámetros de la prueba usando un generador pseudoaleatorio comprendido en el dispositivo electrónico.

17. El método según cualquiera de las reivindicaciones 13 a 16, en donde los parámetros de la prueba comprenden al menos uno con un valor de inicialización, un número de patrones de la prueba a ser generado, y uno o más números de secuencia de los patrones de la prueba a ser generados.

18. Un método (1000) de prueba de un circuito (101) lógico digital comprendido en el dispositivo electrónico según cualquiera de las reivindicaciones 1 – 6, siendo el método realizado por un dispositivo (310) remoto de gestión de la prueba, comprendiendo el método:

la adquisición (1001) de uno o más parámetros de la prueba adecuados para generar uno o más patrones de la prueba para el circuito lógico digital,

la adquisición (1002) de una firma esperada correspondiente a los patrones de la prueba, y

la transmisión (1003) de los parámetros de la prueba a al menos un dispositivo electrónico que comprende el circuito lógico digital,

estando el método caracterizado en que además comprende:

la transmisión (1004) de la forma esperada hasta el al menos un dispositivo electrónico.

19. El método según la reivindicación 18, comprendiendo además la recepción (1005) de la información perteneciente al resultado de la prueba para los patrones de la prueba desde el al menos un dispositivo electrónico.

20. El método según las reivindicaciones 18 o 19, en donde la adquisición de la firma esperada comprende el cálculo de la firma esperada basado en los parámetros de la prueba y el diseño del circuito lógico digital.

21. El método según cualquiera de las reivindicaciones 18 a 20, en donde los parámetros de la prueba comprenden al menos uno con un valor de inicialización, un número de patrones de la prueba a ser generados, y uno o más números de secuencia de los patrones de la prueba a ser generados.

22. Un programa informático (313) que comprende instrucciones ejecutables por ordenador para provocar que un dispositivo (310) remoto de gestión de la prueba realice todos los pasos del método según cualquiera de las reivindicaciones 18 a 21, cuando las instrucciones ejecutables por ordenador son ejecutadas en una unidad (311) de procesamiento comprendida en el dispositivo remoto de gestión de la prueba.

23. Un producto de programa informático que comprende un medio (312) de almacenamiento legible por ordenador, teniendo el medio de almacenamiento legible por ordenador el programa informático representado en este según la reivindicación 22.

Fig. 1

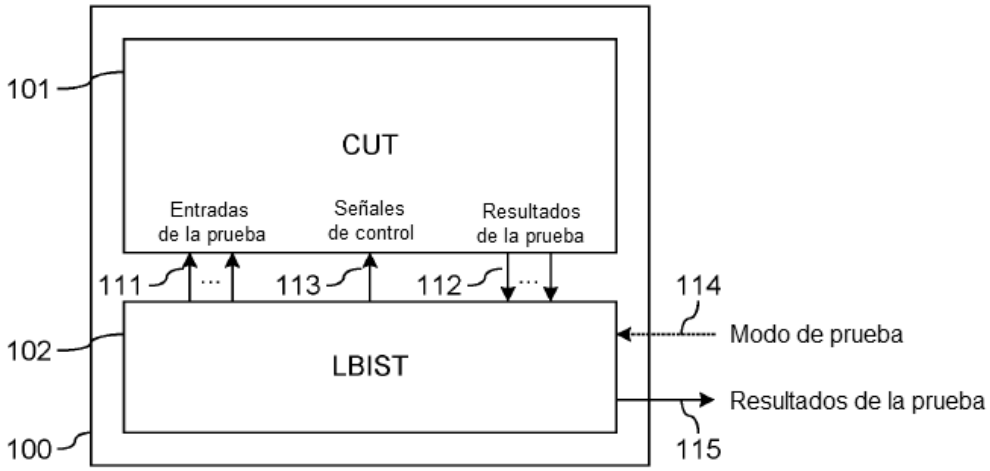
101
CUT
Entradas de la prueba
Señales de control
Resultados de la prueba
111
113
112
114
Modo de prueba
102
LBIST
Resultados de la prueba
100
115

Fig. 2

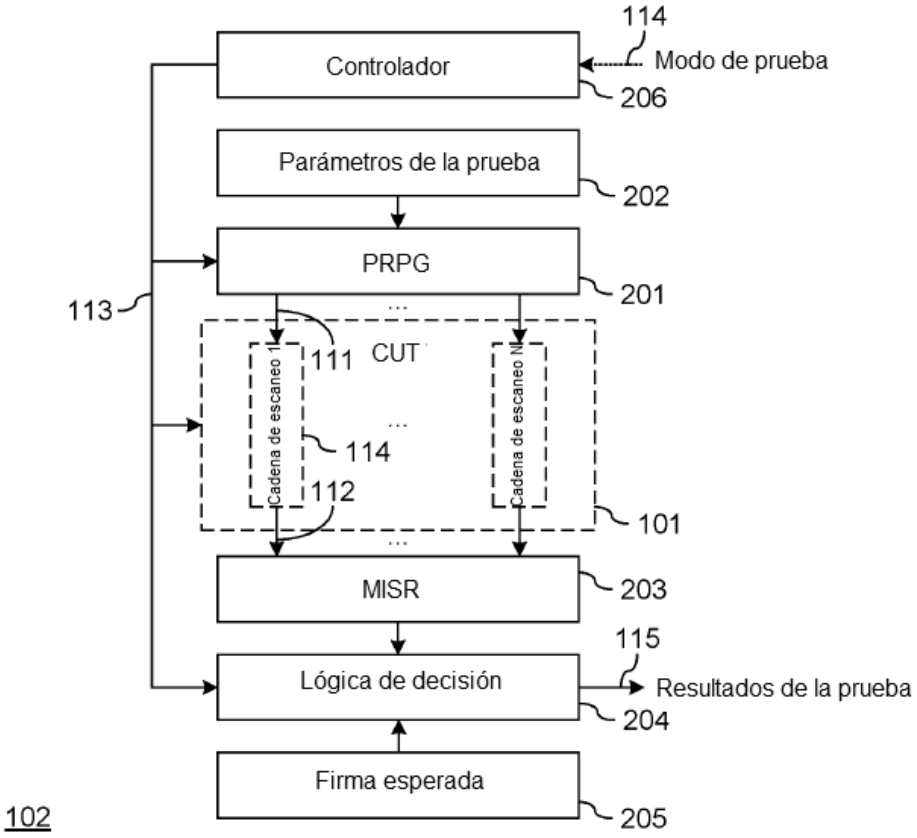
114
Controlador
Modo de prueba
206
Parámetros de la prueba
202
PRPG
201
113
111
CUT
Cadena de escaneo 1
Cadena de escaneo N
114
112
101
MISR
203
115
Lógica de decisión
Resultados de la prueba
204
Firma esperada
205
102

Fig. 3

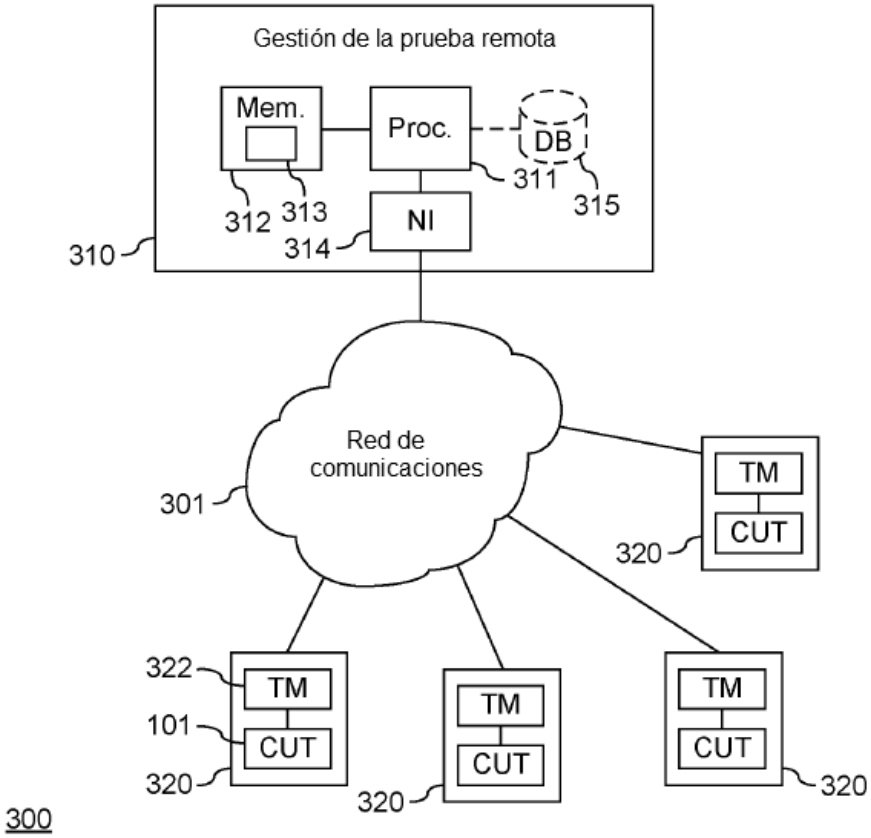
Gestión de la prueba remota
Mem.
Proc.
DB
311
315
312
313
NI
314
310
Red de comunicaciones
301
TM
CUT
320
322
TM
101
CUT
320
TM
CUT
320
TM
CUT
320
300

Fig. 4

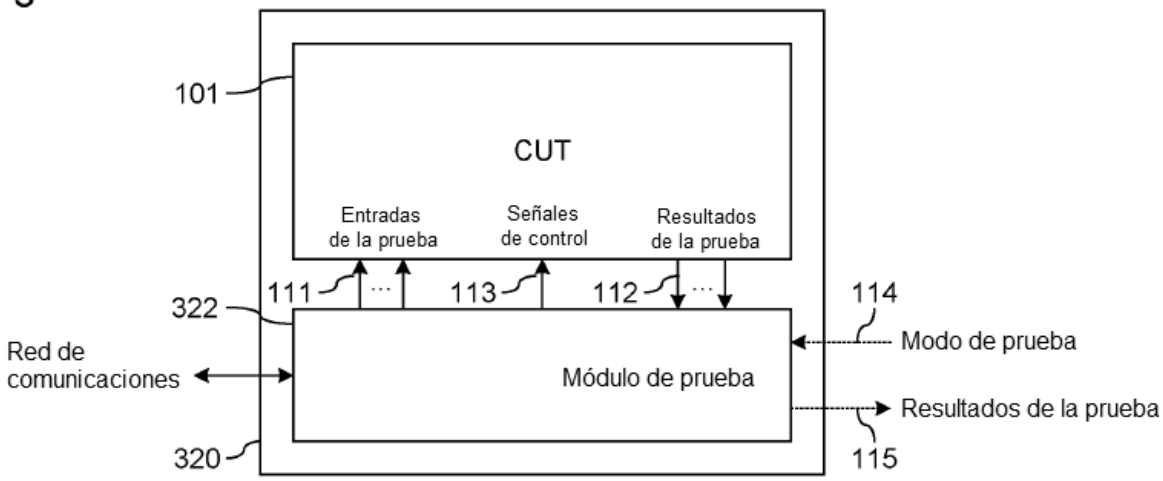
101
CUT
Entradas de la prueba
Señales de control
Resultados de la prueba
111
113
112
114
322
Red de comunicaciones
Módulo de prueba
Modo de prueba
Resultados de la prueba
320
115

Fig. 5

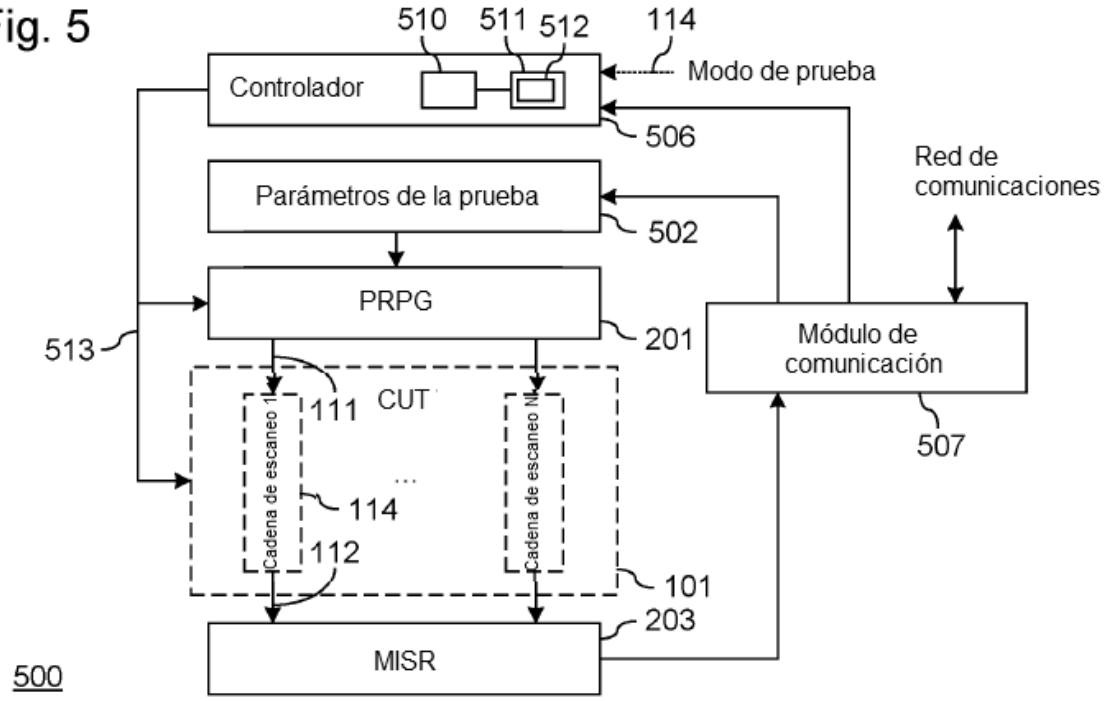
510
511
512
114
Controlador
Modo de prueba
506
Red de comunicaciones
Parámetros de la prueba
502
PRPG
201
513
Módulo de comunicación
111
CUT
Cadena de escaneo 1
Cadena de escaneo N
...
114
112
507
101
203
MISR
500

Fig. 6

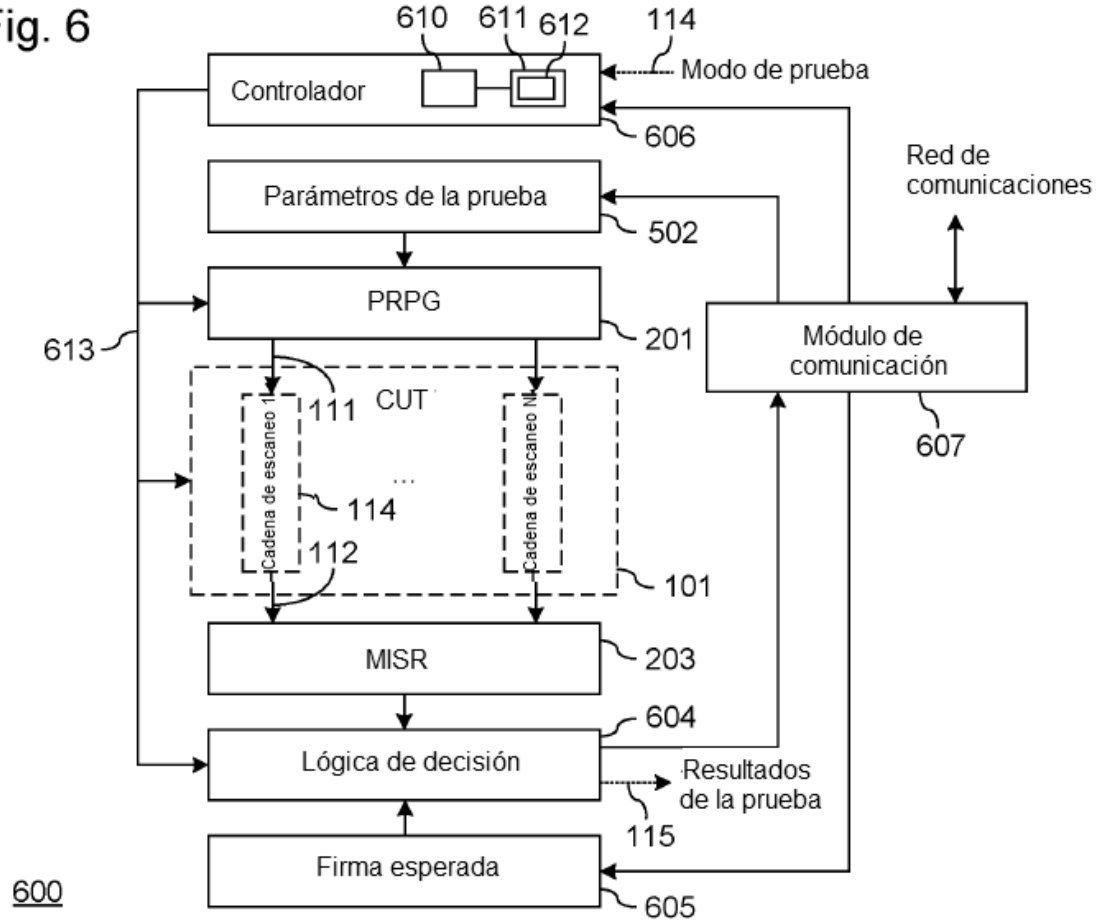
610
611
612
114
Controlador
Modo de prueba
606
Red de comunicaciones
Parámetros de la prueba
502
PRPG
201
613
Módulo de comunicación
111
CUT
Cadena de escaneo 1
Cadena de escaneo N
...
114
112
607
101
MISR
203
604
Lógica de decisión
Resultados de la prueba
115
Firma esperada
600
605

Fig. 7

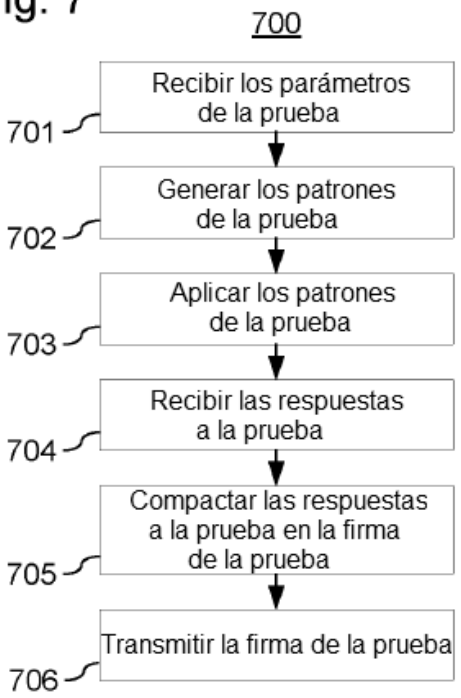

Fig. 8

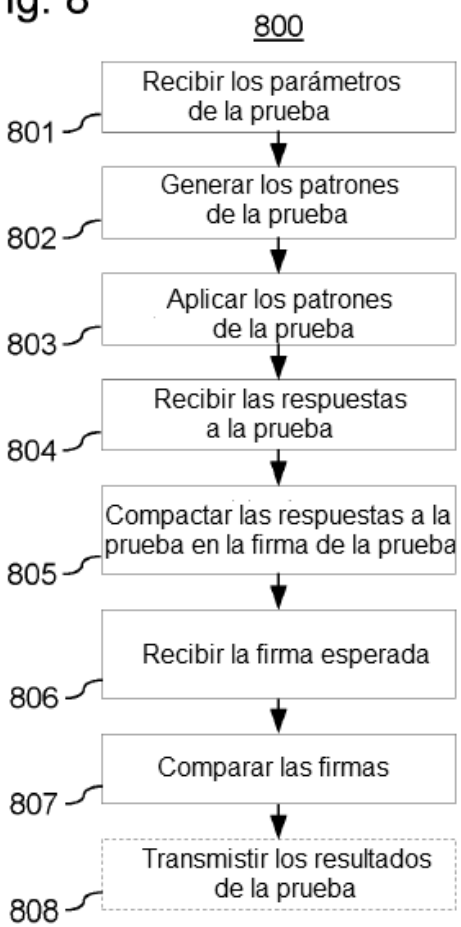

Fig. 9

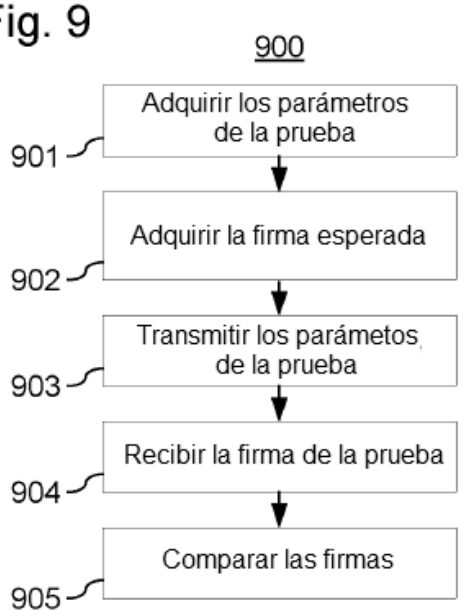

Fig. 10

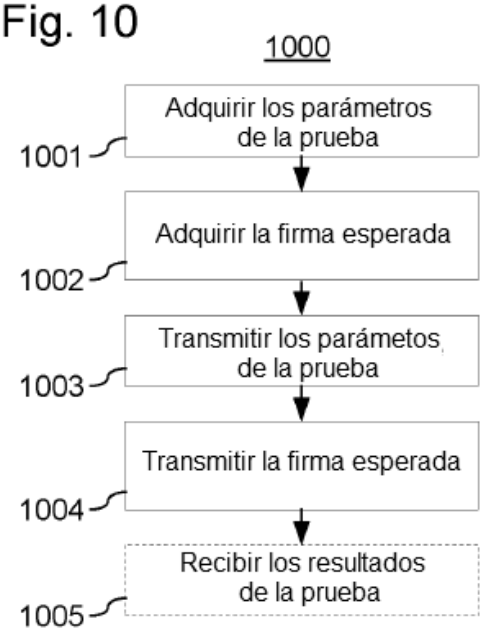

Fig. 11

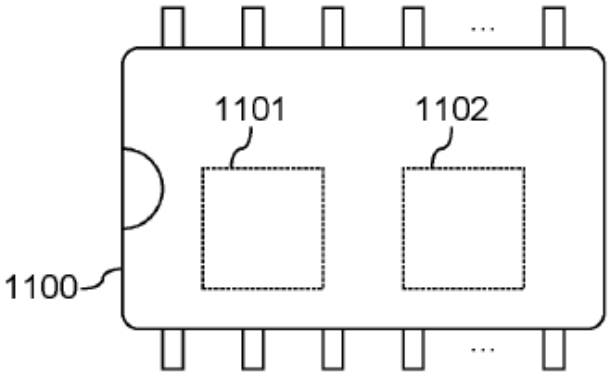

Fig. 12

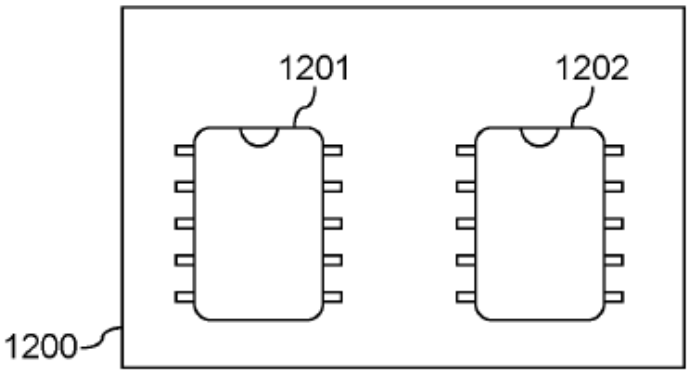
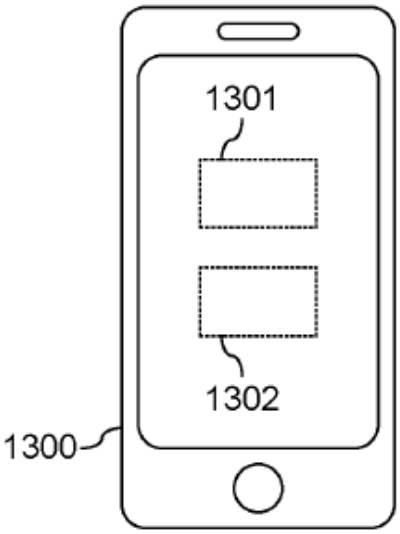
Fig. 13